ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

FINAL REPORT - ANNEX

A study prepared for the European Commission
DG Communications Networks, Content & Technology by:
This study was carried out for the European Commission by:

![Time.lex](image1)

Internal identification

Contract number: 30-CE-0629642/00-85

SMART 2013/0071

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission’s behalf may be held responsible for the use which may be made of the information contained therein.


doi:10.2759/26900

© European Union, 2015. All rights reserved. Certain parts are licensed under conditions to the EU.

Reproduction is authorised provided the source is acknowledged.
COUNTRY REPORT

AUSTRIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Erich Schweighofer and Walter Hötzendorfer, Vienna Centre for Legal Informatics (WZRI)

Date: 29.08.2014
Contents

Part 1: Management summary ........................................................................................................3
Part 2: Answers to the questionnaire ...............................................................................................4
Part 1: Management summary

Management summary for Austria

The transposition of the ePrivacy Directive into Austrian law can be summarized as follows:

- The provisions with regard to the scope of the Directive have been transposed in a single act, the Telecommunications Act 2003, which also implements Directive 2002/21/EC (Framework Directive) and other related legislation. Although Austria is a federal country, due to the federal competence in this field, the transposition was only necessary at the federal level.
- Various authorities are competent for the execution of the Telecommunications Act 2003, which – as mentioned – contains a lot more than the provisions implementing the ePrivacy Directive. Regarding these provisions it should be made more explicit which authority is competent for executing which provision and it seems that the fragmentation of competencies is not an ideal situation altogether for achieving an effective enforcement of the law. The competent authority for executing the majority of these provisions is the Austrian Data Protection Authority, which, however, notoriously has a very limited number of staff and a very high workload. This leads to the situation that it focuses primarily on executing the Data Protection Act and dealing with individual complaints and seemingly not much on (proactively) executing the provisions implementing the ePrivacy Directive. This is not because of a lack of expertise but because of a lack of resources and a resulting focus on cases where individuals complain actively.
- Several of the provisions implementing the ePrivacy Directive follow the requirements of the Directive closely. In some provisions significant differences to the Directive can be found, e.g. in the provision implementing article 5.3 (with regard to scope). Some provisions are not fully clear, e.g. the consent requirement for cookies.
- Amendments of the telecommunications act are usually drafted in close collaboration with RTR GmbH (i.e. the regulator, see below), the primary focus of which is not data protection.
- The amount of written guidance on the application of the provisions implementing the ePrivacy Directive is very limited. The more informal communication within the community of Austrian telecommunication lawyers working either for the providers or their lobby groups or for the competent authorities seems to work very well and the RTR GmbH, which is the – well-equipped – competent authority for the majority of the (general) regulatory issues on the Austrian telecommunications sector works closely with the providers. This, however, does not mean that there are any signs of a lack of independence of RTR GmbH.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)


Following the 2009 amendments of the European Regulatory Framework for Electronic Communications, the Austrian legislator amended the Telecommunications Act 2003 to implement the new provisions.

<table>
<thead>
<tr>
<th>Concordance table</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePrivacy Directive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Art. 2 (Definitions)</td>
<td>Telecommunications Act 2003, Sec. 92 para. 3</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
<td>Telecommunications Act 2003, Sec. 92 para. 1</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>Telecommunications Act 2003, Sec. 93</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Not explicitly transposed. It follows from general data protection law that such recording can be lawful under certain circumstances.</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Telecommunications Act 2003,</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 6 (Traffic data)</td>
<td>Telecommunications Act 2003, Sec. 99</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Telecommunications Act 2003, Sec. 102</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
<tr>
<td>Art. 13 (Unsolicited communications)</td>
<td>Telecommunications Act 2003, Sec. 107</td>
<td><a href="https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html">https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2003_1_70/ERV_2003_1_70.html</a></td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datenschutzbehörde (DSB)</td>
<td>Data Protection Authority</td>
<td>All provisions having an impact on privacy or data protection</td>
<td><a href="http://www.dsb.gv.at/DesktopDefault.aspx?alias=dsken">http://www.dsb.gv.at/DesktopDefault.aspx?alias=dsken</a></td>
</tr>
<tr>
<td>Oberste Fernmeldebehörde und Fernmeldebüros</td>
<td>National Telecommunications Authority and Telecommunications Offices</td>
<td>For all official acts under the Telecommunications Act 2003 unless otherwise provided, i.e. administrative penalties and unsolicited communications (sec. 113 para. 3 Telecommunications Act 2003).</td>
<td>No website. Information here: <a href="http://www.bmvit.gv.at/telekommunikation/organisation/ofb.htm">http://www.bmvit.gv.at/telekommunikation/organisation/ofb.htm</a> and here:</td>
</tr>
</tbody>
</table>
### 3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?


Sec. 3 no. 11 of the Telecommunications Act 2003 defines **communications network** as “means transmission systems and, where applicable, switching or routing equipment and other resources which permit the electronic conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed”. This definition is identical with the definition of article 2 (a) of the Framework Directive. The only difference is the term itself: The Telecommunications Act 2003 uses the term “communications network” while the Directive uses the term “electronic communications network”.

Sec. 3 no. 17 of the Telecommunications Act 2003 defines **public communications network** as “a communications network used wholly or mainly for the provision of publicly available communications services”. This definition has a different wording than the definition of article 2 (d) of the Framework Directive. However, no material difference can be noticed.

Sec. 3 no. 9 of the Telecommunications Act 2003 defines **communications service** as “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using communications networks and services; it does not include information society services, as defined in § 1 (1) item 2 of the Notification Act [Notifikationsgesetz], BGBI. I no. 183/1999, which do not consist wholly or mainly in the conveyance of signals on communications networks”. This definition is identical with the definition of article 2 (c) of the Framework Directive. The only difference is the term itself: The Telecommunications Act 2003 uses the term “communications service” while the Directive uses the term “electronic communications service”. However, this does not make any difference; it is clear from the context that the provisions are only applicable to electronic communication.1

Sec. 3 no. 3 of the Telecommunications Act 2003 defines **operator of a communications service** as “an undertaking that exercises the legal control over the functions in their entirety that are needed to provide the respective communications service and that offers these services to others”.

Sec. 3 no. 4 of the Telecommunications Act 2003 defines **operator of a communications network** as “an undertaking that exercises the legal and actual control over the network functions in their

---

entirety. Operation of a communications network within the meaning of this Act shall not be the case if the connection to other public communications networks is exclusively effected via the interfaces generally used for the local loop”.

In the context of the provisions of the Telecommunications Act 2003 implementing the ePrivacy Directive sec. 92 para 3 no. 1 defines that provider “means an operator of public communications services”. Many provisions of the Telecommunications Act 2003 implementing the ePrivacy Directive explicitly address the “provider”.

It can be concluded that the scope of the Austrian implementing legislation corresponds to the scope of the ePrivacy Directive, also with regard to fact that both apply to publicly available electronic communications services.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

<table>
<thead>
<tr>
<th></th>
<th>In 2005 RTR GmbH published guidelines for providers of VoIP services. In the document an important distinction is made between “internet-only” VoIP services and VoIP services that provide access to the common telephone network (public switched telephone network, PSTN). “Internet-only” VoIP services do not provide this access and the actual transmission of IP packages between the calling and the called VoIP user are not part of the VoIP service. Therefore “internet-only” VoIP services do not fall within the definition of a public communications service and hence not within the scope of the Telecommunications Act 2003. Conversely, all VoIP services that do provide access to the PSTN are regarded as publicly available telephone services (PATS) pursuant to sec. 3 no. 16 Telecommunications Act 2003 and hence do fall within the scope of the Telecommunications Act 2003. Also the information page regarding the notification of the provision of communications networks and services on the RTR GmbH website follows this interpretation. The same is true for webmail and location based services because and insofar these services only use but do not provide actual transmission of IP packages and hence do not fall within the definition of a communications service.</th>
</tr>
</thead>
</table>

---


3 https://www.rtr.at/de/tk/AGGInfos (13 Aug 2014), only available in German.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The Telecommunications Act 2003 does not explicitly say anything about its territorial scope. According to RTR GmbH the implementing legislation is applicable to all operators of public communications networks or services that underlie the notification obligation laid down in sec. 15 para. 1 of the Telecommunications Act 2003: “The intended provision of a public communications network or service as well as its modifications and its termination shall be notified to the regulatory authority prior to the start of operation, modification or termination.” However, this doesn’t answer the question directly, but only implicitly, because it can be concluded that sec. 15 para. 1 of the Telecommunications Act 2003 applies to the intended provision of a public communication network or service on the territory of Austria.

There is a decision on this matter where the implementing legislation was been applied to foreign entities: In case R 8/08-03 the Telekom-Control Commission “suspend Skype Communications S.a.r.l.’s right to provide communications services which establish connections to the public switched telephone network (PSTN) in Austria until the company complies with the provisions of Articles 15, 20, 22 and 25 Par. 1 of the Austrian Telecommunications Act (TKG) 2003. In particular, this decision concerns the service offered under the name ‘Skype Out’.

The service provided by Skype Communications S.a.r.l. in which registered Skype users can establish connections to other registered Skype users (who are addressed by way of the user names administered by Skype) exclusively via the Internet is not regarded by the regulatory authority as a communications service pursuant to Art. 3 No. 9 TKG 2003, and therefore the regulatory authority does not consider this service to be a public telephone service pursuant to Art. 3 No. 16 TKG 2003. As a result, the official decision did not apply to this service.”

This is an example where the telecommunications service provider (Skype) was not established in Austria but provided a public telecommunications service “in Austria” (as mentioned on page one of the decision) and did not comply with the notification obligation pursuant to the aforementioned provision of sec. 15 (misleadingly called “Article” in the cited text). Skype continued (and most likely still continues) to provide the service in the same way while it did not follow its notification obligation even after this decision.

From this example it can be concluded that in practice a telecommunications service provider needs to have at least a branch office in Austria to make effective application of the implementing provisions possible.

---

4 From [https://www.rtr.at/en/tk/R_8_08](https://www.rtr.at/en/tk/R_8_08), where the (German) full text can also be found.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

| a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases) |
| b. national courts through rendering of case law |

a. RTR GmbH publishes opinions on important questions in its field of action, but only on rare occasions, i.e. less than one opinion per year. In 2005 it published guidelines for providers of VoIP services. For details on these guidelines see the answer to question 4 above. Other opinions or guidelines do not deal with the definitions mentioned in this section.

b. Case VwGH 27. 5. 2009, 2007/05/0280: The Austrian Administrative court ruled in the context of investigative powers of the police that operating of a chat room is not a telecommunications service pursuant to sec. 3 no. 9 Telecommunications Act 2003 and hence does not fall within the Telecommunications Act 2003.

---


6 https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vwgh&Dokumentnummer=JWT_2007050280_20090527X00, not available in English.
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The definitions are relatively clear and logically consistent and follow the definitions in the Directives closely. The provisions regulating which authority is competent for which issues could be clearer and more explicit.


   There is no obvious solution to improve the situation of the difficulty to execute decision concerning providers not established in Austria, which was discussed under question 5 above.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

In Austria the principle of confidentiality of communications is a fundamental right laid down in article 10a of the Basic Law on the General Rights of Nationals (Staatsgrundgesetz, StGG)⁷. In addition, already before the transposition of the ePrivacy Directive the principle of confidentiality of communications was laid down in sec. 88 of the Telecommunications Act 1997 in a very similar way to the current provision that implements article 5.1 of the ePrivacy Directive.

This provision is sec. 93 of the Telecommunications Act 2003:

“(1) The content data, traffic data and location data shall be subject to confidentiality of the communications. Confidentiality of the communications shall also refer to the data of unsuccessful connection attempts.

(2) Every operator and all persons who are involved in the operator’s activities shall observe confidentiality of the communications. The obligation to maintain confidentiality shall continue to exist also after termination of the activities under which it was established.

(3) Persons other than a user shall not be permitted to listen, tap, record, intercept or otherwise monitor communications and the related traffic and location data as well as pass on related information without the consent of all users concerned. This shall not apply to the recording and tracing of telephone calls when answering emergency calls and to cases of malicious call tracing, monitoring of communications and the information on data of a communication as well as to technical storage which is necessary for the conveyance of a communication.

(4) If communications are received unintentionally by means of a radio system, a telecommunications terminal equipment or any other technical equipment which are not intended for this radio system, this telecommunications terminal equipment or the user of the other equipment, the contents of the communications as well as the fact that they have been received must neither be recorded nor communicated to unauthorised persons nor used for any purposes. Recorded communications shall be erased or otherwise destroyed.

(5) The protection of editorial confidentiality (§ 31 Media Act) as well as other confidentiality obligations laid down in other federal acts must be respected in accordance with the protection of the clerical official secrecy and of professional secrets as well as the prohibition of bypassing them pursuant to §§ 144 and 157 para. 2 Criminal Procedure Act. The provider has no corresponding duty of inspection.”

Note: The exceptions laid down in the second sentence of para. 3 refer to call tracing on request of the subscriber in the case of malicious calls (in German “Fangschaltung”) and to particular investigative powers of the police (in German “Überwachung von Nachrichten” and “Auskunft über Daten einer Nachrichtenübermittlung”) laid down in the respective provisions. See details below at question 3.

The provision uses the term “communication” (in German: „Nachricht“, which generally also

translates to “message”) as defined in sec. 92 para. 3 no. 7 of the Telecommunications Act 2003: “any information exchanged or conveyed between a finite number of parties by means of a publicly available communications service. This does not include any information conveyed as part of a broadcasting service to the public over a communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information”.

The sanctions for breaching the confidentiality of communications are laid down in sec. 119 of the Criminal Code. Breach of the confidentiality of communications can result in a prison sentence of up to six months.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

Neither the Telecommunications Act 2003 nor any other act of legislation contains a transposition of Article 5.2 of the ePrivacy Directive. Such processing does not fall within the data protection provisions specific to telecommunications, but rather – as mentioned in recital 23 of the ePrivacy Directive – Directive 95/46/EC applies to such processing. Therefore in Austria such processing must be assessed under the provisions of the Data Protection Act 2000 and it seems appropriate to interpret it in the light of recital 23 of the ePrivacy Directive.\(^8\)

As a result, e.g. the recording of emergency calls can be lawful under sec. 8 para. 1 no. 3 of the Data Protection Act 2000 when vital interests of the data subject require the processing and also the recording of commercial call-center calls can be lawful, when the data subject is informed (cf. recital 23 of the ePrivacy Directive).\(^9\)

The issue does not seem to be a problem in practice but the legal situation in Austria is not as clear as it could be (and probably should be, given the existence of Article 5.2 of the ePrivacy Directive).


\(^9\) Ibid.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

As already mentioned above, sec. 93 para. 3 of the Telecommunications Act 2003 lays down the following exception (second sentence):

“Persons other than a user shall not be permitted to listen, tap, record, intercept or otherwise monitor communications and the related traffic and location data as well as pass on related information without the consent of all users concerned. This shall not apply to the recording and tracing of telephone calls when answering emergency calls and to cases of malicious call tracing, monitoring of communications and the information on data of a communication as well as to technical storage which is necessary for the conveyance of a communication.”

As already mentioned above, the exceptions laid down in the second sentence of para. 3 refer to call tracing on request of the subscriber in the case of malicious calls (in German “Fangschaltung”) and to particular investigative powers of the police (in German “Überwachung von Nachrichten” and “Auskunft über Daten einer Nachrichtenübermittlung”) laid down in the following provisions:

Sec. 106 Telecommunications Act 2003:

(1) Call tracing is the process of establishing the identity of a calling line, irrespective of the calling user’s will.
(2) If a subscriber so requests for the tracing of malicious calls, the operator shall set up a trace or override the elimination of the presentation of calling line identification for future calls. He may collect a charge for this service.
(3) The subscriber shall be informed of the result of the trace if he convincingly shows during the trace that he has been receiving malicious calls.

Sec. 134 para. 2 and 3 Criminal Procedure Code define the relevant terms. Sec. 135 Criminal Procedure Code lays down the conditions under which these measures are permitted. “Auskunft über Daten einer Nachrichtenübermittlung” is the provision of information about traffic data, access data or location data relating to a telecommunications service or information society service. “Überwachung von Nachrichten” is the investigation of the content of a communication which is transferred on a communications network or through an information society service. Generally speaking both measures are permitted in cases of kidnapping, or generally for investigating a serious act of crime (sec. 135 para. 2 and 3 of the Criminal Procedure Code). Pursuant to sec. 137 Criminal Procedure Code a court order is required for conducting these measures.

More exceptions to the confidentiality of communications are laid down in the Security Police Act: The police authorities can obtain information from telecommunications service providers or other service providers if necessary for their duties laid down in the Security Police Act. In particular they can obtain information on name and address of the users and IP Adresses of a particular message or of a particular user at a particular point in time (sec. 53 para. 3a of the Security Police Act).

In case a person is in danger the police authorities are authorised by sec. 53 para. 3b of the Security Police Act.
Police Act to obtain location data and the IMSI of the communication device of the endangered person from operators of public telecommunications services and to use technical measures to localise the person.

The Austrian provisions implementing the Data Retention Directive (Directive 2006/24/EC) have been repealed by the Austrian Constitutional Court\(^\text{10}\) with effect from 30 June 2014 in the light of the annulment of the Data Retention Directive by the ECJ. Currently, therefore, there are no data retention provisions in place in Austria but there is political discussion on if and how new measures replacing the unlawful data retention provisions should be implemented.

4. 

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

   a. The Austrian legislation doesn’t explicitly address “automated breaches of confidentiality without human intervention”. In principle such breaches of confidentiality are considered as an infringement of sec. 93 of the Telecommunications Act 2003 if they are outside the scope of the exceptions described above. This provision does not distinguish between content of the communications and other data relating to communications.

   In the context of non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks by Google during the capturing of the Google Street View images it was discussed that the capturing of payload (content) data from unencrypted Wi-Fi networks, as far as the data is personal data, is unlawful under general data protection legislation (Data Protection Act 2000). This was also the subject of a case of the Austrian Data Protection Authority after which Google promised to stop the capturing of Wi-Fi payload data.\(^\text{11}\) In this context it was also discussed that MAC addresses can also be regarded as personal data and the interception of MAC addresses would therefore be unlawful.\(^\text{12}\)

   b. Under the circumstances laid down therein, both automated and non-automated breaches of confidentiality can also be an act of crime under sec. 119 of the Criminal Code as far as it regards the content data. So in this case there is an important difference between content data and other data.

   That the principle of confidentiality of communications is a fundamental right laid down in article 10a of the Basic Law on the General Rights of Nationals was already mentioned above.

   In addition, if not under more specific provisions, private electronic communications are personal data and fall within the rules of the general data protection legislation.

\(^\text{11}\) Cf. Website of the Austrian Data Protection Authority: https://www.dsb.gv.at/site/6733/default.aspx (19 Aug 2014), English version at the bottom of the page.

\(^\text{12}\) Cf. Opinion of 25 May 2010 by the Austrian Data Protection Council on the collection and processing of data from Wi-Fi networks and payload data from publicly accessible Wi-Fi networks (only available in German), http://www.bka.gv.at/DocView.axd?CobId=39681 (19 Aug 2014)
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Based on a pre-existing provision (sec. 91 para. 3 Telecommunications Act 1997) on the provider’s information obligations, the provision of sec. 96 para. 3 Telecommunications Act 2003 transposes article 5.3 of the Directive. The provision is very similar to article 5.3 of the Directive. In addition, it contains the following: “The subscriber shall also be informed of the usage possibilities based on search functions embedded in electronic versions of the directories. This information shall be given in an appropriate form, in particular within the framework of general terms and conditions and, at the latest, upon commencement of the legal relations. The right to information pursuant to the Data Protection Act shall remain unaffected.”

A major difference between article 5.3 of the Directive and sec. 96 para. 3 Telecommunications Act 2003 is that the latter specifies an obligation to inform the subscriber or user only with regard to the collection, processing or transmission of personal data while the Directive does not contain this limitation. In this regard the Austrian implementation is narrower than the Directive.

A second difference is that the text of sec. 96 para. 3 Telecommunications Act 2003 limits the consent requirement to the collection of the data and does not mention processing and transmission. However an interpretation in conformance with the Directive and with the purpose of the provision leads to the conclusion that the consent is also required for processing and transmission of the data.\(^{13}\)

b. Sec. 96 para. 3 Telecommunications Act 2003 does not make any distinctions of these kinds.

\(^{13}\) Cf. Pachinger, Der neue "Cookie-Paragraph" - Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idF BGBl I 2011/102, jusIT 2012, 16.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Sec. 96 para. 3 Telecommunications Act 2003 does not establish any detailed requirements of these kinds. The level of detail corresponds to that of article 5.3 of the Directive. The text of sec. 96 para. 3 Telecommunications Act 2003 does not seem to allow the setting up of cookies before individuals have provided consent: “permitted only when the subscriber or user has provided his consent”. However, this is not completely clear. A related open question is whether consent must be explicit. On the one hand, the legislative materials mention that, if technically possible, user consent can be obtained by the use of the according settings in the browser or similar application. On the other hand, in the literature the opinion is expressed, that in the light of opinion WP 188 of the Article 29 Data Protection Working Party the common practice in Austria of not obtaining explicit consent cannot be upheld any more.

15 ErläutRV 1389 BlgNR 24, GP 25 (i.e. the official explanatory remarks regarding the government bill of the Telecommunications Act 2003).
16 Cf. Anderl and Tlapak, Für Cookies muss der User erst gefragt werden, Der Standard 2014/10/01.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent (i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The wording of the two explicit exceptions in 96 para. 3 Telecommunications Act 2003 is virtually identical to the wording in the Directive. However, as mentioned above, the provision itself contains additional fundamental exemptions:

A major difference between article 5.3 of the Directive and sec. 96 para. 3 Telecommunications Act 2003 is that the latter specifies an obligation to inform the subscriber or user only with regard to the collection, processing or transmission of personal data while the Directive does not contain this limitation. In this regard the Austrian implementation is narrower than the Directive.

A second difference is that the text of sec. 96 para. 3 Telecommunications Act 2003 limits the consent requirement to the collection of the data and does not mention processing and transmission. However an interpretation in conformance with the Directive and with the purpose of the provision leads to the conclusion that the consent is also required for processing and transmission of the data.17

According to the literature, an example for the first exception (“sole purpose of carrying out the transmission”) are cookies in the context of the use of parallel servers for load balancing purposes which are needed in case of failure of one server to enable another server to take over seamlessly.18 Examples for the second exceptions (“strictly necessary [...] to provide the service”) are shopping cart cookies (user-input cookies), multimedia player session cookies and authentication cookies, as long as they are only session cookies and not used for other purposes like targeted advertising.19 User-oriented security cookies that are used to prohibit the misuse of the log-in system are an example of cookies which extend beyond a single session and do not require user consent.20

---

17 Cf. Pachinger, Der neue "Cookie-Paragraph" - Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idf BGBl I 2011/102, justIT 2012, 16.
18 Cf. Hellbert, Nicht alle Kekse sind erwünscht, Der Standard 2013/12/06.
19 Ibid.
20 Ibid.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

<table>
<thead>
<tr>
<th>Time.lex</th>
<th>Spark Legal network and Consultancy Ltd</th>
</tr>
</thead>
</table>

Personal experience shows that during day-to-day use of popular Austrian websites the user is not regularly confronted with the issue of cookies. In particular the user is hardly ever asked for consent. A small non-representative test on the own computer shows that cookies are set by popular websites depending on the browser settings, without trying to obtain active consent. Whether this practice can be considered lawful depends on which one of the two opinions presented above (question 6) one follows.

Statistics, surveys, cases etc. on the Austrian situation could not be found.
9. Please describe and give references to any form of 'guidance' on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>No such guidance could be found.</td>
</tr>
<tr>
<td>b.</td>
<td>No case law could be found.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. We consider the rules to be not completely clear. As mentioned under question 6 above, it is an open question whether cookie-friendly browser settings can be regarded as user consent. In the light of opinion WP 188 of the Article 29 Data Protection Working Party we doubt that, in particular, given the fact that the average user does not actively change browser settings and the default settings concerning cookies might be cookie-friendly. It should not happen that user ignorance is interpreted as user consent. Hence, depending what interpretation finally turns out to be correct, we tend to consider them to be not appropriate to protect privacy in this context.

   b. In practice the situation concerning cookies is lacking supervision and enforcement. Enforcement decisions would also lead to a clarification regarding the question raised under (a) above.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Traffic data are defined in sec. 92 para. 3 no. 4 Telecommunications Act 2003 as “any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof”.

The wording is identical to the wording in the Directive.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Sec. 99 Telecommunications Act 2003 contains the Austrian legal framework with regard to processing of traffic data:

“§ 99. (1) Except for cases regulated in this act, traffic data must not be stored and shall be erased or made anonymous after termination of the connection. The lawfulness of the further use of traffic data transferred under para. 5 is subject to the provisions of the Criminal Procedure Code and the Security Police Act.

(2) If required for the purposes of subscriber billing, including interconnection payments, the operator of a public communication network or service shall store traffic data. The traffic data shall be erased or anonymised after the payment was made and the payment was not challenged within a period of three months. The data must not be erased, if

1. a challenge was raised in time, up to the end of the period during which the bill may be lawfully challenged.
2. the bill was not paid, up to the end of the period during which the claim for payment can be raised, or
3. proceedings on the amount of the charges are instituted, until the final decision.

These data shall be made available in full to the decision-taking body as well as to the arbitration authority (sec. 122). The amount of stored traffic data must be restricted to what is absolutely necessary.

(3) Processing of traffic data must be restricted to persons who handle billing or traffic management, fault recovery, customer enquiries, fraud detection or marketing communications services or provide value added services, or have been commissioned by these persons, and must be restricted to what is absolutely necessary.

(4) Except for cases specially regulated by law, the operator shall not process a subscriber line according to subscriber numbers called from that line beyond the purposes of billing. With the subscriber’s consent the operator may use the data for the purpose of marketing his own telecommunications services or for the provision of value added services.

(5) The processing of traffic data for the purpose of inquiries is permitted for inquiries about

1. data of a communication pursuant to sec. 134 no. 2 Criminal Procedure Code.
2. access data to courts and public prosecution authorities subject to sec. 76a para. 2 Criminal Procedure Code.
3. traffic data and master data, if the processing of traffic data is necessary in this regard, and for inquiries about location data by the police authorities which are competent pursuant to the Security Police Act subject to sec. 53 para. 3a and 3b Security Police Act. If the current position can not be identified processing of the Cell-ID of the last communication activity is permitted.
4. access data, if they have been store not longer than three months before the inquiry, by police authorities which are competent pursuant to the Security Police Act subject to sec. 53 para. 3a no. 3
Security Police Act.”

The general rule, laid down in para. 1, is, in essence, not different from the provision of art. 6 para. 1 of the Directive. Also the remainder of the provision is very similar to the Directive. The information obligation laid down in art. 6 para. 1 of the Directive is implemented as a general rule in sec. 96 para. 3 Telecommunications Act 2003. Hence, altogether, the Austrian provisions regarding traffic data follow closely the rules laid down in the Directive.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</th>
</tr>
</thead>
</table>
| See above. The general rule is that they must be “erased or made anonymous after termination of the connection”.  

(From sec. 99 para. 1 Telecommunications Act 2003: “Except for cases regulated in this act, traffic data must not be stored and shall be erased or made anonymous after termination of the connection. The lawfulness of the further use of traffic data transferred under para. 5 is subject to the provisions of the Criminal Procedure Code and the Security Police Act.”) |
<table>
<thead>
<tr>
<th>4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
</tr>
</tbody>
</table>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Yes, we consider these rules to be clear, logically consistent and appropriate to protect privacy. If anything, it is not always clear whether particular instances of data fall within the definition of the term traffic data (i.e. the definition in the Directive) or not.
### D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>Location data are defined in sec. 92 para. 3 no. 6 Telecommunications Act 2003 as “any data processed in a communications network, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The wording is virtually identical to the wording in the Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Sec. 102 Telecommunications Act 2003 contains the Austrian legal framework with regard to processing of location data:

“§ 102. (1) Irrespective of sec. 98, location data other than traffic data may be processed only if they are
1. made anonymous or
2. the users or subscribers have given their consent which may be withdrawn at any time.
(2) Even in cases where consent of the users or subscribers has been obtained for the processing of data pursuant to subsection (1), the user or subscriber must have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each transmission.
(3) Processing of location data other than traffic data in accordance with subsections (1) and (2) must be restricted to what is necessary for the purposes of providing the value added service as well as to persons acting under the authority of the provider or of the third party providing the value added service. Notwithstanding sec. 93 para. 3 the collection and processing of location data which are not related to an act of communication for the purpose of inquiries is not permitted.”

Whether the content of this provision is different from art. 9 of the Directive depends on the interpretation of art. 9 of the Directive, which is not clear regarding the following point in para. 1: Does the part “to the extent and for the duration necessary for the provision of a value added service” only belong to the part “or with the consent of the users or subscribers” or does the provision also restrict the use of anonymised location data to a value added service? Also from reading the provision in three different language versions, which are not identical in this respect, were not able to determine the correct interpretation. The text of the Austrian provision follows the latter interpretation. However, the former would seem more likely because data protection provisions generally are not applicable to anonymised data.

The provision also applies to third parties. There is no restriction with regard to who is processing the location data.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

See above. Sec. 102 para. 1 of the Telecommunications Act 2003 is worded as follows:

“Irrespective of sec. 98, location data other than traffic data may be processed only if they are
1. made anonymous or
2. the users or subscribers have given their consent which may be withdrawn at any time.”
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. No such guidance or decisions could be found.

   b. No such decisions could be found.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The rules regarding location data are not fully clear. This goes back to the wording of art. 9 para. 1 of the Directive, as described above (question 2).

[Remark: We would be very interested in literature or case law that clarifies the interpretation of art. 9 para. 1 of the Directive in this respect.]

Similar to the case of traffic data mentioned above, it is not always clear whether certain instances of data fall within the definition of location data.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. In sec. 101 of the Telecommunications Act 1997 a prohibition for advertising via phone, fax or e-mail without prior consent from the user existed already prior to the ePrivacy Directive. The Austrian legislator therefore did not change the substance of this provision when he transposed article 13 of the ePrivacy Directive in sec. 107 of the new Telecommunications Act 2003, which is, however, a more detailed provision than its predecessor sec. 101 of the Telecommunications Act 1997.

   The Austrian implementation is an opt-in solution with regard to all means of communication article 13 deals with. Therefore the Austrian implementation makes no difference between communication systems without human intervention and other communication systems.

   Sec. 107 para. 1 deals with unsolicited phone calls and faxes. Para. 1a prohibits the non-disclosure or disguise of the caller’s phone number with regard to calls for advertising purposes. Para. 2 prohibits unsolicited electronic messages and para. 3 lays down the respective exceptions. In addition para. 5 prohibits electronic messages for purposes of direct marketing in any case, when the identity of the sender is disguised or concealed, when the information provisions of sec. 6 para. 1 of the E-Commerce Act are breached, when the recipient is asked to visit website that breach this provision or when there is no valid address to which the recipient can send a request to stop sending any such messages.

   b. The Austrian provisions are in line with the Directive, including the exceptions laid down therein.

   Sec. 107 para. 2 goes beyond the requirements of the Directive. It not only prohibits e-mail and text messages without prior consent of the user for advertising purposes but also if the message is sent to more than 50 recipients regardless of its purpose.

   Sec. 107 para. 3 no. 4 lays down a special possibility for users to initially refuse the receipt of electronic messages for direct marketing purposes (article 13 para. 2 of the Directive): The user can add his address to a list (“robinson list”) which is maintained by RTR GmbH under sec. 7 para. 2 of the E-Commerce Act.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

See partly already above. Sec. 107 para. 2 and 3 lay down the relevant rules as follows:

“(2) The sending of electronic mail - including SMS messages - to consumers as defined in § 1 (1) item 2 Consumer Protection Act [Konsumentenschutzgesetz] without the recipient’s prior consent shall not be permitted if
   1. the sending takes place for purposes of direct marketing or
   2. is addressed to more than 50 recipients.

(3) Prior consent to electronic mail pursuant to subsection (2) shall not be required if
   1. the sender has received the contact details for the communication in the context of a sale or a service to his customers and
   2. the communication is transmitted for the purpose of direct marketing of his own similar products or services and
   3. the customer clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and
   4. the customer has not initially objected to the communication, in particular by entry into the list mentioned in sec. 7 para. 2 of the E-Commerce Act.”
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

See already above. Sec. 107 para. 3 lays down the following exception:

“(3) Prior consent to electronic mail pursuant to subsection (2) shall not be required if
   1. the sender has received the contact details for the communication in the context of a sale or a service to his customers and
   2. the communication is transmitted for the purpose of direct marketing of his own similar products or services and
   3. the customer clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and
   4. the customer has not initially objected to the communication, in particular by entry into the list mentioned in sec. 7 para. 2 of the E-Commerce Act.”
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Yes, it distinguishes between calls, including facsimile transmissions (sec. 107 para. 1 Telecommunications Act 2014) and electronic mail including short messages (sec. 107 para. 2 and 3). Regarding the latter, the following special provisions apply, as already mentioned above:

Sec. 107 para. 2 goes beyond the requirements of the Directive. It not only prohibits e-mail and text messages without prior consent of the user for advertising purposes but also if the message is sent to more than 50 recipients regardless of its purpose.

Sec. 107 para. 3 no. 4 lays down a special possibility for users to initially refuse the receipt of electronic messages for direct marketing purposes (article 13 para. 2 of the Directive): The user can add his address to a list (“robinson list”) which is maintained by RTR GmbH under sec. 7 para. 2 of the E-Commerce Act.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b. There is a number of cases in this context.</td>
</tr>
<tr>
<td>In <strong>VwGH 19. 12. 2013, 2012/03/0052</strong> the Austrian Administrative Court dismissed a complaint against the rule laid down in sec. 107 para. 6 Telecommunications Act 2003 that if administrative offences under sec. 107 Telecommunications Act 2014 have not been committed in Austria shall be considered as having been committed in the place where the unsolicited communication reaches the subscriber.</td>
</tr>
<tr>
<td>In <strong>VwGH 24.05.2012, 2010/03/0056</strong> the Austrian Administrative Court elaborated on how the rule of sec. 107 para. 3 no. 3 Telecommunications Act 2003 that “the customer clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected” must be interpreted in the context of text messages.</td>
</tr>
<tr>
<td>Specific cases on particular providers or sectors could not be found.</td>
</tr>
</tbody>
</table>

---


6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| In practice the rules on unsolicited communications are very ineffective. This is a notorious problem not specific to Austria. The main reason for this seems to be not the rules themselves but the difficulty to execute them in an international context. |
COUNTRY REPORT
BELGIUM

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Prof. Jos Dumortier, time.lex

Date: 30 June 2014
Contents

Part 1: Management summary......................................................................................................................... 3
Part 2: Answers to the questionnaire.................................................................................................................. 4
Part 1: Management summary

Management Summary
The transposition of the ePrivacy Directive into Belgian law can be summarized as follows:

- The provisions with regard to the scope of the Directive have been transposed taking into account the federal structure of the Belgian State. According to this structure regulatory competences in the field of broadcasting have been transferred to the three “Communities” (Flanders, French Community, German Community). “Broadcasting” includes the regulation of electronic communications networks and services used for this purpose. As a consequence of this division of competences, Belgium has maintained the distinction between “broadcasting” (competence of the Communities) and “other electronic communications services” (federal competence). The ePrivacy Directive has therefore not only been transposed at the federal level but also at the level of the Communities.

- At the federal level Belgium transposed most of the provisions in the federal Electronic Communications Law of 2005, of which the scope is largely determined by the term “operator”. Nearly all the provisions of the Electronic Communications Law are addressed to “operators”. Unfortunately this term is not clearly defined in the Law and therefore the Belgian NRA is currently drafting a guideline for the interpretation of this term in practice. At the moment of writing this report this guideline is still “under construction”. Some of the provisions transposing the ePrivacy Directive have a different scope and are not only applicable to providers of public electronic communications networks and services. This is in particular the case for the provisions with regard to cookies and similar techniques, which are applicable to the users of public electronic communications networks and services, irrespective of whether the origin of the cookies.

- Art. 5.3 of the Directive (about “cookies” etc.) has been more or less literally transposed into Belgian law. As a consequence it generates multiple questions with regard to its application in practice. The Belgian Privacy Commission has therefore launched a public consultation on a proposed recommendation in order to introduce practical guidelines in this domain. The current version of the recommendation is largely based on the documents of the Art. 29 WP.

- Belgium has developed more precise rules on traffic and location data than those contained in the ePrivacy Directive, making use of the margin left to the Member States in this respect. Whether or not the rules are applied in practice, is not really monitored and left to the sole responsibility of the “operators”. As far as the processing of location data is concerned, the Belgian Privacy Commission issued an opinion on automated vehicle location via GPS, carried out in the context of an employment relationship;

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into Belgian law in the context of the transposition of the eCommerce Directive and they are consequently applicable to information society service providers established in Belgium. The application of these provisions in Belgium is supervised by the Federal Public Service for Economy (in the framework of consumer protection) and – additionally – by the Privacy Commission.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject

- Directive 2002/58/EC has been (partly) transposed into Belgian federal legislation by the Law of 13 June 2005 regarding Electronic Communications (hereafter “the “Electronic Communications Law”) and further within the Region of Flanders, where Directive 2002/58/EC has been (partly) transposed by the Media Decree of 27 March 2009, and (implicitly) by corresponding decrees of the French and German Communities.
- The provisions with regard to unsolicited communications were earlier integrated in the Law of 11 March 2003 transposing the Electronic Commerce Directive.
- Particular provisions with regard to telemarketing have been inserted in the Law on Market Practices and Consumer Protection.
- Following the 2009 amendments of the European Regulatory Framework for Electronic Communications, the Belgian legislator amended its legal framework by a Law of 21 June 2012 introducing various provisions regarding electronic communications.
- Finally, the provisions of the Electronic Commerce Law and of the Market Practices and Consumer Protection Law have recently (December 2013) been integrated in the Belgian Code of Economic Law.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed in Belgian law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
### Art. 6 (Traffic data)
Law of 13 June 2005 regarding Electronic Communications, art. 122
[Link](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2005061332&table_name=wet)

### Art. 9 (Other location data)
Law of 13 June 2005 regarding Electronic Communications, art. 123
[Link](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2005061332&table_name=wet)

### Art. 13 (Unsolicited communications)
Code of Economic Law, art. XII-13
[Link](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2013022819&table_name=wet)

---

**2. Which enforcement authority(ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)**

For each authority please provide in the table below:

- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL linking to its website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it is supervising</th>
<th>the URL linking to its website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgian Institute for Post and Telecommunications</td>
<td>BIPT</td>
<td>All provisions transposed in the Electronic Communications Law</td>
<td><a href="http://www.bipt.be">www.bipt.be</a></td>
</tr>
<tr>
<td>Ombudsman for Telecommunications</td>
<td>Ombudsman for Telecommunications</td>
<td>All provisions transposed in the Electronic Communications Law</td>
<td><a href="http://www.ombudstelecom.be">www.ombudstelecom.be</a></td>
</tr>
<tr>
<td>Regional supervisory authorities for the media sector</td>
<td>VRM / CSA / Government of the German-speaking Community</td>
<td>All provisions transposed in the decrees of the Communities</td>
<td><a href="http://www.vlaamseregulatormedia.be">www.vlaamseregulatormedia.be</a>; <a href="http://www.csa.be">www.csa.be</a>; <a href="http://www.dg.be">www.dg.be</a></td>
</tr>
<tr>
<td>Federal Public Service for Economy</td>
<td>FPS Economy</td>
<td>Provisions with regard to unsolicited communications</td>
<td><a href="http://www.economie.fgov.be">www.economie.fgov.be</a></td>
</tr>
<tr>
<td>Privacy Commission</td>
<td>Privacy Commission</td>
<td>All provisions having an impact on privacy or data protection</td>
<td><a href="http://www.privacycommission.be">www.privacycommission.be</a></td>
</tr>
</tbody>
</table>
Explanation:

- The Belgian Institute for Post and Telecommunications (www.bipt.be) is, as the federal NRA for the electronic communications sector, the supervisory authority for the provisions transposing the ePrivacy Directive which have been inserted into the Belgian Electronic Communications Law.

- Subscribers and users of electronic communications services and networks can also address complaints to the Ombudsman for Telecommunications (www.ombudstelecom.be).

- Complaints with regard to electronic communications networks used for audiovisual services have to be addressed to the regional supervisory authorities for the media sector (in Flanders: www.vlaamseregulatormedia.be; for the French Community: www.csa.be).

- The provisions with regard to unsolicited direct marketing communications, transposed in the Electronic Commerce Law and recently integrated into the Code of Economic Law, are supervised by the Federal Public Service for Economy (www.economie.fgov.be).

- As far as the provisions transposing the ePrivacy Directive are related to privacy and personal data protection, supervision is also exercised by the Belgian Privacy Commission (www.privacycommission.be).
### 3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Article 2, 3° of the Electronic Communication Law defines **electronic communication networks** as “transmission systems and, where applicable, switching or routing equipment and other resources, including passive network elements which enable the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, insofar as they are used for the purpose of transmitting signals other than signals for radio and television broadcasting”. Networks used only to transmit broadcasting signals are therefore excluded from this definition.

The most important difference between the Belgian definitions of “electronic communications network” and the definition of this concept in the ePrivacy Directive is the exclusion of networks which are exclusively used to transmit broadcasting signals. The reason for this exclusion is that the competence to regulate these networks is in the hands of the legislators of the Communities.

The Law distinguishes between “public” and “non-public” networks. Some of its provisions apply only to public networks. The following is regarded as a “public” network: “an electronic communication network that is used entirely or mainly to make electronic communications services accessible to the public to support the transfer of information between network connection points” (art. 2, 10° of the Law).

Article 2, 5° contains a definition of an **“electronic communication service”**: “a service usually for payment, which entirely or principally consists in the transmission, including switching and routing operations, of signals via electronic communication networks, to the exclusion of:
(a) services that provide or control content that is transmitted through electronic networks and services
(b) services of the information society as described in Article 2 of the Law of 11 March 2003 regarding certain legal aspects of information society services, which do not.
The most important difference between the Belgian definitions of “electronic communications network” and the definition of this concept in the ePrivacy Directive is the exclusion of networks which are exclusively used to transmit broadcasting signals. The reason for this exclusion is that the competence to regulate these networks is in the hands of the legislators of the Communities
(c) radio and television broadcasting”.

Article 2 of the Electronic Communication Law further defines the concept of **“operator”**. This definition is important because many provisions of the Law are explicitly addressed to “operators”. Article 2, 11° refers to Article 9 and one can conclude from this latter Article that the term “operator” relates to “providing or re-selling in one’s own name or for one’s own account electronic communication services or networks”.

Again, one has to keep in mind that the Belgian federal legislator transposed the provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications in the framework of the eCommerce legislation. This legislation is applicable to providers of information society services established in Belgium.

Finally one should also keep in mind that the data or activities addressed by the provisions of the ePrivacy Directive involve the processing of personal data. As such the scope of these provisions is
also determined by the (scope of the) Belgian data protection law and in particular by the provision transposing Art. 4 of Directive 95/46/EC.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

The answer to this question entirely depends on whether or not these services “entirely or principally consists in the transmission, including switching and routing operations, of signals via electronic communication networks”.

The practical application can easily lead to disputes because it requires weighing up what is regarded as a principal matter and what is regarded as a secondary matter in a particular service provision package. For a service to be regarded as an “electronic communication service” in the sense of the federal legislation, it must consist entirely or – at least – principally of transmitting signals. (This matter came under discussion in the Yahoo case, where one of the questions was whether a “provider of an electronic communication service” mentioned in Article 46bis of the Code of Criminal Procedure should be interpreted in line with the definition of Article 2, 5° of the Electronic Communications Law. The Court of Cassation answered this question negatively but this judgment is not relevant for the question under consideration. See [Cass.18 januari 2011](#); P. DE HERT en M. BOULET, “De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten”, Computerr.2012, p. 324-330)

If the emphasis of a service provided is on content, this service does not fall under the definition of “electronic communications service” and, therefore also not under the scope of the law. In practice services such as Skype, Gmail, etc. will today be considered as information society services because the part of the service that is related to content, is dominant and more important than the mere transmission of signals. Furthermore, broadcasting services (and services provided by the information society, which are more content-oriented than transport-oriented) are – naturally – also excluded.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

Because the ePrivacy Directive has been transposed into Belgian law partly by the Electronic Communications Law, partly by legal provisions which have been integrated into the Code of Economic Law and partly by a series of provisions in other Belgian Codes, the answer to the question about the territorial scope of the provisions is not obvious.

In principle the provisions of the Belgian Electronic Communications Law are applicable to “operators”. Operators are providers of electronic communications networks and electronic communications services under the obligation to notify their activities to the BIPT.

According to the communication of the BIPT published on 23 May 2014, the BIPT is only competent in relation to network providers established - wholly or partly - in Belgium for services provided on the Belgian territory. Operators established in Belgium who don’t provide services on the Belgian territory are not covered by the notification duty and therefore do not fall under the definition of “operator”. In practice this would mean that the Belgian legal provisions regarding, for example, the processing of traffic data or location data are applicable to electronic communications service providers not established in Belgium but providing services on the Belgian territory.

The problem is, however, that these operators also have to be considered as “controllers” under the Belgian data protection legislation and the European Directive 95/46/EC. Under this regime the Belgian data protection rules are applicable to:

1° to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established on Belgian territory or in a place where Belgian law applies by virtue of international public law;

2° to the processing of personal data by a controller who is not permanently established on European Community territory, if the means used, which can be automatic or other means located on Belgian territory, are not the same as the means used for processing personal data only for the purposes of transit of personal data through Belgian territory. “(Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data)

The Code of Economic Law is addressed to service providers who are established on the Belgian territory. Article XII.3 provides that the provision of information society services by a provider established on the Belgian territory is subject to the rules applicable in Belgium. This provision transposes, in other words, the “rule of origin” established by the European eCommerce Directive. Because the provisions of the ePrivacy Directive regarding unsolicited commercial communications have been transposed by the Belgian legislator in the framework of the eCommerce legislation, the Belgian legal provisions in this domain, logically, only apply to advertisers established in Belgium.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law
a. In order to clarify the term “operator”, the Belgian federal NRA for the electronic communications sector – the Belgian Institute for Post and Telecommunications (BIPT) - recently organised a public consultation and, subsequently, published a draft communication on 23 May 2014.

The purpose of this communication is to explain the notion of "operator" as well as the hypotheses in which a person will have to submit a notification to BIPT as an operator. The communication is not exhaustive and will evolve according to the specific cases BIPT will be confronted with, as well as feedback from stakeholders, and the need to study certain notions in depth.

This does not exclude the fact that in some specific cases BIPT may still adopt ad hoc decisions. See further http://www.bipt.be/public/files/en/21295/EN_Consultation-note-operateurs-UK.pdf for an English version of the public communication.

b. Besides the public communication of the BIPT mentioned before, we are not aware of any administrative decisions or court cases in Belgium with regard to the interpretation of the term “operator” in the context of the federal Electronic Communications Law.
### 7. What is your individual view of:

| a. | the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country? |
| b. | possible improvements of the effectiveness of this legal framework. |

**a.** The distinction between providers of electronic communications services and providers of information society services is, in the context of the application of provisions with regard to privacy and personal data protection, entirely irrelevant. More specifically in the Belgian context, the division of competences between the federal State and the Communities to regulate electronic communications networks leads to additional complexity.

**b.** Given that the distinction between providers of electronic communications services and providers of information society services is entirely irrelevant in the context of the application of provisions with regard to privacy and personal data protection, this aspect of the ePrivacy Directive should better be revised.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

| a. Article 124 of the Law on Electronic Communication provides that “it is forbidden to do the following, if one has not obtained the consent of all the other persons directly or indirectly involved:

1° take cognisance with intent of the existence of information of any nature which is sent electronically and which is not personally intended for the person taking cognisance;
2° identify with intent persons who are involved in the transmission of the information and its contents;
3° take cognisance with intent of data relating to electronic communication and relating to another person;
4° change, delete, disclosing, store or make any use of the information, identification or data that were obtained with or without intent.”

Article 124 consequently forbids taking cognisance of the existence of electronic communication. This must involve communication between two or more persons or between a person and an information system, where an outsider takes cognisance of the existence of communication not intended for him. Communication in the sense of this provision includes visiting a website or watching a programme or a film on television.
Intent is required for the first three crimes of Article 124. Therefore, if the existence of communication that is not intended for one comes to one’s knowledge accidentally or unintentionally, this is not punished. That is the case, for example, when one receives messages actually addressed to someone else due to a technical fault or by mistake. However, if one were to subsequently disseminate, store or use such messages, this would indeed be punishable pursuant to Article 124, 4°.

The actions outlined in Article 124 are not punishable if the person concerned had the consent of all other persons who were directly or indirectly involved in the communication. The consent of all persons concerned must be obtained. The penalty – a monetary fine of between EUR 50 and EUR 50,000 – upon contravention of Article 124 is included in Article 145 § 1 of the Electronic Communications Law.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

This provision has been transposed in Article 128 of the Electronic Communications Law.

Article 128 provides that “the registration of electronic communication and the relative traffic data performed in the legal business traffic as proof of a commercial transaction or other business communication” is allowed. However, this is subject to the condition that all parties involved in the communication are informed, before registration, that the communication is registered, what the exact purposes for registration are and for how long it will be stored. The said data must be deleted no later than at the end of the period within which the transaction can be contested at law.”
Furthermore, taking cognisance of and registering electronic communication and the traffic data, the sole purpose of which is to check the quality of the service provision in call centres, are allowed, on condition that the persons working in the call centre are informed in advance of the fact that cognisance may be taken of the electronic communication and that it may be registered, as well as of the exact purpose of the registration and for how long the registered communication and data will be stored. These data may not be stored for longer than one month.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

<table>
<thead>
<tr>
<th>Article 125, § 1 of the Law on Electronic Communication contains six exceptions to the confidentiality of communication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“The provisions of Article 124 of this Law and of Articles 259bis and 314bis of the Criminal Code do not apply:</td>
</tr>
<tr>
<td>1. when the Law allows or requires that the intended actions be performed;</td>
</tr>
<tr>
<td>2. when the intended actions are performed with the sole purposes of checking proper operation and securing the performance of an electronic communications service;</td>
</tr>
<tr>
<td>3. when actions are performed to enable the intervention of aid and emergency services in response to their targeted requests for aid;</td>
</tr>
<tr>
<td>4. when the actions are performed by the BIPT (Belgian Institute for Postal Services and Telecommunication) within the context of its general mission relating to surveillance and supervision;</td>
</tr>
<tr>
<td>5. when the actions are performed by the ombudsman for telecommunication, by the officials who are authorised by the Minister of Economy (Economic Inspection) or by the Ethics Commission for telecommunication or its Secretariat, or at the request of these institutions, within the context of their legal research assignments, and such actions do not involve tapping communication;</td>
</tr>
<tr>
<td>6. when the actions are performed for the sole purpose of providing the end user with services consisting of preventing the receipt of inappropriate electronic communication, on condition that the end user’s necessary consent has been obtained.”</td>
</tr>
</tbody>
</table>

In the case of the first exception, the first thing that springs to mind is the legal provisions that allow the public prosecutor’s office to break the confidentiality of telecommunications for the purposes of a judicial or preliminary investigation. These provisions are part of the Belgian Code of Criminal Procedure. They are not further explained in this report. The first exception is also the legal basis for monitoring electronic communications of employees at the workplace or during the execution of their employment contract. (This is, at least, the opinion of the Privacy Commission published in a legal report of 2011, p. 13; the procedure to be followed by employers for the monitoring of electronic communications of employees has been further implemented in a Collective Bargaining Agreement nr. 81 of 26 April 2002.)
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Belgian legislation doesn’t explicitly address “automated breaches of confidentiality without human intervention”. In principle such breaches of confidentiality will be considered as an infringement of Article 124 of the Electronic Communications Law if they are outside the scope of the exceptions provided in Article 125.

b. Long before the ePrivacy Directive was introduced the Belgian legislator introduced provisions in the Criminal Code incriminating interception of the content of private communications and telecommunications. Articles 259bis and 314bis have been inserted into the Criminal Code by the Law of 30 June 1994 to protect privacy against wiretapping, and taking cognisance of and opening private communications and telecommunications (Law of 30 June 1994 to protect privacy against wire tapping, and taking cognisance of and opening private communications and telecommunications). The two provisions relate to identical crimes (see below) but Article 259bis applies if the crime is committed by “any public official or civil servant, holder or agent of public authority”, whereas Article 314bis is applied if the same crimes are committed by persons other than those referred to in Article 259bis.

The first crime that was made punishable by both articles is the “wilful tapping, or having tapped, with the aid of any device, of any private communication or telecommunication in which he does not participate, during its transmission, taking due note of it or having due note take of it, recording it or having it recorded, without the consent of any of the participants to such communication or telecommunication”. The crime is widely defined, even though a few conditions must be met to make it punishable.

The crime refers not only to telecommunications but also to private communication in general. “Telecommunications” is understood in the broad sense and therefore encompasses not only telephony but also telex, fax, mobile phone, online banking, electronic mail, etc. The network or end device used for this is irrelevant. Communication consists of “any expression of language, either oral or not, direct or from a distance, regardless of the number of persons involved”. (Parl. Doc. Senate, 1992-1993, nr. 843-1, p. 3.)
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

<table>
<thead>
<tr>
<th>a. As regards the use of “cookies” and other techniques whereby, especially through the internet, it is possible to get remote access to the user’s end equipment and/or to store data on this equipment, Article 129 of the Electronic Communication Law provides the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Storing information or obtaining access to information that is already stored in the end equipment of a subscriber or user is only allowed on the condition that:</td>
</tr>
<tr>
<td>1° in accordance with the conditions provided in the Law of 8 December 1992 on the Protection of Privacy regarding the Processing of Personal Data, the subscriber or user concerned receives clear and precise information on the purposes of the processing and on his rights by virtue of the Law of 8 December 1992;</td>
</tr>
<tr>
<td>2° the subscriber or end user has given his consent after he has been informed in accordance with the provisions in 1°.</td>
</tr>
<tr>
<td>The first paragraph does not apply to the technical storage of information or the access to information saved in the end equipment of a subscriber or an end user, the sole purposes of which are to send communication through the electronic communications network or to provide a service explicitly requested by the subscriber or end user when it is strictly essential to do so.</td>
</tr>
<tr>
<td>The consent in the sense of the first paragraph or the application of the second paragraph does not release the controller from the obligations of the Law of 8 December 1992 on the Protection of Privacy regarding the Processing of Personal Data, which are not imposed in this Article.</td>
</tr>
<tr>
<td>The controller affords the subscribers or end users the opportunity of simply withdrawing the consent given, free of charge.”</td>
</tr>
<tr>
<td>Article 129 of the Electronic Communications Law is not specifically addressed to “operators” but aims at protecting all subscribers or users of public electronic communications networks. This interpretation has also been confirmed by the Belgian Privacy Commission.</td>
</tr>
<tr>
<td>b. The provision quoted above doesn’t distinguish between types of cookies or between categories of end equipment.</td>
</tr>
</tbody>
</table>
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applies in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Article 129 of the Belgian Electronic Communications Law doesn’t contain an answer to these questions and there aren’t any court decisions yet interpreting this provision and applying it to concrete situations. In April 2014 the Privacy Commission has submitted to public consultation a draft recommendation (62 pages) with practical guidelines for the application of Art. 129. The public consultation closes on 31 July 2014.
How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

According to an opinion issued by the Privacy Commission, the cookies that are exempt from the obligation of consent are certain “first party” cookies and, in particular, those of the “user input session cookies” type, i.e., cookies that are entered personally by the user and which remember language settings and personal preferences in a webshop, such as customer identity and virtual shopping trolley (Privacy Commission, Advice 10/2012 of 21 March 2012).

On the other hand, it is, according to the Privacy Commission, clear that certain cookies do not fall under the exemption to the obligation to inform. Reference is made in the literature to the most intrusive and newest forms of cookies by way of various names which are sometimes used haphazardly, such as “persistent cookies”, “flash cookies”, “supercookies” and “evercookies” (The Privacy Commission refers to the ENISA “Bittersweet Cookies” Study of 2 February 2011). The properties of such cookies have far-reaching effects. These are cookies that have clearly not been requested by the user, which sometimes stay on the end equipment even after the action has been deleted, and are used for various or indefinite purposes. This often concerns “third-party” cookies, for which those responsible communicate very little or not at all and which require specific expertise and software to remove them.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The first guidelines issued by the Privacy Commission in 2012 did not lead to legal certainty in this area. This is the reason why the Privacy Commission recently started a public consultation on this issue. Meanwhile the practical implementation of the new rules is still very diverse.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

a. The Privacy Commission recently (April 2014) launched a public consultation on a draft Recommendation on this issue (Draft recommendation regarding the use of cookies, submitted to public consultation, (CO-A-2012-004)). The draft Recommendation – a document of 62 pages - builds further on the Article 29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies (Article 29 Data Protection Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, adopted on 2 October 2013). It contains numerous practical guidelines on how to apply the rules with regard to the use of cookies on various devices and in various circumstances. The public consultation will close on 31 July 2014. It is expected that the Privacy Commission, after having processed all the input, will come up with a final Recommendation at the end of this year.

d. Not available
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. Without additional guidance of the Privacy Commission the provisions of the Belgian legislation transposing Art. 5.3 of the ePrivacy Directive are too vague to allow a consistent application in practice by service providers. Moreover the scope of the provisions is unclear. From a strictly legal point of view the provisions are only applicable to “operators” under the scope of the Electronic Communications Law.

   b. In practice, website owners (information society service providers) start to implement the rules and inform users about the possibility to accept or refuse cookies in the form of a one-time banner that can easily be “clicked away”.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Article 2,6° of the Electronic Communications Law defines traffic data as “data processed for the transmission of the communications over an electronic communications network or for the invoicing of such communications.”

Art. 2, 8° defines “service relating to traffic” as follows: “service requiring a particular processing of traffic data beyond what is strictly necessary for the transmission of the invoicing of the communications”.

2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Article 122 of the Electronic Communications Law contains the Belgian legal framework with regard to processing of traffic data.

"§ 1. The operators delete the traffic data with regard to subscribers and end users from their traffic data or make these data anonymous, as soon as they are no longer needed for the transmission of the communication.

The application of the first alinea doesn’t prevent the respect of duties established by law or regulation relating to the collaboration with:
1° authorities competent for the investigation and prosecution of criminal facts;
2° the ombuds service for telecommunications in order to discover the identity of any person who made malicious use of a telecommunications network or service;
3° the intelligence and security services in the framework of the law of 30 November 1998 regulating the intelligence and security services.

§ 2. By way of derogation from § 1 and with the only purpose of invoicing subscribers or interconnection payments the operators process and store the following data:
1° the identification of the calling line;
2° the address of the subscriber, the location of the connection and the type of terminal equipment;
3° the total amount of of units for the accounting period;
4° the identification of the called line;
5° the type, start time and duration of the call or the amount of data transmitted;
6° the date of the connection or of the service.
7° other data relating to payments, such as advance payment, periodic payment, disconnection and reminders.

Notwithstanding the application of the law of 8 December 1992 protecting personal life with regard to the processing of personal data, the operator informs the subscriber or, if applicable, the user to which the data relate, of:
1° the types of traffic data processed;
2° the precise purposes of the processing;
3° the duration of the processing.

The processing of the data listed in the first alinea is only permitted till the end of the period of possible contestation of the invoice or till the end of the period during which the payment can be enforced by judicial means.

§ 3. By way of derogation from § 1 and with the only purpose to ensure the marketing of electronic communications services provided by themselves, the establishment of the user profile or to provide services related to traffic or location data, the operators can process the data mentioned under § 1 under the following conditions:

1° The operator informs the subscriber or, if applicable, the end user to whom the data relate, prior to the collection of the consent, about:
a) the type of traffic data processed;
b) the precise purposes of the processing.
c) the duration of the processing.

2° The subscriber or, if applicable, the end user has given his consent prior to the start of the processing.

Consent in the meaning of this provision is defined as the free and specific expression of will based on information, whereby the person concerned or his representative accepts that traffic data
relating to him may be processed.

3° The operator concerned offers to his subscribers or end users without any cost the possibility to withdraw the consent in a simple manner.

4° The processing of the data concerned remain limited to the actions and the duration needed for the provision of the services related to traffic or location data, the establishment of the user profile or the marketing action concerned.

These conditions have to be combined with those required by the application of the Law of 8 December 1992 protecting private life with regard to the processing of personal data.

§ 4. By derogation of § 1 the data can be processed to detect potential fraud. In case of a criminal fact the data will be communicated to the competent authorities.

§ 5. The data mentioned in this article should only be processed by persons who, on behalf of the operator, are in charge of invoicing, traffic management, the processing of requests of clients for information, the detection of fraud, the marketing of electronic communications services provided by themselves or the provision of services related to traffic or location data. The processing is limited to what is strictly necessary for performing these activities.

§ 6. The BIPT, the Belgian Competition Authority, the judicial authorities and the Council of State in the framework of their competences can obtain relevant traffic and accounting data for the purpose of solving disputes, for example with regard to interconnection or invoicing."
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Article 122, § 1 of the Electronic Communications Law is formulated as follows:

“§ 1. The operators delete the traffic data with regard to subscribers and end users from their traffic data or make these data anonymous, as soon as they are no longer needed for the transmission of the communication.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

The Belgian Privacy Commission has formulated some remarks on Art. 122 in its advice on the draft Electronic Communications Law (the Privacy Commission can issue opinions on all matters – e.g. on all legislative initiatives - which have potential impact on privacy and data protection rights of individuals). In the opinion on the draft Electronic Communications Law the Commission mainly criticized a) the reduced rights for individuals when the subscriber is a legal person (e.g. the employer), and b) the exception for the investigation of “fraud”, the text of the ePrivacy Directive is much narrower in this respect (http://www.privacycommission.be/sites/privacycommission/files/documents/advies_08_2004_0.pdf)
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions of Article 122 of the Electronic Communications Law are not sufficient for the protection of subscribers and users because their scope is limited to “operators”. The processing of traffic data by network and service providers, other than “operators” as defined in the Electronic Communications Law is only protected via the general data protection legislation (in particular the proportionality principle).
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>The term “location data” is defined in Article 2, 7° of the Electronic Communications Law, as follows: “data processed in an electronic communications network, under which satellite networks, fixed (circuit and packet switched, including the internet) and mobile terrestrial networks, electricity power networks, by which the geographical position of an end user of a publicly available electronic communications service is rendered”.</th>
</tr>
</thead>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Article 123 of the Electronic Communications Law transposes the provisions of the ePrivacy Directive with regard to location data.

“§ 1. Notwithstanding the application of the Law of 8 December 1992 protecting private life with regard to the processing of personal data the operators of mobile networks should process location data relating to a subscriber or an end user only when they are made anonymous or if the processing fits in the framework of the provision of a service related to traffic or location data.

§ 2. The processing in the framework of a service based on traffic or location data is submitted to the following conditions:

1° The operator informs the subscriber or, if applicable, the end user to whom the data relate, prior to the collection of the consent, about:
   a) the type of location data processed;
   b) the precise purposes of the processing.
   c) the duration of the processing.
   d) the possible third person to which the data will be transmitted;
   e) the possibility to, definitely or temporarily, withdraw the consent at any time.

2° The subscriber or, if applicable, the end user has given his consent prior to the start of the processing.

Consent in the meaning of this provision is defined as the free and specific expression of will based on information, whereby the person concerned or his representative accepts that location data relating to him may be processed.

3° The processing of the data concerned remains limited to the actions and the duration needed for the provision of the services related to traffic or location data, the establishment of the user profile or the marketing action concerned.

4° The operator concerned offers to his subscribers or end users without any cost the possibility to definitely or temporarily withdraw the consent in a simple manner.

§ 4. The data mentioned in this article should only be processed by persons who are employed on behalf of the operator or the third person who provides the service based on traffic or location data. The processing is limited to what is strictly necessary to provide the service based on traffic or location data, are in charge of processing

§ 5. In case of an emergency call to the call centres of the emergency services providing assistance on the spot and for the purpose of handling the emergency request, the operators, insofar as this is technically possible, switch off the temporary refusal or the absence of consent of the subscriber or end user per separate calling line. This operation is for free.

Some additional practical aspects related to the provision of location services are further implemented in the Ethical Code for Telecommunications (Royal Decree of 9 February 2011 establishing the Ethical Code for Telecommunications). These rules relate, for example, to the communication between the operator and the provider of the location based service about the
consent or the withdrawal of consent by the subscriber or the end user, the procedure for unsubscribing a location based service, the duration of storage of user data with regard to location based service, advertising of location based services, etc.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>Table 3. Legal Requirements for Anonymising or Deleting Location Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 123 of the Electronic Communications Law is worded as follows: “§ 1. Notwithstanding the application of the Law of 8 December 1992 protecting private life with regard to the processing of personal data the operators of mobile networks should process location data relating to a subscriber or an end user only when they are made anonymous or if the processing fits in the framework of the provision of a service related to traffic or location data.”</td>
</tr>
</tbody>
</table>
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. The Privacy Commission published a recommendation on “automated vehicle location” via GPS but had to conclude that such location data escapes from the scope of Article 123 of the Electronic Communications Law because the data are not being processed by “operators” ([http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_03_2013.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_03_2013.pdf)).

   b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

Article 123 of the Electronic Communications Law doesn’t sufficiently protect individuals against illegitimate processing of location data because the scope of the Article is limited on “operators”.
E. Unsolicited commercial communications

<table>
<thead>
<tr>
<th>1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the scope and substance of your national implementation</td>
</tr>
<tr>
<td>b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.</td>
</tr>
</tbody>
</table>

a. The Belgian legislator transposed the provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications in the Law of 2003 on certain aspects regarding information society services (the “eCommerce Law”, Law of 11 March 2003 regarding particular legal aspects of the information society services, abrogated by the Law of 13 December 2013 inserting Book XII “Law of the digital economy” in the Code of Economic Law). However a prohibition for advertising via e-mail, fax and automatic calling systems existed already in the Belgian legislation on commercial practices and consumer protection before that date. For the transposition of Art. 13 and following of the ePrivacy Directive, the rules with regard to advertising via e-mail have been transferred to the eCommerce Law and were completely redrafted to be in line with the ePrivacy Directive. The rules with regard to advertising via fax and automatic calling systems remained in the Law on commercial practices and consumer protection. Very recently both the eCommerce Law and the Law on commercial practices and consumer protection have been inserted in the new Belgian “Code of Economic Law”.

As a result the provisions with regard to unsolicited direct marketing communications (transposing the corresponding provisions of the ePrivacy Directive) are today included in Book XII of the Code of Economic Law. Book XII contains the provisions of the former Law on Electronic Commerce.

b. Article XII.13, § 1 provides that the use of electronic mail for “advertising” is forbidden without the prior, free, specific and informed consent of the addressee. Besides the use of the term “advertising” (publicité in French, reclame in Dutch) instead of “direct marketing” the provisions on this topic are entirely in line with those of the ePrivacy Directive.

Besides and in addition to the rules of the ePrivacy Directive with regard to unsolicited communications, the Belgian legislation contains an obligation for electronic communications service providers to provide spam filtering. Article 114, § 4 of the Electronic Communications Law imposes on providers of electronic communications networks and electronic communications services the obligation to provide their subscribers, free of charge and considering the state of the art, appropriately secure services that enable the end users to prevent unwanted electronic communication in any form.

Finally, also in addition to the rules of the ePrivacy Directive the Belgian legislator has recently (in 2012) introduced detailed provisions with regard to telemarketing (use of telephone numbers for direct marketing calls).
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Requirements for the lawful sending of unsolicited messages other than via e-mail can be found in the legislation on market practices and consumer protection included in Book VI of the Belgian Code of Economic Law. The first paragraph of Article VI.110 of this Code contains a prohibition on the use of automated call systems without human intervention (automatic calls) and on faxes for personally addressed advertising without the addressee’s prior, free and informed consent. Taking technological evolution into account, this prohibition can be extended to other communication techniques by Royal Decree. The person who gave his consent may withdraw it at any time and at no cost. The burden of proof of the correct application of this provision is on the side of the sender.

Since 2012 Belgium has, in addition to the provisions mentioned above, particular legal provisions with regard to telemarketing. According to Art. VI.111, § 1 of the Code of Economic Law every operator of public electronic communications networks or services should provide his subscribers the possibility to communicate at any time his objections against the use of his telephone number of or the telephone numbers attributed to him for purposes of direct marketing. The subscriber exercises this right for free and at least by way of telephone, letter or e-mail. The operator has to point the attention of the subscriber to this right at the moment of the subscription in an explicit and prominent manner. Every objection of a subscriber needs to be registered by the operator within five working days in a dedicated database and the date of registration is communicated to the subscriber. The database is made available to the persons wishing to use telephone calls for direct marketing purposes. This latter legal assignment can be delegated to a non-profit entity.

The Belgian Commission for the Protection of Privacy issued - on 30 January 2013 - an update to its recommendation on direct marketing. The update provides the Privacy Commission's position on the recent telemarketing law of 10 July 2012, and on the introduction of a 'do not call' list created by the Belgian Direct Marketing Association (BDMA). The recommendation states that 'all telecommunications operators must offer its customers the option to prevent his/her telephone numbers from being used for direct marketing purposes. Furthermore, the Privacy Commission requires that all marketers conducting telemarketing campaigns must utilise this list to remove any numbers from their own files. Maintained by the BDMA and created in collaboration with the major Belgian telecommunications operators, the 'do not call' list provides a central privacy registry where individuals can register to no longer receive telemarketing calls (https://www.ne-m-appelez-plus.be/). The Privacy Commission stated that it 'welcomes any initiative which contributes to the fair and transparent processing of data in the direct marketing sector.' However, the Privacy Commission highlighted that 'telecommunications operators can choose whether to adhere or not to the list and that they can always choose to use their own privacy lists.' Furthermore, the 'do not call' list 'does not offer any guarantee against abuse, such as the illegal sale of addresses following a security breach, spam or phishing.'

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Entirely in line with Art. 13 of the ePrivacy Directive the Royal Decree of 4 April 2003 regulating advertising by electronic mail (Royal Decree of 4 April 2003 regulating advertising by electronic mail) contains two exceptions to the principle of Article XII.13, § 1 of the Code of Economic Law.
The first exception exempts consent by one's customers to send advertisements by electronic mail when three conditions have been met, cumulatively:

- Firstly, the customer’s electronic data must have been obtained from the sale of a product or service in accordance with the legal and regulatory conditions on privacy protection.
- Secondly, the electronic contact data may be used exclusively for similar products or services that one delivers personally.
- Thirdly, when collecting the contact data, the customers must be afforded the opportunity of easily objecting to future advertisement, free of charge.

The second exception concerns legal persons. It is not necessary to obtain a legal person’s prior consent before being allowed to send advertisements by electronic mail, on condition that the electronic contact data are impersonal.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Electronic mail is defined as: "a text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient". This definition covers not only electronic mail through the internet, but also MMS/SMS/text messages, voice mail, etc., in line with the definition of "electronic mail" in the ePrivacy Directive.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong> The supervisory authority for the correct application of these rules is the Federal Public Service for Economy <a href="http://economie.fgov.be/nl/consument/Internet/Spam/">http://economie.fgov.be/nl/consument/Internet/Spam/</a>. However, since the sending of unsolicited direct marketing messages also falls under the scope of the legislation on personal data protection, the Belgian Privacy Commission is competent in this area as well. Victims of unsolicited messages have therefore, in practice, a choice to send their complaints to the FPS Economy or to the Privacy Commission.</td>
<td></td>
</tr>
<tr>
<td><strong>b.</strong> There is very little jurisprudence on the application of the rules with regard to unsolicited direct marketing communications. One exception is the topic of “viral marketing” on which also some opinions have been published by the FPS Economy and by the Belgian Privacy Commission. Whether or not “viral marketing” is compliant with the Belgian legislation depends on the circumstances. In principle both the rules of the Code of Economic Law and of the Data Protection Law are applicable.</td>
<td></td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| The Belgian regulatory framework with regard to unsolicited direct marketing communications is complex and almost 100% ineffective. As in other countries the vast majority of e-mails (more than 50%) addressed to Belgian internet users are unsolicited messages (so-called “spam”), [http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/](http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/); [https://www.securelist.com/en/analysis/spam?topic=199380272](https://www.securelist.com/en/analysis/spam?topic=199380272). A European study on the activities undertaken at national, European and international level against spam and spyware has been conducted by time.lex in 2008 (SMART 2008/0013). We refer to the Belgian country profile in the context of that study. (also available for the other Member States). |
COUNTRY REPORT

BULGARIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Assoc. Prof. Dr. George Dimitrov, Dimitrov, Petrov & Co.

Date: 18.08.2014
Part 1: Management summary ........................................................................................................3
Part 2: Answers to the questionnaire: ...........................................................................................4
Part 1: Management summary

Management Summary for Bulgaria
The transposition of the ePrivacy Directive into Bulgarian law can be summarized as follows:

- The provisions of the ePrivacy Directive have been transposed in two different legislative acts, namely the Electronic Communications Act of 22 May 2007 (the ECA) and the Electronic Commerce Act of 23 June 2006. All of the amendments to the ePrivacy Directive have been duly reflected. Except for the provisions regarding cookies all other provisions have been transposed in the Electronic Communications Act.

- The scope of the ECA is largely determined by the term “undertaking”. Nearly all the provisions of the Electronic Communications Act are addressed to the “undertakings”. This term is defined in the ECA in its Additional Provisions and is entirely in line with the definition of an undertaking according to the Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services. Some of the provisions transposing the ePrivacy Directive have a different scope and are not applicable only to providers of public electronic communications networks and services. This is in particular the case for the provisions with regard to unsolicited communications for direct marketing, which are applicable to any kind of senders, irrespective of whether natural persons or legal entities.

- Art. 5.3 of the Directive (about “cookies” etc.) has been more or less literally transposed into Bulgarian law. As a consequence it generates multiple questions with regard to its application in practice. It seems unclear for the information society service providers how they should comply with the cookies requirements. Also, these provisions have not been very well communicated to the public. The fact that Bulgarian society is not aware of the adoption of these rules has led to the situation where these rules have proved to be useless now. Unless the competent authorities undertake some steps to make these rules more popular and understandable this will continue to be the case.

- Bulgaria’s rules on traffic and location data are more or less identical to those contained in the ePrivacy Directive. The rules on location data are in line with the provisions of the Directive, but the question remains whether the European legislation is appropriate for the protection of privacy in the sector. With regard to traffic data the implementing legislation is not so clear and some amendments are needed in the future in order to provide better protection.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into Bulgarian law without taking into consideration the transposed provisions of the eCommerce Directive in this respect and they are simultaneously applicable to information society service providers established in Bulgaria. The application of these provisions is unclear. Due to the different legislation regulating identical issues there are two different regulatory bodies in Bulgaria which supervise the unsolicited communications – the Communications Regulation Commission and the Commission for Consumer Protection.
Part 2: Answers to the questionnaire:

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Bulgaria:
- Directive 2002/58/EC has been (partly) transposed into Bulgarian legislation through the **Electronic Communications Act** of 22 May 2007 (hereafter the “ECA”).

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed in Bulgarian law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
English: [http://www.mtitc.government.bg/upload/docs/Electronic_Communications_Act_en.pdf](http://www.mtitc.government.bg/upload/docs/Electronic_Communications_Act_en.pdf) (This version contains the last amendments to the provisions relevant to the study, but is not actual with regard to the following amendments of the Act) |
<table>
<thead>
<tr>
<th>Article</th>
<th>Description</th>
<th>Date and Article</th>
<th>Link (Bulgarian)</th>
<th>Link (English)</th>
</tr>
</thead>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- the full name in your national language
- the English translation of the short name
- the part or the provision(s) of the ePrivacy Directive it supervises
- URL link to website

<table>
<thead>
<tr>
<th>Bulgaria:</th>
<th></th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full name of the authority</strong></td>
<td><strong>English translation of the short name</strong></td>
<td><strong>The part or provision(s) it supervises</strong></td>
<td><strong>URL link to website</strong></td>
</tr>
<tr>
<td>Council for Electronic Media/Съвет за електронни медии</td>
<td>CEM</td>
<td>Provisions regarding audiovisual services and broadcasting</td>
<td><a href="http://www.cem.bg/info">http://www.cem.bg/info</a> bg/1</td>
</tr>
</tbody>
</table>

**Explanation:**
- Complaints with regard to electronic communications networks used for audiovisual services and broadcasting have to be addressed to the supervisory authority in the media sector – the Council for Electronic Media ([http://www.cem.bg/info bg/1](http://www.cem.bg/info bg/1)). The CRC also has competences in this respect, however.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

In the additional provisions of the ECA (§ 1, point 15) electronic communications networks are defined as follows: ‘Electronic communications network’ shall mean a totality of transmission facilities and, where necessary, switching and routing equipment, and other resources, which serve to transmit signals over wires, radio, optic or other electromagnetic means, including satellite networks, fixed (with channel or package switching, including Internet) and mobile land networks, electricity distribution networks, when they are used to transmit signals, networks used for radio and television broadcasting, and cable electronic communications networks for broadcasting of radio and television programmes, irrespective of the type of transmitted information.

The Law (ECA, § 1, point 39) distinguishes between “public” and “non-public” networks. The following is regarded as a “public” network: “Public electronic communications network’ shall mean an electronic communications network, used wholly or partially for the provision of public electronic communications services and/or for the provision of electronic communications to an unlimited number of users for commercial purposes.

The ECA (§ 1, point 17) defines electronic communications service as follows: ‘Electronic communications service’ shall mean a service, usually provided against remuneration, which consists wholly or mainly in conveyance of signals over electronic communications networks, including transmission services, provided through broadcasting networks, excluding services, related to content and/or the control over it. It does not include information society services, which do not consist wholly or mainly in the conveyance of signals over electronic communications networks.

A provider of electronic communication networks and/or services is defined in the following manner: ‘Undertaking providing public electronic communications networks and/or services’ shall mean any natural person – sole trader, or any legal person, who provides electronic communications for commercial purposes in accordance with the provisions laid down in this Law. (ECA, § 1, point 50)

As far as Directive 2002/58/EC refers to the Framework Directive’s definitions it should be noted that the Bulgarian legislation transposes almost literally the provisions of the Framework Directive as can be seen from the abovementioned definitions. Thus, no major differences can be outlined.

In Bulgaria, rules with respect to unsolicited communications are present in two different legislative acts – the ECA and the Electronic Commerce Act 2006. The ECA (Art. 261) provisions are applied to both legal entities and natural persons. The Electronic Commerce Act provisions refer only to information society service providers.

With regard to unsolicited communications and cookies Art. 3, para 1, of the Electronic Commerce Act gives a definition of a provider of services to the information society: Service provider shall be
any natural or legal person that provides information society services.

Under the Electronic Commerce Act information society services are defined as follows: Information society services are those services, including the provision of commercial communications, which are normally provided for remuneration and are provided at a distance by using electronic means after the explicit statement on behalf of the recipient of the service.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

**Bulgaria:**
The ECA sets forth specific criteria which have to be satisfied in order to classify a service as an electronic communications service. First, the service should be remunerated (without prejudice to the fact that this is not an obligatory requirement as far as the law uses the term “normally”). Second, the service should consist wholly or mainly in the conveyance of signals. It has to be emphasized that the electronic communications service might also include information society services in its scope. This would be the case where the information society services consist wholly or mainly in the conveyance of signals.

The main issue then is whether VoIP, webmail and location based services consist wholly or mainly in the conveyance of signals. Currently different types of VoIP services exist (services such as Skype, Viber, etc. and services like VoIP services provided by electronic communications services and/or networks providers). In practice, it seems that services such as Skype do not satisfy the criteria for an electronic communications service and should be qualified as an information society service pursuant to the Electronic Commerce Act. As to webmail and location based services, they are more likely to be defined as information society services.

Furthermore, the Bulgarian NRA distinguishes two types of VoIP services provided by electronic communications services and/or networks providers. Services operating via numbers from the Bulgarian National Numbering Plan (they are regarded as public telephone service pursuant to the ECA) and services operating without such numbers. The first type of service is regulated entirely by ECA provisions. There are doubts with regard to the applicable rules in respect of the second type of VoIP service. It is most likely that they will also be regulated by the ECA.

The Bulgarian NRA has explicitly provided through Decision № 1797 from 26.07.2012 that VoIP services operating without a number from the Bulgarian National Numbering Plan are not public telephone service and are considered an entirely separate type of service. Thus, the distinction is clearly drawn. The Decision lays out a specific list of services and networks through which electronic communications are provided.

In conclusion, the concept of electronic communications services given above must be taken as a baseline in order for one to assess whether a particular service can be defined as an electronic communications service. In this context, if a service falls under the definition of an electronic communications service the service would fall within the scope of the law.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The answers to the questions referred above are rather complicated due to the ICT sector’s complexity as a whole and its transnational nature.

The legislation does not explicitly define the territorial scope of the provisions. Nevertheless, it is important to note that the ECA is strictly applicable to undertakings as defined in the law (‘Undertaking providing public electronic communications networks and/or services’ shall mean any natural person – sole trader, or any legal person, who provides electronic communications for commercial purposes in accordance with the provisions laid down in this Law. (ECA, § 1, point 50). It is also clear that in cases where undertakings are using individually assigned scarce resources Bulgarian legislation will be applicable.

In Art. 1 of the ECA the scope of the act is defined as follows: This Act regulates the social relations pertaining to the provision of electronic communications. I.e. all questions regarding electronic communications services and electronic communications networks and the undertakings providing them are regulated by the ECA. Issues regarding cookies are dealt with within the Electronic Commerce Act.

In this sense, irrespective of the fact whether an entity is established in Bulgaria or not Bulgarian national law would be applicable to undertakings providing electronic communications services and/or networks in Bulgaria. In order to provide such services and/or networks in Bulgaria foreign undertakings are not obliged to register in the Bulgarian Commercial Register as legal entities, but they must be registered as legal entities according to their national law. Their only obligation is to notify the CRC. If an individual scarce resource is needed they have to obtain respective permissions. Once they have done this, they can start operating. In providing these electronic communications services and/or networks they must comply with Bulgarian legal norms, particularly the provisions of ECA. In cases of breach of any of the provisions of the Act foreign undertakings will be subject to the corresponding actions against them.

There is no clarity whether the CRC applies specific requirements with respect to international undertakings (i.e. entities established outside the European Union). However, at the present moment there such entities entered in the public register of the undertakings providing electronic communications services.

In 2010 all undertakings (including foreign entities providing service in Bulgaria) were fined by the CRC due to failure to comply with the provisions on portability of telephone numbers, thus showing that as long as undertakings provide electronic communications services and/or networks in Bulgaria they will be subject to the relevant Bulgarian legislation. Generally speaking, Bulgarian law is normally applied to wholly internal situations. In cross-border situations, however, International
Trade Law provisions might apply if certain conditions are met.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Currently, no relevant guidelines with regard to the interpretation of the definitions laid out in the implementing legislation have been released.</td>
</tr>
<tr>
<td>b.</td>
<td>No relevant court cases with regard to the interpretation of the definitions laid out in the implementing legislation could be found.</td>
</tr>
</tbody>
</table>
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

a. and b.

Currently, there is no clarity with regard to the role of the Commission for Protection of Personal Data (CPPD) with respect to the privacy rules provided by the ECA. Thus, in practice the CRC had exercised competences that are related to personal data issues and normally should fall within the scope of competence of the CPPD. For example, the CRC issues guidelines on the form and contents of the consent for the processing of personal data in contracts between undertakings and customers).

Some uncertainty also exists regarding the distinction between information society services under the Electronic Commerce Act and electronic communication services under the ECA. This leads to difficulties when applying the ePrivacy Directive.

More complicated issues may arise in the future, as well, in connection to the absence of clear provisions on the territorial scope of the privacy provisions with respect to the development of a variety of cross-border services.

In our opinion, the existence of duplicate provisions on unsolicited communications (present in the ECA, the Electronic Commerce Act and the Personal Data Protection Act) is a problem and may raise a lot of question on the application of the respective provisions.

The abovementioned uncertainties need to be clarified by providing more clear definitions on the respective services. In our opinion this has to be dealt with on a European level rather than at a national level. As to unsolicited communications, all the provisions have to be unified in a single legislative act in contrast to the present situation.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The principle of confidentiality is implemented entirely in Chapter 15, Section 2, Art. 245 – 247 of the ECA. The scope of the provisions is broader than that given in the ePrivacy Directive. The Bulgarian legislator has extended the scope of the principle of confidentiality not only to communications and the related traffic data but also to location data and data necessary to identify the user.

According to Art. 245, undertakings providing electronic communications services are forbidden to disseminate and disclose such data.

Art. 246 prohibits certain activities with the purpose of protecting the confidentiality of communications and the related traffic data: For the purpose of protecting the confidentiality of communications and the related traffic data, the listening, recording, storage or other kinds of interception or surveillance of communications by others than the sender and recipient of the communication without the express consent of the sender and recipient shall be prohibited, with the exception of the cases where this is provided for in a law.

Thus, the law forbids all of the aforementioned actions unless consent is given by the user.

The ECA provides certain exceptions to the confidentiality principle:

- Art. 246, para. 2 states that the prohibitions do not apply in cases where: 1. the storage is required for technical reasons or is an essential part of the provision of the service; 2. the technical parameters of the technical parameters of the service are checked by persons empowered under this Act.

- With regard to storage of communications and the related traffic data Art. 247, para. 1 provides another exception subject to which the restrictions would not apply. They must be cumulatively available: 1. the recording is necessary and is provided for in a law for the purpose of providing evidence of the conclusion of commercial transactions, and; 2. the sender and recipient of the communications have been informed prior to the recording about the recording, the purposes thereof and the duration of the storage, as well as of the right to refuse such recording.

There is a legal definition of the concept of “communication” in the §. 1, p. 68 of the Additional provisions of the ECA: “Communication” shall be any information, exchanged or conveyed between a finite number of parties by means of a public electronic communications service. This does not include any information conveyed as part of a broadcasting services to the public over an electronic communications network, except to the extent that the information can be related to an identifiable subscriber or user receiving the information.

The Bulgarian definition of a communication is literally the same as the definition given in the ePrivacy Directive in para. 2 (d), i.e. the meaning and the interpretation of the concept should be uniform.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

This provision has been transposed in Art. 247 of the ECA. The exception therein, however, differentiates from the wording of the Directive. The provision of the Bulgarian law, as can be seen below, sets more stringent criteria requiring additional conditions to be met. Namely, this is the requirement for the sender and recipient of the communications to have been informed prior to the recording, the purposes thereof and the duration of the storage, as well as the right to refuse such recording. Furthermore, the storage of the information must be necessary and provided for by law for the purpose of providing evidence for the conclusion of business transactions.

Article 247. (1) In addition to the exceptions covered under Article 246 (2) herein, the restrictions shall furthermore not apply regarding the storage of communications and the related traffic data under the following conditions:
1. the recording is necessary and is provided for in a law for the purpose of providing evidence of the conclusion of commercial transactions, and
2. the sender and recipient of the communications have been informed prior to the recording about the recording, the purposes thereof and the duration of the storage, as well as of the right to refuse such recording.
(2) The recorded communications and related traffic data shall be stored for a period not longer than the period during which the said communications and data can be used according to Item 1 of Paragraph (1).
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

In connection to Art. 15 (1) of the ePrivacy Directive the following legislation is relevant:

First, the Bulgarian Constitution provides an important exception to this principle in Articles 34, para. 2 and 57.

Article 34. (1) Freedom and secrecy of correspondence shall be inviolable.
(2) Exceptions of this rule shall be allowed only upon a permission issued by a judicial authority in cases where this is necessary for investigation or prevention of serious crimes.

Article 57. (1) The fundamental rights of the citizens shall be irrevocable.
(2) No abuse of rights shall be allowed, neither exercise of rights if this exercise infringes upon other persons’ rights or legitimate interests.
(3) In cases of war being declared, of declaration of state of martial law or other state of emergency, the exercise of some rights of the citizens may be temporary restricted, with the exception of the rights envisaged in Articles 28, 29, 31, (1), (2) and (3), Article 32 (1) and Article 37.

The Bulgarian Criminal Procedure Code also contains an exception: Article 159 (1) Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, which may be of significance to the case.

Article 165 Interception and seizure of correspondence
(1) Interception and seizure of correspondence shall be allowed only where this is necessary for disclosure or prevention of serious crime.
(2) Interception and seizure of correspondence in pre-trial proceedings shall be performed upon request of the prosecutor with the authorisation of a judge from the respective first instance court or a judge from the court in the area of which the action is taken.
(3) In court proceedings search and seizure of correspondence shall be performed by a decision of the court which is trying the case.
(4) The interception and seizure of correspondence shall be carried out in pursuance of Article 162, paras 1 - 4.
(5) The provisions of paragraphs 1 - 4 shall also apply to searches and seizures of electronic mail.

An exception is provided as well in the Special Surveillance Means Act. Chapter 1 of the Act stipulates that when the use of special surveillance means is required for the prevention, detection and prosecution of serious intentional crimes, the confidentiality principle shall be temporarily restricted. Permission for the use of special surveillance means can also be obtained in cases related to the national security.

Special surveillance means can be used subject to a strict procedure. Only an exhaustive list of national judiciary bodies, police authorities and bodies of the Ministry of Defence may obtain permission to use such means and solely following a court order.
Another exception is provided in the Act for the National Emergency Call System with a Single European Number 112 and the Rules establishing the Terms and Conditions for the Provision of Location Data and Data Related to Subscribers by Undertakings Providing Public Telephone Services in Emergency Calls to Emergency Call Centers. The incoming and outgoing calls are recorded in a special register and pursuant to Art. 16, para. 4 of the Act emergency services and judicial authorities may request data from the register of the incoming and outgoing calls in relation to a particular incident.

Articles 250a – 251a of the ECA which transpose the provisions of the Data Retention Directive set out rules for the retention of data (this data is de facto traffic data). The latter can be stored and disclosed for the purpose of the investigation, detection and prosecution of serious crime and cybercrime, as well as in cases of tracking down investigated persons.

Such a disclosure of data, however, is subject to a strict procedure. Only an exhaustive list of national judiciary bodies, police authorities and bodies of the Ministry of Defence (defined in the ECA) may obtain access to these types of data and solely following a court order.
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Bulgarian legislation does not specifically address automated breaches of confidentiality without human involvement. No differentiation with respect to breach of confidentiality with or without human participation is present. The general provision of the ECA (Art. 245) regarding the principle of confidentiality does not distinguish between the protection of content of the communications and other data relating to communications.

As to interception, the law specifically points out that the interception of communications and the related traffic data is unlawful unless a prior consent has been given by the sender or the receiver of the communication.

Other legislative acts, however, make a distinction between the protection of content of the communications and other data relating to communications (i.e. traffic data).

First, the Bulgarian Constitution in Articles 34 declares the principle of confidentiality of the correspondence of all citizens. From the text of the legal norm it can be concluded that the Constitution protects the content of the communication rather than any other electronic data related.

*Article 34. (1) Freedom and secrecy of correspondence shall be inviolable.*

(2) *Exceptions of this rule shall be allowed only upon a permission issued by a judicial authority in cases where this is necessary for investigation or prevention of serious crimes.*

Secondly, the Bulgarian Criminal Code makes a distinction between traffic data and content of communications. This is clear from the following articles:

Art. 171 incriminates all violation of the confidentiality of communications as a general principle.

*Article 171*  
(1) *(Amended, SG. No. 28/1982, SG No. 10/1993)* A person who contrary to the law:  
1. opens, falsifies, hides or destroys a letter, telegram, sealed papers, package and the like of another person;  
2. takes another person's, although opened, letter or telegram for the purpose of obtaining knowledge of their contents, or for the same purpose delivers another person's letter or telegram to someone else;
3. (New, SG No. 92/2002) becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee. shall be punished by deprivation of liberty for up to one year or by a fine from BGN one hundred to three hundred.

(2) If the act was perpetrated by an official who availed himself of his official position, the punishment shall by deprivation of liberty for up to two years, and the court may also rule deprivation of the right under Article 37 (1), sub-paragraph 6.

(3) (Supplemented, SG No. 92/2002) A person who, by use of special technical means, unlawfully obtains information not addressed to him, communicated over the telephone, telegraph, computer network or another telecommunication means, shall be punished by deprivation of liberty for up to two years.

(4) (New, SG No. 38/2007) Where the act under paragraph 3 has been committed with a venal goal in mind or considerable damages have been caused, the punishment shall be deprivation of liberty for up to three years and a fine of up to BGN five thousand.

The legislator has adopted a specific provision with regard to the protection of traffic data.

Article 171a
(New, SG No.26/2010)
(1) A person who unlawfully acquires, discloses or disseminate traffic data as collected, processed, stored or used under the Electronic Communications Act is sentenced to imprisonment up to three years or is sentenced to probation.

(2) When the act under paragraph (1) is committed from mercenary motives, the sentence is imprisonment from one to six years.

b. In addition to the aforementioned legislation (as well as those mentioned in point 3) the following provisions also have an impact:

In Art. 348a, para. 1 the Bulgarian Criminal Code a special provision on the unlawful use of telecommunication networks, equipment and services:

Article 348a. (1) The one who, through deceit or any other unlawful means, makes use of a telecommunication network, equipment or service, in order to generate or redirect, to his own or the interest of another, the directed transmission of signals, written text, image, sound, data or messages of any type, through conductors, radio waves, optical or any other transmission environment, shall be punished by deprivation of liberty of up to six years and a fine of up to BGN ten thousand.

In Chapter 9A of the Criminal Code cybercrimes are regulated. These provisions incriminate different types of interference with computer systems and computer data. Computer data is defined as:
Article 93, item 22. (New, SG No. 92/2002, amended, SG No. 38/2007) “Computer data” is any representation of facts, information or concepts in a form suitable for automatic processing, including computer programs.
## 5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

| a. the scope and substance of your national implementation |
| b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)? |

**a.** Cookie provisions are transposed in the Electronic Commerce Act, Art. 4a. The wording of the legal norm is rather different to the ePrivacy Directive but the interpretation seems to be identical without prejudice to the fact that the Bulgarian legislation has restricted the scope of application of this provision only to providers of information society services (in comparison with the ePrivacy Directive where no such restriction is present). This is due to the fact that this provision is implemented in the Electronic Commerce Act and applies to information society service providers.

**Article 4a. (New - SG No. 105/2011, in force as of 29.12.2011) (1) The information society service provider may store information or gain access to information stored in the terminal equipment of the service recipient, provided that:**

1. the information society service recipient is provided with clear and exhaustive information concerning the purpose of storage or access to information in accordance with the Personal Data Protection Act, as well as for the purpose of processing thereof;
2. the information society service recipient is provided with the option to refuse the storage or access to information.

**(2) In the cases under Paragraph (1), the information society service providers provide the service recipient the option to obtain at any time information about the data stored in the terminal device.**

**(3) Upon any subsequent storage or gaining of access to information by the same provider, the requirements of Paragraph (1) are not mandatory, provided that the service recipient does not object thereto.**

**(4) The requirements of Paragraph (1) shall not apply to the storage and provision of access to information where such are necessary for:**

1. transmission of communications over the electronic communication network;
2. provision of an information society service expressly requested by the information society service recipient.

**b.** The provision quoted above doesn’t distinguish between types of cookies or between categories of end equipment nor does any other legislation at present.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Article 4a of the Bulgarian Electronic Commerce Act does not contain an answer to these questions and there are not any court decisions yet interpreting this provision and applying it to concrete situations.

As a matter of fact, the wording of the law on this point is rather obscure and states that the information society service recipient should be provided with the option to refuse the storage or access to information. This means that unless the recipient has been provided with such an option the use of cookies by the provider of information society services will be unlawful. The law doesn’t provide for any form or manifestation of the consent in order to satisfy the conditions laid out in the Act.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

<table>
<thead>
<tr>
<th>This is implemented in Art. 4a, para. 4 of the Electronic Commerce Act:</th>
</tr>
</thead>
</table>
| (4) The requirements of Paragraph (1) are not applied to the storage and provision of access to information where such are necessary for:  
1. transmission of communications over the electronic communication network;  
2. provision of an information society service expressly requested by the information society service recipient. |

However, the wording of the above provision is not very clear and it is difficult to determine which types of cookies should fall within its exceptions. It is unclear what the criteria for determining the “necessity” of the use of cookies should be. Furthermore, all kind of information society services are normally expressly requested by their users which may lead to application of the above exception to almost every information society service.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

It is very difficult to make an assessment whether the compliance with cookie rules and provisions is observed. This is because the competent authority (CCP) usually acts under a complaint on these issues and users are not really aware of the existence of rules on cookies. According to the law, however, the CCP has the competence to issue different instructions and impose sanctions for non-compliance with the provisions of the Electronic Commerce Act, which means that it can impose sanctions for breach of cookie rules if it detects any violations. However, there have not been any enforcement actions yet. Also, no relevant court practice on the application of Art. 4a of the Electronic Commerce Act which transposes Art. 5.3 of the Directive could be found.

In practice, many providers introduce pop-up screens or one-time banners (positioned at the top or the bottom of the screen), etc. allowing users to accept or refuse cookies. This is due to the perception of foreign practices. However, some providers of information society services (e.g. website owners) are not willing to completely allow users to refuse all types of cookies.

No relevant statistics on cookies are available.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>No relevant guidelines on the interpretation and/or application on these questions could be found.</td>
</tr>
<tr>
<td>b.</td>
<td>No relevant court cases with regard to the interpretation of the definitions laid out in the implementing legislation could be found.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The provisions of the Bulgarian legislation transposing Art. 5.3 of the ePrivacy Directive are too vague to allow a consistent application by the service providers. Moreover, the scope of the provisions is unclear. Additional guidance from the NRA with respect to the practical application of the cookie rules is needed.

   As far as the CCP tends to act under a complaint and consumers are not really aware of the existence of rules on cookies and their scope, these provisions cannot have significant impact and do not provide effective protection.

   In our opinion, the effectiveness of these rules on European level is also very unclear. Instead of promoting the development and provision of user-friendly services, Art. 5.3 of the ePrivacy Directive imposes on the service providers requirements which make the use of their services clumsy and inconvenient. The users are supposed to consent with cookies use almost any time when they access a European website and they are provided with information that normally they do not understand. Raising the awareness of the society regarding the nature of the cookies may improve the effectiveness of the protection of their privacy much better that the adoption of such rules.

   b. In our opinion, it is advisable the competent national authorities to issue guidelines in order to inform the society on the existence of these rules and how they should apply in practice.

   Likewise, we consider that the wording of the law should be amended in order to make it more comprehensible.
C. Traffic data

<table>
<thead>
<tr>
<th></th>
<th>In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Additional provisions, § 1, item 71 of the ECA define traffic data as follows: “Traffic data” shall be data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.</td>
</tr>
<tr>
<td></td>
<td>The wording of the Bulgarian legislation is in conformity with the definition provided in the Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

The legal requirements for the lawful processing of traffic data are generally the same as those provided by the ePrivacy Directive. However, there are some specific provisions which do not follow strictly the ePrivacy Directive’s wording. In particular, it is interesting to mention the provision of Art. 256 of the ECA which stipulates several specific purposes for which the traffic data could be processed. In particular, traffic data could be processed for: 1) detecting, locating and eliminating defects and software errors in the electronic communications networks; 2) detecting and terminating unauthorized use of electronic communications networks and facilities, where there is reason to consider that such actions are performed and this has been claimed in writing by the affected party or by a competent authority; 3) detecting and tracing of nuisance calls, upon a request by the affected subscriber requesting that the undertaking providing the service take measures. Although, there is no similar provision in the ePrivacy Directive, in our opinion Art. 256 of the ECA cannot be considered as significant deviation from the Directive’s requirement, because the above mentioned purposes are related to the very provision of electronic communications services, transmission of communications, billing and traffic management and fraud detection. In this respect, it could be considered that the specific purposes under Art. 256 of the ECA fall within the scope of the larger purposes specified by Art. 6 of the ePrivacy Directive.

**Article 248.** (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) (1) (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) The undertakings providing public electronic communications networks and/or services including networks supporting equipment for data collection and identification may process data on users where such data are designated directly for the provision of the electronic communications services.

(2) The data on users shall include:

1. traffic data: data necessary for the provision of electronic communications services, for billing, for the formation of the subscriber bills, as well as for proving their reliability:
   (a) number of the calling end-user and number of the called end-user, card number if electronic pre-payment cards are used;
   (b) start and end of the call, specified by date and time, with accuracy up to the second, to the extent technically feasible, and/or, in case of data transfer, volume of the transferred data, for billing purposes;
   (c) type of the service provided;
   (d) points of interconnection upon establishment of the call, start and end of the use of the said points, specified by date and hour, with accuracy up to the second, to the extent technically feasible;
   (e) data on the type of connection or time zones and geographical areas, necessary for billing purposes;
   (f) location of a user of a service provided over a mobile network, including where a roaming service is provided;

2. data necessary for the formation of subscriber bills, as well as for proving the reliability of the said bills, including the following data:
   (a) data on the subscriber: in respect of natural persons: forename, patronymic and surname, Standard Public Registry Personal Number and in respect of non-resident persons, Personal Number, in respect of legal persons and of sole trader natural persons: business name, registered office, address of the place of management and relevant identification code;
   (b) type of electronic communications services used;
(c) total number of price units charged for the period of formation of the bill in case of periodic payment;
(d) price of the services used for the relevant period;
(e) information related to the option for payment chosen by the subscriber and the payments made and payments due;
(f) information regarding changes in the use of the service: restriction of use, lapse of a restriction;
3. location data: data processed in electronic communications networks giving the geographic position of the electronic communications terminal equipment of the user.

There are the general requirements for the traffic data processing.

Article 250. (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) (1) (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) The undertakings providing public electronic communications networks or public electronic communications services, which collect, process and use traffic data for the purpose of a specific call or the establishment of a connection, must delete the said data or make them anonymous upon termination of the said call or connection, unless the said data is directly necessary for the establishment of a new call or connection or in the cases provided for in this Act.

(2) (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) The undertakings providing public electronic communications services must provide to the users accurate and full information about the type of traffic data which are processed for billing purposes and for interconnection payments, and about the duration of such processing.

(3) The undertakings referred to in Paragraph (1) shall store and process traffic data for the purposes of billing subscribers and for interconnection payment until the payment is effected, except in the cases where they are challenged or payment is pursued according to the procedure established by this Act.

(4) The undertakings referred to in Paragraph (1) shall provide information about traffic data to the Commission at its request, in connection with settlement of disputes regarding access, interconnection and billing.

(5) The undertakings referred to in Paragraph (1) may use the data under Paragraph (1) for the purpose of market research, including the extent to which the electronic communications services provided by the said undertakings satisfy the requirements of users, or for the provision of value added services, requiring further processing of traffic data or location data other than traffic data necessary for the conveyance of the communication or for the billing of the communication, solely where the said undertakings have obtained the consent of users. The personal data on end-users, received in connection with the research, shall be made anonymous.

(6) After obtaining the prior consent of users, the undertakings referred to in Paragraph (1) may process the information about the types of traffic data for the purpose of market research.

(7) The undertakings referred to in Paragraph (1) shall provide to users accurate and full information about the type of traffic data which is processed, as well as about the duration of such processing.

(8) After obtaining the consent of users, the undertakings referred to in Paragraph (1) shall have a right to provide traffic data related to the users for the purpose of provision of value added services requiring an further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for the billing of the communication.

(9) The undertakings referred to in Paragraph (1) shall include a mechanism in their relations with the users, making it possible for user to withdraw the consent thereof given under Paragraph (5) at any time.
Article 252. (1) Traffic data shall be processed by persons acting under the authority of the undertakings providing public electronic communications services who are responsible for:
1. management of traffic data and of data referred to in Item 2 of Art. 248 (2) herein;
2. user enquiries;
3. fraud detection;
4. marketing electronic communications services;
5. providing value added services requiring further processing of traffic data or of location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.
(2) The access of officials shall be restricted to the data necessary for the relevant activity.

Article 256. (1) The undertakings providing public electronic communications services may collect, process and use the data under Art.248 (2) herein for:
1. detecting, locating and eliminating defects and software errors in the electronic communications networks;
2. detecting and terminating unauthorized use of electronic communications networks and facilities, where there is reason to consider that such actions are performed and this has been claimed in writing by the affected party or by a competent authority;
3. detecting and tracing of nuisance calls, upon a request by the affected subscriber requesting that the undertaking providing the service take measures.
(2) Upon taking the actions covered under para. (1), the undertakings providing public electronic communications services shall inform the persons concerned as soon as possible, unless this will prevent the achievement of the objectives of this provision.
(3) The data collected according to the procedure established by this Article shall be used only for the purposes indicated in para. (1).
### 3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Article 250, para. 1 of the ECA contains rules which prescribe that traffic data must be anonymised or deleted under certain conditions:

**Article 250. (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) (1) (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) The undertakings providing public electronic communications networks or public electronic communications services, which collect, process and use traffic data for the purpose of a specific call or the establishment of a connection, must delete the said data or make them anonymous upon termination of the said call or connection, unless the said data is directly necessary for the establishment of a new call or connection or in the cases provided for in this Act.**
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

There are a few cases mentioning traffic data but no relevant cases can be mentioned in the context of the present Study.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

It seems that the law, as well as the Directive, forbids undertakings to use third parties for the processing of traffic data, which could have its positive effects. In our judgement, however, third parties who have expertise in processing of data could deal with these functions much better than the personnel. Nowadays, where the services become more and more complex the prohibition of subcontracting any activities outside the undertakings may actually impede the development of the sector. In the context of the development of cross-border services and complexity of e-communication and information society services the restrictive legislation can be an obstacle to the competitiveness of the European undertakings. On the other hand, the benefits for the protection of the privacy are unclear. As far as the undertakings are kept responsible for the security of the data, it should not be important whether these data are processed by their personnel only, or by third parties – processors.

Another weak point is the lack of clear distinction between personalized and anonymized traffic data. Currently, it is not very clearly stipulated that once the traffic data are anonymized, they should not be subject to the restrictive regime of traffic data. Also, the exhaustive list of activities and purposes for which traffic data could be processed seems to prohibit the extraction and processing of anonymized/derivative traffic data for marketing or statistical purposes, although such processing cannot affect private life of the users in any manner.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>The Additional provisions, §. 1, item 7 of the ECA define location data as follows: “Location data” shall be any data processed in an electronic communications network or service, indicating the geographic position of the electronic communications or electronic communications terminal equipment of a user of a public electronic communications service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The definition is identical to the definition provided in the ePrivacy Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Art. 252 – 255 transpose provisions with respect to location data other than traffic data. These rules are in conformity with the Directive and are fairly clear, logical and appropriate and no real differences can be indicated.

Article 252. (1) Traffic data shall be processed by persons acting under the authority of the undertakings providing public electronic communications services who are responsible for:
1. management of traffic data and of data referred to in Item 2 of Art. 248 (2) herein;
2. user enquires;
3. fraud detection;
4. marketing electronic communications services;
5. providing value added services requiring further processing of traffic data or of location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.
(2) The access of officials shall be restricted to the data necessary for the relevant activity.

Article 253. (1) After receiving a prior written consent, the undertakings providing electronic communications services may process location data on users and subscribers subject to the condition that:
1. the data are made anonymous, or
2. the data are necessary for the purposes and duration of provision of value added services requiring further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.
(2) The undertakings referred to in para. (1) shall inform the end-users thereof in advance of the type of location data referred to in para. (1), which will be processed, of the duration and purposes of such processing, and of the possibility to transmit the data to a third party in connection with the provision of value added services requiring further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.
(3) The undertakings referred to in para. (1) shall ensure to users the possibility, free of charge, of:
1. withdrawing at any time the prior consent given thereby to processing of location data thereof;
2. temporarily refusing the processing of location data thereof for each connection to the electronic communications network or for each transmission of a communication.

Article 254. Location data shall be processed by officials designated by the undertakings referred to in Art. 252 (1) herein or by persons empowered by a third party providing value added services and must be restricted to what is necessary for the provision of value added services.

Article 255. (Last Amendment - SG No. 105/2011, in force as of 29.12.2011) (1) The undertakings referred to in Art. 252 (1) herein shall process and provide on their costs location data on end-users in case of emergency calls, even where no prior consent to the processing of such data has been obtained or where such processing has been refused under Art. 253 (3) herein. The data shall be provided only to the relevant centers for receiving calls to the single European emergency call number "112" at the moment the call...
reaches them.
(2) (Last Amendment - SG No. 17/2009) The undertakings referred to in Art. 252 (1) herein shall ensure, for their own costs, the hardware and software necessary for routing calls and transfer to the emergency call centres.
(3) (Last Amendment - SG No. 17/2009) The conditions and order of providing data about the location of end users and subscribers in cases of urgent calls from the enterprises rendering public telephone services to the urgent call centers are determined by regulations adopted by the commission.

Article 256. (1) The undertakings providing public electronic communications services may furthermore collect, process and use the data under covered under Art.248 (2) herein for:
1. detecting, locating and eliminating defects and software errors in the electronic communications networks;
2. detecting and terminating unauthorized use of electronic communications networks and facilities, where there is reason to consider that such actions are performed and this has been claimed in writing by the affected party or by a competent authority;
3. detecting and tracing of nuisance calls, upon a request by the affected subscriber requesting that the undertaking providing the service take measures.
(2) Upon taking the actions covered under para. (1), the undertakings providing public electronic communications services shall inform the persons concerned as soon as possible, unless this will prevent the achievement of the objectives of this provision.
(3) The data collected according to the procedure established by this Article shall be used only for the purposes indicated in para. (1).

Article 256 is applied to all data subject to processing, namely traffic data, location data and data necessary for the formation of subscriber bills.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Such rules are present in Art. 253, para. 1:

Article 253. (1) After receiving a prior written consent, the undertakings providing electronic communications services may process location data on users and subscribers subject to the condition that:

1. the data are made anonymous, or
2. the data are necessary for the purposes and duration of provision of value added services requiring further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.

(2) The undertakings referred to in para. (1) shall inform the end-users thereof in advance of the type of location data referred to in para. (1), which will be processed, of the duration and purposes of such processing, and of the possibility to transmit the data to a third party in connection with the provision of value added services requiring further processing of traffic data or location data other than the traffic data necessary for conveyance of the communication or for billing of the communication.

(3) The undertakings referred to in para. (1) shall ensure to users the possibility, free of charge, of:

1. withdrawing at any time the prior consent given to processing of location data thereof;
2. temporarily refusing the processing of location data thereof for each connection to the electronic communications network or for each transmission of a communication.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. No relevant guidelines on the interpretation and/or application on these questions could be found.

b. No relevant court cases with regard to the interpretation of the definitions laid out in the implementing legislation could be found.
5. **What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?**

| Generally, these rules are in conformity with the Directive and are fairly clear, logical and appropriate. |
| It should only be noted that, as mentioned above, in our opinion we consider the fact that the law forbids undertakings to use third parties (processors) for the processing of traffic data as too restrictive without any actual impact on the protection of privacy. |
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points?

   a. With regard to unsolicited direct marketing communications the provisions from the ePrivacy Directive are transposed in Art. 261 of the ECA. The wording of our law is a bit different, however, in contrast to the ePrivacy Directive. This general provision on unsolicited marketing communications states: "Calls, communications or electronic mail with or without human participation, for the purposes of direct marketing and advertising shall be allowed only in respect of users who have given their prior consent. The consent may be withdrawn at any time."

   b. With respect to the scope and terminology used by the Bulgarian law it must be noted that there are some minor differences. For example, fax machines are not explicitly mentioned in the provision. Nevertheless, it seems that ECA is broader than the Directive and fax machines and all other means of communication must be considered as part of its scope. The ECA states that the use of calls, communications and electronic mail with or without human participation for the purposes of direct marketing is prohibited unless a prior consent has been given.

   The Bulgarian legislator has merged the provisions of the Directive (Art. 13 (1) and (3) into one, namely Art. 261 of the ECA, for legislative economy. In accordance with Art. 13 (3) of the Directive, the legislator has chosen the first option suggested, i.e. to request for a prior consent by the user. This approach, however, provides opportunities for extensive interpretation and wide discussions on the matter. Under the ECA (Additional provisions, §. 1, item 49) users are defined as follows:

   49. ‘User’ shall mean a legal or natural person, using or having declared intent to use a public electronic communications service.

   Thus, it shall be kept in mind that the provisions of Art. 261 of the ECA refer to both legal entities and natural persons.

   Another difference which should be highlighted is that the purposes under Art. 261 of the ECA are both direct marketing and advertising in comparison with the Directive where only direct marketing is indicated.

   In our opinion, however, the provisions of the ECA are in conformity with the Directive.

   Bulgarian legislation had already provided rules on unsolicited commercial communications prior to the adoption of the rules under Art. 261 of the ECA. Those are governed by the Electronic Commerce Act, Art. 6. These provisions apply simultaneously with the rules on unsolicited direct marketing communications under the ECA. However, there is a slight difference between the scopes of their application. The provisions of Art. 6 of the Electronic Commerce Act apply to information society service providers only, whereas Art. 261 of the ECA applies in general to any kind of senders of unsolicited commercial communications.

   Art. 6, Para 4 of the Electronic Commerce Act sets a general prohibition for unlawful sending of
unsolicited communications to individuals: It is prohibited to send unsolicited commercial communications to consumers without their prior consent. Thus, Art. 6, para. 4 of the Electronic Commerce Act provides an opt-in regime for consumers, as long as para. 2 and para. 3 provide an opt-out regime for the legal entities.

A consumer under the Electronic Commerce Act (Additional provisions, §. 1, item 4) is:
4. “Consumer” is considered a consumer under Paragraph 13, pt. 1 of the additional provisions of the Consumer Protection Act.

Consumer Protection Act, Additional provisions, §. 13, item 1:
1. "Consumer" shall be any natural person who acquires products or uses services for purposes that do not fall within the sphere of his or her commercial or professional activity, and any natural person who, as a party to a contract under this Act, acts outside his or her commercial or professional capacity.

With respect to legal entities, para. 2 stipulates that it is permitted to send unsolicited communications to legal entities. However, according to the law, the CCP is obligated to keep an electronic register of the electronic addresses of the legal entities which do not wish to receive unsolicited commercial communication. If a legal person has registered its email addresses at this register, it will be unlawful to send unsolicited commercial communications to the respective addresses.

Para. 1 provides a specific condition with regard to information society service providers in cases where all other conditions for lawful sending unsolicited communications have been fulfilled: A service provider who sends unsolicited commercial communication by electronic mail without prior consent of the recipient must provide clear and unambiguous identification of the commercial communication as an unsolicited one yet on its filing with the recipient.

Finally, pursuant to the Consumer Protection Act, Art. 68k sending persistent and unsolicited commercial communications might be declared unfair and aggressive commercial practice.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The legal requirements for the lawful sending of unsolicited messages via electronic mail or other means pursuant to Article 13(1) and 13(3) of the Directive are indicated in Art. 261 of the ECA. As explained above, the scope of the Bulgarian provision is broader than the scope of the Directive and all means of electronic communications must be considered part of its scope. This includes electronic mail, fax machines, automatic calling machines, text messages, instant messaging, calls, telemarketing, etc. Except for the scope of application there are no differences from the definition provided in the Directive.

The conditions which have to be met are: 1) a prior consent by the user must be obtained; 2) an option that the consent may be withdrawn at any time must be provided by the undertakings. It is not explicitly mentioned but the withdrawal is free of charge.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

<table>
<thead>
<tr>
<th>ECA lays down the following exception to the opt-in mechanism in Art. 261, para. 2 of the ECA:</th>
</tr>
</thead>
</table>

**Art. 261, para. 2.** Any person who, within the context of a commercial transaction or upon provision of products or service, has obtained data allowing electronic contact with the customer, may use such data to send direct marketing or advertising messages of that person’s own, similar products or services, providing each customer with the opportunity in an easy manner and free of charge to:

1. express his dissent at the moment of conclusion of the transaction;
2. express his dissent to receive such communications in a future moment in case that has not been done upon conclusion of the transaction.

The provision of Art. 261 of the ECA is applicable both to legal entities and natural persons.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The law does not distinguish between different communication channels. The definition of an electronic mail is given in § 1, point 15 of the Additional provisions of the ECA: “Electronic mail” shall be any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or is received in the recipient’s terminal equipment. In the scope of the definition are included all communication channels who meet the requirements of the legal norm. This would most likely include MMS/SMS/text messages, Bluetooth messages, instant messaging, etc.

Under the Electronic Commerce Act an electronic mail is defined (§ 1, point 8 of the Additional provisions) as follows: “An Electronic mail” is an electronic instrument for storage and transfer of electronic communication on the internet network by means of standardized protocols.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>No relevant guidelines on the interpretation and/or application on these questions could be found.</td>
</tr>
<tr>
<td>b.</td>
<td>There have been several cases where the abovementioned provisions of the ECA have been applied to mobile operators and advertising services. Mostly, Art. 261, par. 1 and para. 5 have been infringed, especially in cases where a prior consent from users has not been obtained and in cases where the identity of the sender was not clearly indicated. Nevertheless, there have not been cases where the concepts have been interpreted in a way to provide some general guidelines for the interpretation of the provisions to the public or other courts.</td>
</tr>
<tr>
<td>6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td>These rules are not clear and logically consistent. This is due to the fact that rules on unsolicited communications are regulated in two (even three – together with the Personal Data Protection Act which implements Directive 95/46/EC and regulates the processing of personal data for direct marketing purposes) different legislative acts. These provisions are almost identical and apply simultaneously. Thus, two separate rules on one issue exist at the same time. In this way, a possibility exists that a couple of penalties can be imposed on persons (legal or natural) for one violation.</td>
<td></td>
</tr>
<tr>
<td>This confusion stems from the fact that the Bulgarian legislation on these issues almost literally transposes the respective EU Directives. All definitions and concepts are as prescribed from European law, but the European legislation also contains some discrepancies.</td>
<td></td>
</tr>
<tr>
<td>In our opinion a uniform regulation of the rules on unsolicited communications is needed.</td>
<td></td>
</tr>
</tbody>
</table>
COUNTRY REPORT

CYPRUS

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Olga Georgiades, Lexact Solutions Ltd

Date: 10/9/2014
Contents

Part 1: Management summary ....................................................................................................................... 3
Part 2: Answers to the Questionnaire ............................................................................................................ 5
Part 1: Management summary

Management Summary for Cyprus

The transposition of the ePrivacy Directive into Cyprus law can be summarized as follows:

- The provisions with regard to the scope of the Directive have been transposed into Cypriot legislation by the Law Regulating Electronic Communications and Postal Services of 2004 (hereafter “the Electronic Communications Law”), and in particular Part 14 thereof. The Electronic Communications Law is compatible as regards its wording with the Directive. The Electronic Communications Law and the relevant Decrees issued on the basis of the Law are sufficiently clear as to their wording and quite appropriate for protecting privacy in Cyprus. Furthermore, it should be noted that there are a number of other Laws and secondary legislation which also protect privacy and which afford additional protection to individuals, coupled with the provisions of the Constitution of the Republic.

- There is a territorial limitation on the application of the Law which only affects the provision of electronic communications networks and services in the Republic of Cyprus and it is deemed that the Law does not affect operators outside of the national territory.

- The Office for the Commissioner of Electronic Communications and Postal Regulation (http://www.ocecpr.org.cy) (‘OCECPR’) is the Cypriot NRA regulating the electronic communications sector and is one of the two supervisory authorities for the provisions transposing the ePrivacy Directive which have been inserted into the Cypriot Electronic Communications Law. According to the provisions of section 107, the responsibilities of the Data Protection Commissioner were extended to cover the part of the Electronic Communications Law that deals with secrecy of communications, traffic and location data, telephone directories and unsolicited communications. Subscribers and users of electronic communications services and networks can address complaints to the OCECPR and the DP Commissioner. The same applies for complaints with regard to electronic communications networks used for audio visual services. Improvements can be made for the effectiveness of the Cypriot legal framework. These consist in the better distinction of powers between the OCECPR and the DP Commissioner. Due to the fact that they both have concurrent powers, in practice this may hinder proper decision making (or may lead to unwillingness) because it is not clearly established internally which NRA will undertake a specific responsibility. Another problem is the co-decision powers afforded to both the DP Commissioner and the OCECPR. Most complaints end up being addressed to the DP Commissioner’s office instead of the OCECPR. Furthermore, due to the fact that they both have jurisdiction, decision-taking and the issuing of guidance papers is a timely procedure as it needs to be examined by both.
As regards unsolicited communications, provisions with regard to unsolicited communications are found in the Electronic Communications Law, as well as in the Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited Communications) of 28 January 2005 issued by the Electronic Communications Commissioner.
Part 2: Answers to the Questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

<table>
<thead>
<tr>
<th>Cyprus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Directive 2002/58/EC was transposed into Cypriot legislation by the Law Regulating Electronic Communications and Postal Services of 2004 (hereafter “the Electronic Communications Law”), and in particular Part 14 thereof.</td>
</tr>
<tr>
<td>- As regards data retention, Directive 2002/58/EC was partly transposed by the Data Retention and Processing Decree, No. 3/2007, issued on the basis of section 100 of the Electronic Communications Law. This Decree contains a specific reference to transposition of Directive 2002/58/EC. It was further partly transposed by the Retention of Telecommunication Data for Purposes of Investigation of Serious Criminal Offenses Law of 2007, N. 183(I)/2007 (the “Data Retention Law”). Even though this Law does not specifically mention which articles of the Directive were transposed, it mainly concerns security of data (Article 4) and confidentiality of communications (article 5). It should however be noted that this Law was found by the Supreme Court to be contrary to the Cyprus Constitution. [Cyprus Supreme Court (Civil applications 65/2009, 78/2009, 82/2009 and 15/2010-22/2010)]</td>
</tr>
<tr>
<td>- As regards unsolicited communications,</td>
</tr>
<tr>
<td>- provisions with regard to unsolicited communications are found in the Electronic Communications Law, section 106.</td>
</tr>
<tr>
<td>- relevant provisions are found in the Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited Communications) of 28 January 2005, No. 34/2005, which was issued by the Electronic Communications Commissioner pursuant to the provisions of section 106 of the Electronic Communications Law.</td>
</tr>
<tr>
<td>- relevant provisions are also found in the Decree on Legal Persons (Recording of Data in Public Telephone Catalogues), No. 35/2005, which was issued by the Electronic Communications Commissioner pursuant to the provisions of section 105 of the Electronic Communications Law.</td>
</tr>
<tr>
<td>- It should be noted that the Law on the Processing of Personal Data (Protection of the Individual) of 23 November 2001, Law No. 138(I)/2001, as amended by the Processing of Personal Data (Protection of the Individual) (Amending) Law of 2 May 2003, Law No. 37(I)/2003 and the Processing of Personal Data (Protection of the Individual) (Amending) Law of 11 July 2012, Law No. 105(I)/2012 (collectively, the “Data Protection Law”) is also relevant as regards general data protection. This Law implemented Directive 95/46/EC. The Data Protection Law which establishes the Data Protection Commissioner and</td>
</tr>
</tbody>
</table>
its office and by means of the Electronic Communications Law the Data Protection Commissioner is given joint powers on matters regulated by Directive 2002/58/EC.

- The Law on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce and Associated Matters of 2004, Law No. 156(I)/2004 as amended (the Electronic Commerce Law) also contains provisions regarding commercial communications and electronic mail. However, there is no reference in this law as to harmonisation with the ePrivacy Directive.

### Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into Cyprus law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2 (Definitions)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 4</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">http://www.cylaw.org/nomoi/indexes/2004_1_112.html</a></td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 2</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">http://www.cylaw.org/nomoi/indexes/2004_1_112.html</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrpr&amp;lang=gr">http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrpr&amp;lang=gr</a></td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 99 &amp; 100 (1)</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">http://www.cylaw.org/nomoi/indexes/2004_1_112.html</a></td>
</tr>
<tr>
<td></td>
<td>Retention of Telecommunication Data for</td>
<td>Greek <a href="http://www.cylaw.org/nomoi/arith/200">http://www.cylaw.org/nomoi/arith/200</a></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 100 (1)(b)</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">link</a> English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrp&amp;lang=gr">link</a></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 98A and 99</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">link</a> English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrp&amp;lang=gr">link</a></td>
</tr>
<tr>
<td>Art. 6 (Traffic data)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 100</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">link</a> English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrp&amp;lang=gr">link</a></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 101</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">link</a> English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrp&amp;lang=gr">link</a></td>
</tr>
<tr>
<td>Art. 13 (Unsolicited communications)</td>
<td>Law Regulating Electronic Communications and Postal Services of 2004, Law No. 112(I)/2004 as amended, section 106</td>
<td>Greek (consolidated law with all amendments) <a href="http://www.cylaw.org/nomoi/indexes/2004_1_112.html">link</a> English (only the original law) <a href="http://www.ocecpr.org.cy/nqcontent.cfm?a_id=767&amp;tt=ocecrp&amp;lang=gr">link</a></td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- the full name in your national language
- the English translation of the short name
- the part or the provision(s) of the ePrivacy Directive it supervises
- URL link to website

| Cyprus |
|-----------------|-----------------|-----------------|-----------------|
| **Full name of the authority** | **English translation of the short name** | **The part or provision(s) it supervises** | **URL link to website** |
| Office for the Commissioner of Electronic Communications and Postal Regulation | OCECPR | All provisions transposed in the Electronic Communications Law | [http://www.oecpr.org.cy](http://www.oecpr.org.cy) |
| Office of the Commissioner for Personal Data Protection | DP Commissioner | All provisions having an impact on privacy or data protection | [http://www.dataprotection.gov.cy](http://www.dataprotection.gov.cy) |

**Explanation:**

- The Office for the Commissioner of Electronic Communications and Postal Regulation ([http://www.oecpr.org.cy](http://www.oecpr.org.cy)) (‘OCECPR’) is the Cypriot NRA regulating the electronic communications sector and is one of the two supervisory authorities for the provisions transposing the ePrivacy Directive which have been inserted into the Cypriot Electronic Communications Law.

- The other supervisory authority is the Office of the Commissioner for Personal Data Protection ([http://www.dataprotection.gov.cy](http://www.dataprotection.gov.cy)) (DP Commissioner). The Electronic Communications Law affords co-decision powers to the DP Commissioner to regulate data protection matters and as far as the provisions transposing the ePrivacy Directive are related to privacy and personal data protection.

- Subscribers and users of electronic communications services and networks can address complaints to the OCECPR and the DP Commissioner. The same applies for complaints with regard to electronic communications networks used for audio visual services.

- The provisions with regard to unsolicited direct marketing communications, transposed in the Electronic Commerce Law are supervised by the OCECPR and the DP Commissioner.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Section 4 of the Electronic Communications Law defines **electronic communication networks** as “transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.” Networks used for the purpose of transmitting signals are included in this definition.

Section 4 of the Electronic Communications Law contains a definition of **“public communications network”** which means an electronic communications network which is used to provide publicly available electronic communications services which support the transfer of communications between network termination points.

Section 4 of the Electronic Communications Law contains a definition of an **“electronic communication service”**: “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing content transmitted using electronic communications networks and services or exercising control over such content; it does not also include information society services, as defined in Annex 1 of Procedure for the Provision of Information in the field of technical standards Law which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Section 4 of the Electronic Communications Law further defines the concept of **“operator”**. This definition is important because many provisions of the Law are explicitly addressed to “operators”. An “operator” means an undertaking providing or authorised to provide a public communications network or an associated facilities. In addition, there is a definition of the term “public electronic communications network provider” which means a person who is authorised to provide a public electronic communications network. Finally, Section 4 of the Electronic Communications Law contains a definition of a "universal electronic communications service provider" which means the public provider or providers of an electronic communications network, which are designated by way of a law or under a law as providers of a universal electronic communications service or part of it in Cyprus.

Where the processing of personal data is concerned, the provisions of the Data Protection Law which transpose the provisions of Directive 95/46/EC also apply.

Finally it should be noted that as regards the Electronic Commerce Law, it contains certain definitions concerning service providers, however, this law was not adopted or amended in order to transpose the provisions of the ePrivacy Directive, although it is generally applicable to providers of information society services established in Cyprus.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

Section 4 of the Electronic Communications Law contains a definition of "voice telephony service" which means a service to which the public has access for the commercial provision and direct transport of real time speech via the public switched network or network such that any user can use equipment connected to a network termination point at a fixed location to communicate with another user of equipment connected to another termination point. As a result, voice services fall within the scope of implementing legislation.

It should also be noted that VoIP consists of electronic communications and must be authorized by the OCECPR according to the provisions of the decision of the terms and conditions of general authorizations, PI 436/2005 and the Order of the Cyprus numbering plan, PI 850/2004. The Decision contains the terms that may be imposed by the Commissioner on the providers of networks and / or services, according to the General Authorisation that they hold. Annex I to that Decision contains the General Conditions, Annex II contains the Terms for Networks, Annex III contains the Terms of Service

Webmail could fall within the scope of the definition of “electronic mail” provided by the Electronic Communications Law. “Electronic mail” as any message consisting of text, voice, sound or image sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient. This definition is broad and intended to be “technology neutral.” Any message by electronic communications where the simultaneous participation of the sender and the recipient is not required is covered by this concept of electronic mail.

There is no mention of location based services in the applicable law and it is not clear what types of services are included in this term. Therefore, it is not clear whether they actually fall within the scope.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The Electronic Communications Law specifically provides that “...the provisions of this Law constitute the framework for the regulation of electronic communications networks and services that are provided by persons within the territory of the Republic of Cyprus”.

It should be noted however that according to section 102 of the Law relating to Calling and connected-line identification, it is provided that:

“102.(1) Where the presentation of calling-line identification is offered, the calling user shall be able by a simple means and free of charge, to eliminate this function on a per-call basis. The calling subscriber will have this possibility per calling line.

... (5) The provisions of subsection (1) apply also with respect to calls from Cyprus to other countries outside the Member States of the European Union and the provisions of paragraphs (2), (3) and (4) apply also with respect to incoming calls which originate from other countries outside the European Union.”

Therefore, there is a territorial limitation on the application of the Law which only affects the provision of electronic communications networks and services in the Republic of Cyprus and it is deemed that the Law does not affect operators outside of the national territory.

As regards privacy and personal data protection issues on which the Data Protection Law applies and for which the DP Commissioner has powers on the basis of the Electronic Communications Law, this Law also has a territorial limitation. According to section 3(3) of this Law, it is provided that:

“(3) This Law shall apply to any processing of personal data, where this is performed:
(a) by a controller established in the Republic or in a place where Cyprus law applies by virtue of public international law;
(b) by a controller not established in the Republic who, for the purposes of the processing of personal data, makes use of means, automated or otherwise, situated in the Republic, unless such means are used only for purposes of transmission of data through the Republic. In such a case, the controller must designate, by a written statement submitted to the Commissioner, a representative established in the Republic, who is vested with the rights and undertakes the obligations of the controller, the latter not being discharged of any special liability.”
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

<table>
<thead>
<tr>
<th>a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. The OCECPR has issued a number of decisions on the definition of an “operator with significant market power” taking into account the provisions of, inter alia, Directive 2002/58/EC. (E.g. decision 26/2006, 27/2006, 28/2006 etc.). Other than this the OCECPR has not issued any guidance papers on the aforementioned definitions. The OCECPR general issues Decisions and Decrees on relevant matters.</td>
</tr>
</tbody>
</table>

   The DP Commissioner has issued 2 guidance/directions on the use of the Internet which contain some definitions on the above:


   and


<table>
<thead>
<tr>
<th>b. national courts through rendering of case law</th>
</tr>
</thead>
</table>
| b. The Supreme Court of the Republic of Cyprus has dealt with a number of cases, mainly concerning applications for judicial review of the decisions of the OCECPR on the basis of Articles 146 of the Constitution which provides authority to the Court to annul or uphold decisions of the OCECPR (administrative review). These decisions mainly deal with the decision of the OCEPR to declare a specific operator as an “operator with significant market power” (see for instance OCECPR v. CYTA (2011) 3 AAD 756)

   http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_3/2011/rep/2011_3_0756.htm&qstring=%E7%EB%E5%EA%F4%F1%EF%ED%E9%EA*%20and%20%F5%F0%E7%F1%E5%F3%E9* )
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The Electronic Communications Law and the relevant Decrees issued on the basis of the Law are sufficiently clear as to their wording and quite appropriate for protecting privacy in Cyprus. Furthermore, it should be noted that there are a number of other Laws and secondary legislation which also protect privacy and which afford additional protection to individuals, coupled with the provisions of the Constitution of the Republic. For instance Articles 15 and 17 of the Constitution afford the right to privacy and secrecy of correspondence. Article 17 was amended in 2010 in order to afford extra privacy protection. Article 15 is modelled after Article 8 of the European Convention of Human Rights. Furthermore, the Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996 also forms an effective basis for protecting privacy. Finally, the right to privacy has been the subject matter of a number of decisions of the Cyprus Courts which have upheld that this is a fundamental principle.

   b. The improvements that can be made for the effectiveness of the Cypriot legal framework consist in the better distinction of powers between the OCECPR and the DP Commissioner. Due to the fact that they both have concurrent powers, in practice this may hinder proper decision making (or may lead to unwillingness) because it is not clearly established internally which NRA will undertake a specific responsibility.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Section 99(1) of the Electronic Communications Law entitled “Confidentiality of communications” provides that public electronic communications network and/or services providers as well as their employees, must take the appropriate technical and organisational measures to safeguard the confidentiality of any communication carried out through electronic communications networks and publicly available electronic communications services as well as relevant traffic data.

Section 99(2) and (3) provide that no person, other than users communicating between themselves from time to time, shall be allowed to listen to, tap, store, intercept and/or undertake any other form of surveillance of communications and relevant traffic data without the consent of the users concerned, except in the case of interceptions of communications in circumstances provided for by the law and with the authorisation of a Court.

According to section 99(4) the above provisions do not affect any legally authorised recording of electronic communications and traffic data in the course of lawful business practice, for the purpose of providing evidence of a commercial transaction and/or of any other business communication.

Section 99(5) provides that the storage of information or gaining access to information already stored in the terminal equipment of a subscriber or user is only allowed on the condition that the subscriber or user concerned has given his consent in accordance with the provisions of the Data Protection Law for the purposes of processing. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Article 5.2 of the ePrivacy Directive is implemented by section 99(4) which provides that despite the provisions of section 99(2) and (3) (see above under question 1) any legally authorised recording of electronic communications and traffic data in the course of lawful business practice, for the purpose of providing evidence of a commercial transaction and/or of any other business communication is permitted.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996 also prohibits the “Interception of a communication.” This is defined as the aural or any other form of receiving the content of any private communication with the use of any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine. This includes the hearing, magnetic taping or any other form of registration or reception of the content of this communication either in whole or in part or with regards to its substance, meaning, importance, or aim.

According to the above Law, a person shall be guilty of an offense and shall be liable to imprisonment up to three years if he:

- Taps or intercepts or attempts to tap or intercept or causes or allows or authorizes any other person to tap or intercept any private communication, on purpose;
- Uses, attempts to use, instigates or causes or authorizes another person to use or to attempt to use any electronic, mechanical, electromagnetic, acoustic or other apparatus or machine in order to tape or intercept any private communication, on purpose;
- Intentionally reveals or attempts to reveal to any another person the content of any private communication while being aware or having reason to believe that the information was received by bugging or interception of private communication; or
- Intentionally uses or attempts to use the content of any private communication, when being aware or having reason to believe that the information was received by tapping or intercepting of a private communication.

There are numerous exemptions. For example, the above provisions do not apply with regards to a person who:

- Intercepts private communication after an authorization or approval, or with bona fide assists another person in intercepting a private communication where she has reasonable cause to believe that they are acting under authorization or approval;
- Intercepts the private communication of persons communicating with third parties in prison; or
- Has received any information in relation to the interception of private communication or its content or testimony arising from such an interception, and reveals its content while testifying as a witness at any criminal or civil procedure before the competent court, provided that this interception took place according to the authorization or approval granted by CYTA or another authority.

Furthermore, the provisions above also do not apply if the monitoring is conducted with the prior express consent of both the caller and the recipient of the communication or, in the case of immoral, disturbing or threatening anonymous telephone conversations, the consent of either one of the two parties.

Finally, the provisions of Article 17 of the Constitution are relevant where confidentiality and secrecy of correspondence. Article 17 was amended on June 4, 2010, by Law 51(I) of 2010 (the “Sixth Amendment of the Constitution”) and currently provides that:

(1) “Every person has the right to respect for, and to the secrecy of, his correspondence and other
(2) “There shall be no interference with the exercise of this right except in the following cases:

(a) convicted and non-convicted prisoners;

(b) following a court order issued in accordance with the provisions of the law following an application by the Attorney General of the Republic and the intervention consists in a measure that, in a democratic society is necessary solely for the interests of the security of the Republic or for the prevention, investigation or sanctioning of certain serious crimes (such as murder, child pornography, trading in illegal drugs, etc.); and

(c) following a court order issued for the purposes of investigation of serious crimes sanctioned by imprisonment for a term exceeding five years and provided that the intervention concerns access to electronic communications traffic and location data and relevant data which is necessary for identifying the subscriber and/or user.”

The aforementioned amending Law provides that this amendment was enacted because according to the case law of the Supreme Court no person has the right, unless authorized by law for reasons prescribed by the Constitution, to monitor or interfere with the communications between citizens. In addition, the amendment was necessary in order to make possible an intervention that is necessary for securing the safety of the Republic as well as for preventing, investigating, or sanctioning serious criminal offenses.
4. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Electronic Communications Law does not explicitly address “automated breaches of confidentiality without human intervention” although such breaches of confidentiality may be considered as an infringement of section 99 of the Electronic Communications Law.

Furthermore, the Data Protection Law is also relevant where ‘processing of personal data’ is concerned because according to the definition of this term, it encompasses all operations that are performed upon personal data, whether or not by automated means, including the collection, recording organization, preservation, storage, alteration, extraction, use, transmission, dissemination or other form of disposal, connection combination blocking, erasure, or destruction. Therefore, if data is not processed in the manner provided by the Law, automated breaches may also be covered.

It should be noted that on the basis of the Electronic Communications Law, the OCECPR has issued the Legal Persons (Protection of Legal Interests with respect to Automated Communications) Order of 2005 (CEC Order 34/2005) which is related to automated calls and is to some extent related to breached of confidentiality by automated means without human intervention.

b. Please see the answer under question 3 above. The relevant legislation, apart from the Electronic Communications Law and the Data Protection Law, is the

- Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996
- Article 17 of the Constitution
### 5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

<table>
<thead>
<tr>
<th>a. the scope and substance of your national implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc.), and/or between the type of device (e.g. general computers, mobile phones, tablets)?</td>
</tr>
</tbody>
</table>

a. The Electronic Communications Law was amended in 2012 by amending Law N.51(I) of 2012 for the purpose of harmonising Cyprus law with:

- Directive 2009/136/EC
- Directive 2009/140/EC
- Regulation (EC) 1211/2009

A new definition was included in the Law of the term “consent” under section 4 of the Law:

"consent" means consent of the data subject, any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject, having been previously informed, consents to the processing of personal data concerning him;

In addition, section 99 of the Law was amended by including new subsection (5) described above which is similar to Article 5(3) of the Directive:

"99(5) The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his consent, having been provided with clear and comprehensive information, in accordance with the provisions of the Processing of Personal Data (Protection of Individuals) Law 2001 and 2003, inter alia, about the purposes of the processing. Provided that this shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

b. The provision quoted above doesn’t distinguish between types of cookies or between categories of end equipment.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. As mentioned under question 5 above, the Electronic Communications</td>
<td>The Electronic Communications Law was amended in 2012 by amending Law N.51 (I) of 2012. A new definition was included in the Law of the term &quot;consent&quot; under section 4 of the Law:</td>
</tr>
<tr>
<td>Law was amended in 2012 by amending Law N.51 (I) of 2012. A new definition</td>
<td>&quot;consent&quot; means consent of the data subject, any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject, having been previously informed, consents to the processing of personal data concerning him;</td>
</tr>
<tr>
<td>was included in the Law of the term &quot;consent&quot; under section 4 of the Law:</td>
<td>In addition, under section 99(5) of the Law which is similar to Article 5(3) of the Directive:</td>
</tr>
<tr>
<td>&quot;99(5) The storing of information, or the gaining of access to information</td>
<td>&quot;99(5) The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his consent, having been provided with clear and comprehensive information, in accordance with the provisions of the Processing of Personal Data (Protection of Individuals) Law 2001 and 2003, inter alia, about the purposes of the processing.</td>
</tr>
<tr>
<td>concerned has given his consent, having been provided with clear and</td>
<td></td>
</tr>
<tr>
<td>comprehensive information, in accordance with the provisions of the</td>
<td>There are no other specific requirements in the Electronic Communications Law itself as to the type of informed consent that needs to be provided.</td>
</tr>
<tr>
<td>Processing of Personal Data (Protection of Individuals) Law 2001 and</td>
<td>It should be noted that the DP Commissioner has indicated that the Article 29 Working Party's opinion on the cookie consent exemption (WP194) and the working document providing guidance on obtaining consent for cookies (WP208) can be used as guidance on the use of cookies (<a href="http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/8CBF6E0E97A198EDC2257C43002477BA?OpenDocument">http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/8CBF6E0E97A198EDC2257C43002477BA?OpenDocument</a>)</td>
</tr>
<tr>
<td>2003, inter alia, about the purposes of the processing.</td>
<td></td>
</tr>
</tbody>
</table>
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The provisions of section 99(5) of the Electronic Communications Law are relevant, according to which:

"99(5) The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his consent, having been provided with clear and comprehensive information, in accordance with the provisions of the Processing of Personal Data (Protection of Individuals) Law 2001and 2003, inter alia, about the purposes of the processing.

Provided that this shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

It should be remembered that the DP Commissioner has been given joint powers with the OCECPR to decide on possible violations and complaints regarding section 99(5) of the Electronic Communications Law. The DP Commissioner has given some guidance on the matter of cookies and on informed consent (see: the DP Commissioner’s website: (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/8CBF6E0E97A198EDC2257C43002477BA?OpenDocument)

According to the DP Commissioner, cookies are small text files stored on users’ computers during their "visits" at various websites on the World Wide Web, for the purpose of enabling a website to identify the user during his subsequent visits to the same website. More particularly, they provide personalized services such as, for example, users can choose the language in which they prefer to look at a website and this preference is stored so that they do not have to re-select the language during their next visit to the same website. Cookies are also used in the well-known «shopping cart» where the user can store various products which he intends to purchase and return at a later time to purchase same. Apart from the above uses, cookies can be used to track the movements of users on the internet to form a profile of their preferences in order to present their advertisements that users are likely to find attractive.

Following Directive 2009/136/EC, Article 5(3) of the basic Directive 2002/58/EC, was introduced concerning cookies which requires that websites that make use of cookies should receive the prior consent of the user, after informing users on how cookies will be used.

On the basis of the amending Directive and section 99(5) of the Electronic Communications Law, consent is not required for any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the
subscriber or user to provide the service”.

Finally, the DP Commissioner’s website states that Article 29 Working Party’s opinion on the cookie consent exemption (WP194) and the working document providing guidance on obtaining consent for cookies (WP208) can be used as guidance on the use of cookies:


8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The Electronic Communications Law is compatible as regards its wording with the Directive. In practice, no statistics on compliance have been located. No enforcement actions have been located. It is expected the OCECPR and the DP Commissioner will adopt relevant guidelines in the near future. Generally, websites in Cyprus are left free to decide whether to observe cookie rules as there are no relevant guidelines.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. It is expected the OCECPR and the DP Commissioner will adopt relevant guidelines in the near future.

   The DP Commissioner has given some guidance on the matter of cookies and on informed consent (see: the DP Commissioner’s website: [link]

   Following Directive 2009/136/EC, Article 5(3) of the basic Directive 2002/58/EC, was introduced concerning cookies which requires that websites that make use of cookies should receive the prior consent of the user, after informing users on how cookies will be used.

   On the basis of the amending Directive and section 99(5) of the Electronic Communications Law, consent is not required for any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

   Finally, the DP Commissioner’s website states that Article 29 Working Party’s opinion on the cookie consent exemption (WP194) and the working document providing guidance on obtaining consent for cookies (WP208) can be used as guidance on the use of cookies:

   [link]
   [link]

   b. Not available

10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The Electronic Communications Law simply reiterates the provisions of the ePrivacy Directive. However due to the fact that no specific guidance has been provided specifically on cookies, in practice it may be difficult for persons who are not familiar with the workings of the law to properly understand the requirements. From a strictly legal point of view the provisions are only applicable
to public providers of electronic communications networks under the scope of the Electronic Communications Law.

b. In practice a great number of websites have started introducing provisions in their privacy policies for cookies.
### C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 4 of the Electronic Communications Law defines ‘traffic data’ as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. This definition is the same as in the Directive.</td>
</tr>
<tr>
<td>The same section also contains a definition of the term ‘value added service’ as any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Section 100(1) of the Electronic Communications Law provides that traffic data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, should be erased or made anonymous at the end of a call when they are no longer required for the transmission, except in the following circumstances:

(a) for the purpose of subscriber billing and interconnection payments, where the following data are allowed to be submitted to processing:

(i) number of identification of the subscriber station;  
(ii) addresses of the subscriber and the type of station;  
(iii) total number of units to be charged for the accounting period;  
(iv) called subscriber number;  
(v) type, starting time and duration of the calls made and/or the data volume transmitted;  
(vi) date of the call/service;  
(vii) other such information as advance payments, payments made by instalments, disconnection and reminders.

The processing of the above data is permitted only up to the end of the period in which a bill may be lawfully challenged and/or payment pursued;

(b) provided that the subscriber or user consent that the data mentioned in paragraph (a) may be processed from an undertaking for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services. The subscriber or user has the right to withdraw at any time his/her consent for the processing of data traffic.

Section 100 (2)(a) provides that any processing of traffic and billing data shall be restricted to persons who act under the supervision of the persons who either handle billing and/or traffic, and/or with answers to customer enquiries, fraud detection and/or the marketing of electronic communications services or the provision of value added services.

For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process traffic and billing data to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers must be given the possibility to withdraw their consent for the processing of traffic data at any time.

Notwithstanding the above, the OECPR and the DP Commissioner may require persons to provide them any relevant information on traffic data which they have or will have, for the purpose of exercising their regulatory duties and competences for the control of compliance of the said persons with the provisions of section 100(1) of the Law, respectively.

Subscribers have the right to receive non-itemised bills. The OECPR, following consultation with the DP Commissioner, shall prescribe by Decree the alternative modalities of communication among the associated users and called subscribers, in order to reconcile their respective rights to privacy.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

| Section 100(1) of the Electronic Communications Law provides that traffic data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by persons, should be erased or made anonymous at the end of a call when they are no longer required for the transmission, subject to the exceptions referred to in this section as mentioned under question 2 above. |
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

The OCECPR has issued the Decree on the Storage and Processing of Traffic Data, No. 3/2007 which provides for the obligation of all licensed providers of fixed and mobile telephony to store and process traffic data in accordance with section 100(1)(a) of the Electronic Communications Law, as regards their subscribers and/or users, for a period of 6 months for the purpose of, inter alia, billing, payment for interconnection and dispute resolution as regards the interconnection and charging.

(http://www.oucepr.org.cy/ncontent.cfm?a_name=search_1&tt=oucepr&lang=gr)
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

These rules appear to be effective in practice, especially in view of the aforementioned Decree which adds further guidance and obligations on service providers.
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 4 of the Electronic Communications Law defines &quot;location data&quot; as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.</td>
</tr>
<tr>
<td>The same section also contains a definition of the term ‘value added service’ as any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

According to section 101 of the Electronic Communications Law, where location data other than traffic data can be processed, such data may only be processed only when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

Where the consent of users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Processing of location data other than traffic data in accordance with the above must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

According to section 101 of the Electronic Communications Law, where location data other than traffic data can be processed, such data may only be processed only when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. The OCECPR has not issued any Decrees or other guidance concerning location data.

   b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

Section 100 is in line with the provisions of the Directive and could be said to sufficiently protect individuals because it concerns service providers in general. The only issue is that no guidance can be extracted from any specific secondary legislation that could specify the operation of this section even further.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. The Electronic Communications Law, section 4, defines “direct mail” as the dispatch of material consisting solely of advertising or marketing material and comprising an identical message, except for the addressee's name, address and identifying number as well as other modifications which do not alter the nature of the message, which is sent to a significant number of addressees, to be conveyed and delivered at the address indicated by the sender on the item itself or on its wrapping. The Commissioner of Electronic Communications and Postal Regulation shall determine the term “significant number of addressees” each time by decision. Bills, invoices, financial statements, and other non-identical messages shall not be regarded as direct mail. A communication combining direct mail with other items within the same wrapping shall not be regarded as direct mail. Direct mail shall include cross-border as well as domestic direct mail.

   Furthermore, it defines “electronic mail” as any message consisting of text, voice, sound or image sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient. This definition is broad and intended to be “technology neutral.” Any message by electronic communications where the simultaneous participation of the sender and the recipient is not required is covered by this concept of electronic mail.

   One could argue that the above definition could also comprise direct mail dispatched electronically.

   Furthermore, the Electronic Communications Law contains essentially similar provisions to Article 13 of the Directive as amended. More specifically, according to section 106 of the Law, the use of automated calling and communications systems without human intervention (automatic calling machines), fax machines or electronic mail, for the purposes of direct marketing is permitted only with respect to subscribers or users who have given their prior consent.

   Notwithstanding the above, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with the Data Protection Law, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

   The OCECPR, following consultation with the DP Commissioner takes the necessary measures in order to ensure that unsolicited communications for the purposes of direct marketing by means other than those referred to are not permitted without the consent of interested subscribers or users.
In any event, the practice of sending electronic mail for the purposes of direct marketing disguising or concealing the identity of the sender or the person on whose behalf the message is sent, in breach of the provisions of section 9 of the Electronic Commerce Law, or without a valid address to which the recipient may send a request that such communications cease, or encouraging recipients to visit webpages which breach the said section 9, are prohibited

The above provisions apply to subscribers who are natural persons. The OCEPR also has an obligation to ensure, within the framework of Community Law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected. As regards the protection of the legitimate interests of subscribers who are not natural persons with regards to unsolicited communications, the provisions of the Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited Communications) of 28 January 2005, No. 34/2005.

Finally, according to section 106, any natural or legal person adversely affected by infringements of this section and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. The OCECPR, following consultations with the DP Commissioner may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this section.

As regards the Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited Communications) of 28 January 2005, No. 34/2005, it defines the term “automated calls” as the telephone calls carried out without the consent of the called party. It also defines the term “automated communications” as the communications carried out through electronic communications networks carried out without the prior consent of the called party or of the recipient. These include voice telephony calls without human intervention (automatic calling machines), calls via facsimile machines (fax) or electronic mail as well as SMS messages.

The principal purpose of the Decree is to protect the lawful rights of legal persons with respect to automated calls made for the purpose of unsolicited commercial communications. The use of such automated calling systems without human intervention or other machines for the purpose of effecting automated calls for direct marketing purposes directed to subscribers is allowed only where the subscribers have given their consent or where they have declared to the sender that they wish to receive such calls.

Further to the above, other laws also refer to commercial communications, such as the DP Law, the Law on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce and Associated Matters of 2004 (Electronic Commerce Law).

The Data Protection Commissioner has also issued a Directive on the Processing of Personal Data via the Internet as well as a Directive on the Use of the Internet and of Mobile Telephones,57 which also relates to unsolicited commercial communications via the Internet and via the use of mobile phones.

b. National provisions, especially section 106 referred to above, are generally in line with the Directive and mostly use the same terminology with some more specific provisions, e.g. reference to the Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited Communications) of 28 January 2005, No. 34/2005
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

For the lawful sending of unsolicited messages through the use of automated calling and communications systems without human intervention (automatic calling machines), fax machines or electronic mail, for the purposes of direct marketing, subscribers or users must generally give their prior consent (section 106 of the Electronic Communications Law).

Similar requirements are contained in Decree 34/2005, referred to above, which provides that the use of such automated calling systems without human intervention or other machines for the purpose of effecting automated calls for direct marketing purposes directed to subscribers is allowed only where the subscribers have given their consent or where they have declared to the sender that they wish to receive such calls.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Section 15 of the Data Protection Law was amended in 2012 by Amending Law 105(I) of 2012, which essentially consists in an exception to the opt-in mechanism. Section as it stands today, permits the processing of personal data for the purpose of the promotion, sale of goods, or the provision of services at a distance, unless the data subject objects to such processing. For this purpose, the data controller must make this possibility easily available and free of charge, at least once.

Section 15A of the DP Law as amended also provides that political parties and candidates are permitted, for the purposes of political communication, send communication material as regards the promotion of their political position and their candidacy for a position, by using the names and addresses of persons listed in voters’ lists or telephone directories.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Electronic Communications Law, section 4, defines "electronic mail" as any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

This definition covers not only electronic mail through the internet, but also MMS/SMS/text messages, voice mail, etc., in line with the definition of “electronic mail” in the ePrivacy Directive.

Furthermore, as discussed above, according to section 106 of the Law, the use of automated calling and communications systems without human intervention (automatic calling machines) also covers fax and electronic mail that is used for direct marketing purposes.

Finally, according to the has also issued Guidance of the DP Commissioner on direct marketing or goods or services by electronic means (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/577FD8DA6F7F0506C2257914001DF315/$file/Direct%20marketing%20directions%202012.pdf?OpenElement), issued on the basis of section 106 of the Electronic Communications Law and section 15 of the Data Protection Law, the DP Commissioner specifically refers to direct marketing and unsolicited communications sent via email, fax and sms.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. According to the Guidance on the Processing of Personal Data via the Internet issued by the DP Commissioner, spamming and junk mail is prohibited. “Spamming” takes place where a large number of unwanted/unsolicited electronic messages are sent. Usually, such e-mails aim at advertising or direct marketing of products or services and may enclose dangers for recipients. For example, spam e-mails may mislead the recipient to pay an amount of money for participating in virtual vacation offers or large-scale fraud and may, in some cases, cause havoc to networks and computers due to their large volume.

The 2012 Annual Report of the Data Protection Commissioner indicates that it received 465 complaints about spam sent through emails, fax and SMS in 2011 and 251 in 2012. Most of these messages advertise a premium rate number for information about different subjects such as horse racing bets, sports bets, dating services, and horoscope. The said Annual report contains references to the manner in which complaints can be made and how recipients of messages can exclude themselves from the subscriber lists of advertising companies.

The DP Commissioner has also issued Guidance on direct marketing or goods or services by electronic means, on the basis of section 106 of the Electronic Communications Law and section 15 of the Data Protection Law.


b. In 2006 the Supreme Court heard a case between GOLDEN TELEMEDIA LTD v. DP Commissioner (Case no. 519/2006) regarding the application of the plaintiff for judicial review of the decision of the DP Commissioner which had imposed a fine to the plaintiff for breach of the provisions of the Data Protection Law as regards unsolicited mail. The decision of the Court does not really provide guidance on the rules with regard to unsolicited marketing communications but is mostly concerned with administrative matters, i.e. the manner in which the decision of the DP Commissioner should have been taken. In this case the DP Commissioner did not provide the plaintiff with the right to a proper hearing before issuing its decision on the imposition of a fine.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| In my view the rules are sufficiently clear and appropriate to protect privacy in Cyprus. The legislation enables both legal and natural persons to seek protection before the Cypriot NRAs. |
COUNTRY REPORT

CZECH REPUBLIC

For the Study

*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Radim Polcak, Masaryk University, Faculty of Law, Institute of Law and Technology

Date: 27 August 2014
Contents

Part 1: Management summary

Part 2: Answers to the questionnaire
Part 1: Management summary

Management summary for the Czech Republic:

The Czech transposition of the ePrivacy Directive can be summarized to two fundamental categories, i.e. legislative and operational.

- From the legislative point of view, the provisions of the ePrivacy Directive have mostly been transposed into the Czech legislative framework by their substantive translation and inserted either into the Electronic Communications Act or Certain Information Society Services Act. This method of transposition, although widely and frequently used, is far from ideal, as it often leads to copying and pasting formulations that do not really fit into the existing regulatory framework.

- Moreover, in the case of the ePrivacy Directive, the respective provisions had to be split into two relatively different regulatory regimes, i.e. data protection and electronic communications. One of the obvious results of this split is the absence of particular sanctions for some breaches of protection of personal data within the framework of electronic communications. Instead, just general investigative and enforcement rules of data protection apply, which makes it practically impossible for the Czech Telecommunication Authority to engage in any specific enforcement actions.

- The only true legislative mismatch between the Directive and Czech statutory law was noted with regard to the opt-in regime for cookies: the Czech regulatory regime instead uses (probably by a legislative mistake or omission) the opt-out principle combined with relatively vaguely defined information duties.

- As to the operational mode of the transposition, we noted problems mostly caused by the aforementioned split of the subject matter under different parts of the Czech legal system. As a result, a number of specific provisions with regard to the protection of personal data in electronic communications are not practically efficient, as actual investigations and sanctioning takes places mostly under general data protection rules.

- We also noted that the practical application and enforcement of provisions transposing the ePrivacy Directive is done mainly by the Office for Personal Data Protection (the Czech DPA). There is a number of informal guidelines as well as actual proceedings (mainly in anti-spam matters). However, it seems that specifically in the case of anti-spam provisions, the ePrivacy Directive created a relatively large administrative burden with less than significant final effects.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC should have been implemented in the national legislation at the time the Czech Republic joined the EU. However the old Telecommunication Act of 2000 (act no. 151/2000 Sb., on the telecommunications and amendments of some acts) did not include any provisions harmonising the Directive.

- The Directive was finally implemented by the Act no. 127/2005 Sb., on electronic communications and by amendments of some related acts (Electronic Communications Act). This includes all provisions prescribed by the Directive (in the scope of this report) except those regulating unsolicited communication. This has been in force since 1st May 2005.

- Unsolicited communications are regulated in act no. 480/2004 Sb., on certain services of information society and change of some acts (Certain Information Society Services Act). It has been in force since 1st August 2006.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 3 (Scope)</td>
<td>The exact wording of this article was not transposed. However, it can be found in general provisions of Electronic Communications Act (art. 1 and art. 87, which are general provisions of Head 5 that is devoted to privacy in electronic communications) and Certain Information Society Services Act, art. 1.</td>
<td><a href="http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&amp;fulltext=&amp;nr=127~2F2005&amp;part=&amp;name=&amp;rpp=15#local-content">Link</a> (Electronic Communications Act) <a href="http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=58329&amp;fulltext=&amp;nr=480~2F2004&amp;part=&amp;name=&amp;rpp=15#local-content">Link</a> (Certain Information Society Services Act)</td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Electronic Communications Act, art. 90 para. 5</td>
<td><a href="http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&amp;fulltext=&amp;nr=127~2F2005&amp;part=&amp;name=&amp;rpp=15#local-content">Link</a></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Electronic Communications Act, art. 89 para. 3.</td>
<td><a href="http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&amp;fulltext=&amp;nr=127~2F2005&amp;part=&amp;name=&amp;rpp=15#local-content">Link</a></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Electronic Communications Act, art. 91</td>
<td><a href="http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&amp;fulltext=&amp;nr=127~2F2005&amp;part=&amp;name=&amp;rpp=15#local-content">Link</a></td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- the full name in your national language
- the English translation of the short name
- the part or the provision(s) of the ePrivacy Directive it supervises
- URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant professional self-governing chamber established by a statut</td>
<td>e. g. - Czech Bar Association - The Notarial Chamber of the Czech Republic - The Czech Physician Association</td>
<td>Unsolicited communications – within the Chamber</td>
<td>e. g. <a href="http://www.cak.cz">http://www.cak.cz</a> <a href="http://www.nkcr.cz/ww/LKCR">http://www.nkcr.cz/ww/LKCR</a></td>
</tr>
</tbody>
</table>
Explanation:

Note: It is quite common in the Czech Republic that there is a distinction between state bodies that are responsible for drafting of statutory legislation and bodies that engage in its executive implementation. Therefore, the following list includes also two ministries that, although having no immediate executive powers in the course of executive implementation of particular regulatory provisions, are responsible for the transposition of the ePrivacy Directive into the national law. Apart the institutions mentioned above, it is possible to mention also other institutions and organizations that might partially engage in controlling and reporting particular operational defects and omissions within the scope of the ePrivacy Directive like the Office of the Public Defender of Rights (the ombudsman), Czech Trade Inspection Authority, the Czech Advertising Standards Authority etc. These institutions, however, do not have any direct official competences with regards to statutory provisions harmonized upon the ePrivacy Directive, so they are not mentioned in particular.

The competence of the Ministry of Industry and Trade (http://www.mpo.cz/default_en.html) in the field of electronic communications is described in art. 105 of Electronic Communications Act.

“Art. 105:
(1) The Ministry
a) submits to the Government draft proposal of the electronic communications policy of the State and monitor the implementation thereof;
b) submits to the Government the proposals for the main principles of the policy of the State in electronic communications;
c) pursues international relations in the electronic communications area at the levels of Governments, Government agencies and non-governmental organisations, except the relations for the pursuance of which the Government authorised the Office;
d) ensures that obligations in the electronic communications area are fulfilled as ensuing from the international treaties binding on the Czech Republic and published in the Collection of Laws or Collection of International Treaties; ensure the same in respect of the obligations resulting from the Czech Republic’s membership of international organisations, except the obligations carried out by the Office in cases determined by the Government;
e) carries out the state statistical service;
f) co-operates with Member States’ ministries in the area of electronic communications;
g) notifies the Commission about the regulatory authorities in the electronic information area and provides other information if the Commission so requests;
h) within the range of its activity, represents the Czech Republic on the European Union bodies.
(2) In performing its activities, the Ministry shall also rely on the relevant decisions, recommendations and positions issued by the bodies of the Communities and the basic principles of the policy of the State in the electronic communications area. If the Ministry decides not to proceed in accordance with the Commission’s recommendations harmonising the implementation of Community legislation in the electronic communications area, it shall inform the Commission to that effect without delay and shall justify such conduct.”

The Ministry is also responsible for drafting of statutory legislation which incorporates provisions of Directive 2002/58/ES into the Czech legal system. It is also responsible for the creation of general implementation policies, white papers etc. and it bears general political responsibility for public policies in electronic communications (contrary to that, Czech
Telecommunication Office is not regarded as a political body.

The competence of Czech Telecommunication Office (http://www.ctu.eu/main.php?pageid=178) is described in art. 108 of Electronic Communications Act. It is an executive and supervising body in which’s authority fall almost all provisions of the Electronic Communications Act. The exceptions are provisions concerning personal data protection. As is stated in art. 87 para. 3 of the Electronic Communications Act, supervision over compliance is allocated to the Office for personal data protection (http://www.uoou.cz/en/), which is an executive and supervision body in the field of personal data protection.

Art. 87 para. 3 of the Electronic Communications Act:
“Supervision over compliance with the obligations in processing personal data according to this Act shall be provided by the Office for Protection of Personal Data in accordance with a special legal regulation.”

Within the authority of the Office for personal data protection also fall provisions on unsolicited communications, as is stated in art. 10 para. 1 of Certain Information Society Services Act:
“The authority competent to carry out supervision of compliance with the present act (hereinafter referred to as “supervisory authority”) shall be a) the Personal Data Protection Office, in relation to the dissemination of commercial communications under Art. 7; b) the relevant professional self-governing chamber established by statute, in relation to obligations arising out of Art. 8 paragraph 3.”

As can be seen, there is an exception for professional self-governing chambers, which are established by a statute. Art. 8 para. 3 reads as follows:
“Commercial communications from persons exercising a regulated profession must contain the name of the professional self-governing chamber established by statute with which the person exercising a regulated profession is registered, a reference to the professional rules applied in the member state of the European Union in which the person exercising a regulated profession is established, and the manner of permanent access to information about the relevant professional self-governing chamber established by statute which the person exercising a regulated profession is a member of.”

Note: For the English version of the Czech Electronic Communications Act we use an official translation, which is available at the web page of The Ministry of Industry and Trade (http://www.mpo.cz/dokument75810.html).
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Electronic communications network is defined in art. 2 under h) of Electronic Communications Act as “transmission systems and, where applicable, switching or routing equipment and other facilities that permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed circuit-switched or packet-switched networks and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for broadcasting, and cable television networks, irrespective of the type of information conveyed” which is the same definition as is in directive 2002/21/EC, and therefore it is within the scope of the ePrivacy Directive.

The Law distinguishes between “public” and “non-public” networks. A “public” network is defined by art. 2 under j) of Electronic Communications Act as: “an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services and supporting transmission of information between network terminal points; or an electronic communications network by which is provided a television or radio broadcasting service.” The difference between the definition of Directive 2002/21/EC and the Czech Electronic Communications Act is in specific inclusion of electronic communications network by which is provided a television or radio broadcasting service into the public network definition.

Electronic communication service is defined in art. 2 under n) of Electronic Communications Act as “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, and on cable television networks, but excluding services that offer content by means electronic communications networks and services, or exercise editorial control over the offered content transmitted using electronic communications networks and services; it does not include information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.” This definition is roughly the same as the one of the Framework Directive.

The law recognizes “publicly” and “non-publicly” available services. Publicly available electronic communications service is defined by subparagraph o) of the same article as “electronic communications service from the use of which no person is excluded beforehand.” This definition goes beyond Directive 2002/21/EC, and is included for a better understanding of the terms used (it is used as a part of public network definition).

A provider is named an “operator” and is defined in art. 2 under e) as: “an undertaking providing or authorised to provide a public communications network or associated facilities.” Provision of an electronic communications network is defined in the letter f) of the same article as “establishment, operation, supervision or making accessible of such a network.” This concept directly transposes the Framework Directive.
The answer to this question depends on two factors. The first factor is the interpretation of the term “service which consists wholly or mainly in the conveyance of signals on electronic communications networks”. The second factor is whether the service is provided by an operator (a legal body which fits into the legal definition of ‘operator’ as described under Question 3, above) or not. This means the same service may or may not be regarded as an electronic communications service, depending on whether the provider is an operator (then it is an electronic communications service) or not (then it would be an information society service). There is a significant number of rulings in competence disputes by The Supreme Administrative Court of the Czech Republic, deciding whether the service in dispute is an electronic communications service (which means it is in the competence of Czech Telecommunication Office), or not (which means it is in the competence of general courts).

The question of classification of aforementioned ISPs is, however, of more general nature as it involves the overall distinction between services of information society and services of electronic communications. In the first case, the definition used in Act No. 480/2004 Sb. basically copies the definition used by the eCommerce Directive by a reference to Art. 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition of electronic communication services in the Electronic Communications Act then practically copies the definition used in Art. 2(a) of the Framework Directive. Therefore, any further development in the general distinction between the classification of information society providers and electronic service providers might also affect the classification of aforementioned services.

A pragmatic distinction (i.e. distinction upon factual regulatory effects) might be drawn according to the existence of a license – while there is no general licensing obligation for providers of information society services (apart from general requirements regarding registration and operation of business units), licenses are required for providers of electronic communication services. Consequently, if the respective business unit holds a license or is so obliged, it is a subject to the competence of the Czech Telecommunication Office. If not, only the general competence of the Office for Personal Data Protection applies.

VoIP falls within the scope of the implementing legislation. While it is not specifically mentioned in the text of the law, the Czech Telecommunication Office issued a decision, stating that VoIP generally falls under the provisions of the Electronic Communications Act (online, in Czech: [http://www.ctu.cz/cs/download/aktualni_informace/zprava_voip_12-2010.pdf](http://www.ctu.cz/cs/download/aktualni_informace/zprava_voip_12-2010.pdf)). However, this is subject to the condition that the service provider must be an operator in the meaning of Electronic Communications Act.

With regard to location based services, it depends on whether the service itself is provided by an operator (e.g. when a telephone operator provides location data based on cell base station it is an electronic communications service) or not (GPS service provider). Our opinion is that the situation is similar in case of other services.

The services at stake are mostly regarded by Czech law as ‘information society services’, while in
certain specific cases (when both aforementioned conditions are met) they can be at the same time regarded as ‘electronic communications services’. However, there is no significant difference between those two situations with regards to the issues of ePrivacy Directive, whereas they both always fall under the competence of the Office for Personal Data Protection. The most problematic difference between the aforementioned two types of service providers, on which significant Czech case-law is available, mostly concerns the solution of disputes between providers and users, which however, falls outside the scope of this report.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

A person intending to provide services in the field of electronic communications in the Czech republic has a duty to prior notify such intent to the Czech Telecommunication Office (art. 13 of the Electronic Communications Act). The law assumes (in art. 13, paragraph 3) that such a legal person (corporate unit) has its place of establishment in the Czech Republic. Consequently, the Czech law practically applies on all operators active on the Czech market simply through its standard territorial jurisdiction. It also means that operators with their place of establishment outside the Czech Republic cannot access the Czech market unless they are officially established there.

Operators regularly process data of their clients, which means they are also regarded as personal data controllers according to the Personal Data Protection Act. Even though their main place of establishment is in another country, they fall under the competence of the Czech Office for Personal Data Protection due to the current interpretation of the CJEU in ‘Google Spain.’

A different situation might occur should the operator be a natural person. However, since there is no such example on the Czech market of electronic communications, we consider this topic practically irrelevant.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>No relevant guidelines or official interpretations regarding the interpretation and / or application on the (scoping) of definitions mentioned in this section is noted.</td>
</tr>
<tr>
<td>b.</td>
<td>There is a landmark decision no. Konf 24/2013-14 rendered by the joint Competence Senate consisting of selected members of the Supreme Court and Supreme Administrative Court. This case concerned a conflict of competences over an unpaid bill for mobile communication services that also contained adjacent services paid through special SMS services (like transportation tickets). The question was whether providing these extra services which do not consist of electronic communications but are technically provided through mobile networks (transportation tickets are paid as a matter of an SMS and the ticket is delivered in the form of an SMS to a mobile communication device of the consumer) are to be regarded as electronic communication services and consequently whether disputes arising of their provision should be decided in first instance by the Czech Telecommunication Office. The Competence Senate ruled that the fact that an adjacent service is provided and paid through electronic communication service does not make it a part of that service – consequently, the Czech Telecommunication Office was successful in its claim for keeping only its jurisdiction over pure electronic communication services, while any other matters (incl. adjacent services) are to be decided in first instance by general courts as a matter of civil litigation.</td>
</tr>
</tbody>
</table>
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

| a. | It can be in some cases not entirely clear, which service is to be regarded as an electronic communication service or an information society service. However, that question is rather theoretical, as the Office for Personal Data Protection has its administrative jurisdiction over both types of services. The only differentiation that really matters is thus between publicly available electronic communication service, whose operators have to fulfil privacy protection duties stated in art. 88 of the Electronic Communications Act, and providers of (only) information society services that are not bound by this provision. The distinction of information society services and electronic communication services causes confusion namely with regards to the competences of the Czech Telecommunication Office – in result, it does not happen in practice that the Office would investigate and sanction breaches of specific duties in data protection. It is however quite disputable whether and how to clarify this situation – at the moment, it is theoretically possible that simultaneous existence of these competences at the Czech Telecommunication Office and the Office for Personal Data Protection makes it possible for both authorities to cooperate and to use their specific knowledge and investigative tools together with their special competences. This, however, does not happen in everyday practice. |
| b. | The most significant systematic problem of the consistency of national implementation of the ePrivacy directive is the fact that they need to be split into two relatively different parts of Czech statutory law. Consequently, one set of issues tackled consistently in the ePrivacy Directive needed to be harmonised using at least two different regulatory regimes in three different and to a large extent independently existing branches of Czech law which has resulted in an incoherent national legal framework. In our view, the situation would greatly improve if the substance of the ePrivacy Directive wouldn’t form a specific regulatory instrument, but is either included in the EU regulatory framework of electronic communications or in the data protection legislation. |
### B. Confidentiality obligations

1. **How was the principle of confidentiality of communications and the related traffic data (Art. 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?**

   Art. 89 para. 1. of the Electronic Communications Act states:

   “The undertakings providing public communications networks or publicly available electronic communications services shall ensure the technical and organisational measures to safeguard the confidentiality of the messages and the traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided by law. This shall not prevent the technical storage of data as needed for message transmission without affecting the confidentiality principle.”

   The duty of providing a secure environment for electronic communications relies on operators.

   Czech legislation uses the term “zpráva” for “Communication”, which can be translated as a “message” and is defined in art. 89 para. 2 as:

   “Message means any information being exchanged or transmitted between a finite number of subscribers or users via the publicly available electronic communications service, except for the information transmitted as part of the public audio or television broadcasting via the electronic communications network, unless it can be allocated to an identifiable subscriber or user receiving that information.”

   This definition is the same as is the one in the ePrivacy directive.

   The Electronic Communications Act does not include any provisions imposing sanctions in case of breach of the rules. Consequently, breach of confidentiality would be considered under the general sanction regime of the Data Protection Act and/or of the protective provisions regarding privacy and personality under the Civil Code (act no. 89/2012 Sb.) In cases of specific importance (namely when significant harm is caused fraudulently), the Criminal Code might apply as well as ultima ratio (see below question no. 4 b of this section).
2. Art. 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

| The Business exception is only partly transposed into the Czech legal system. It enables only the use of traffic data, and not the recording of the communication itself. This rule can be found in art. 90 para. 5 of Electronic Communications Act: “The undertakings providing public communications networks or publicly available electronic communications services may mutually exchange data relating to the provision of such services, including data on subscribers being connected, in order to ensure connection and access to the network, mutual billing and the identification of any abuse of the network and the electronic communications services. Abuse of the electronic communications service means consistent late payment of the billed cost pursuant to Section 64, or the making of malicious or annoying calls.”

A slight difference between the Czech law and the ePrivacy Directive is noted. The exception laid down in Electronic Communications Act seems narrower as to its scope, as it only applies traffic meta data. |
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Art. 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

This question is addressed in para. 97 of Electronic Communications Act.

“(1) A legal entity or natural person providing a public communications network or publicly available electronic communications service shall, at the applicant’s expense, provide and secure interfaces at specified points of the network to connect terminal equipment for message interception and recording:
   a) for the Police Force of the Czech Republic for the purposes laid down in special legislation,
   b) for the Security Information Service for the purposes laid down in special legislation,
   c) for Military Intelligence for the purposes laid down in special legislation.

(2) The authorities referred to in paragraph (1) shall prove their authorization to intercept and record messages by submitting a written application containing the reference number under which the court ruling maintained at the authority and signed by the person responsible at the authority referred to in paragraph (1) for carrying out message interception and recording. Where message interception and recording is carried out by the Police Force of the Czech Republic in accordance with special legislation, the written application shall indicate the reference number under which the consent of the intercepted station’s subscriber is maintained at the Police Force of the Czech Republic.”

According the para. 8 of the same article, the person listed in para. 1 and its employees are bound by confidentiality of such information. The operator has a duty (para. 10) to establish statistics of cases where users have asked to provide such information, and to provide these statistics annually to the Czech Telecommunication Office.

Para. 97 also includes provisions implementing data retention obligations according to the former Directive 2006/24/EC. Besides bodies listed in para. 1, the Czech National Bank can also ask for data held for this purpose. However, since recent development and since art. 15 para. 1a of Directive 2002/58/EC excludes Data retention (2002/24/EC), we shall not elaborate on this matter further.

We have noted a couple of relatively interesting decisions of Czech courts with regard to the use of retained traffic data in civil law proceedings. In a District Court case no. 23 Co 500/2007 (Okresni soud v Hradci Kralove), the court ruled that an operator is obliged to provide retained traffic data upon a petition of a court not just for criminal but also for civil proceedings – however, it should be noted that the court made such transfer subject to prior approval by the respective data subject.

In an even more interesting decision in a civil law case (No. 21 Cdo 2058/2012), the Supreme Court ruled that an operator actually has to use the retained data in order to proof in a civil dispute with its customer over unpaid services that respective services were actually consumed. This decision attracted academic attention and was negatively commented and annotated. The fact that an obligation and a right of the operator to retain traffic data for a specific purpose was turned by the court into an obligation to actively use these data for a purpose not envisaged by respective laws, was only a part of its problematic nature. The Supreme Court included among the list of types of such “compulsorily processed” data also URL addresses of connections used by the consumer (such a category, however, was missing at that time in the statutory list of traffic data).
4. 

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The term “automated breaches of confidentiality without human involvement” has not expressly been implemented in Czech legislation, so the general provisions regarding confidentiality apply (art. 89 paras. 1 & 2 Electronic Communications Act), whereas the content enjoys relatively higher standard of protection compared to metadata (see question 2).

b. The Criminal Code (act no. 40/2009 Sb. of the Criminal Code) in art. 182 para. 1 under b) states, that the intentional breach of confidentiality of data, text, voice, sound or picture messages, sent via an electronic communications network to an identifiable user, who receives the message, will be punished by imprisonment of up to two years, or prohibition of providing the service.

A specific situation of breeching confidentiality of employee’s email by an employer is regulated in Act no. 262/2006 Sb., Labour Code. Paragraph 2 and 3 of art. 316, which regulates the protection of employee’s privacy, state:

“(2) Without a serious cause consisting in the employer’s nature of activity, the employer may not encroach upon employees’ privacy at workplaces and in the employer’s common premises by open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee.

(3) Where there is a serious cause on the employer’s part consisting in the nature of his activity which justifies the introduction of surveillance (monitoring) under subsection (2), the employer shall directly inform the employees of the scope and methods of its implementation.”

It should be noted that the Criminal Code applies as ultima ratio, i.e. it does not affect situations of minor importance or those that can be sufficiently tackled using relatively less powerful measures offered by private or administrative law.
5. As to cookies and spyware as mentioned in Art. 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. As to the scope and substance of the national implementation of cookies and similar technology provisions, the Czech law uses the same definition as the ePrivacy directive. Art. 89 para. 3 reads as follows:

“Anybody wishing to use, or using, the electronic communications network for the storage of data or for gaining access to the data stored in the subscribers’ or users’ terminal equipment shall inform those subscribers or users beforehand in a provable manner about the extent and purpose of processing such data and shall offer them the option to refuse such processing. This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of message transmission via the electronic communications network, nor does it apply to the cases where such technical storage or access activities are needed for the provision of an information society service explicitly requested by the subscriber or user.”

The provision regulates all situations where anybody wishes to use an electronic communications network for the storage of data or for gaining access to the data stored in the subscribers’ or users’ terminal equipment.

A difference that we noted between the Directive and the Czech implementation is in the adoption of the opt-in principle. The amending Act no. 468/2011 Sb. removed the words ‘exclusively for the purposes’ from the sentence “This obligation does not apply to activities relating to technical storage or access and serving exclusively for the purposes of performing or facilitating message transmission via the electronic communications network,” while the wording of the first sentence remained the same as before the adoption of the Directive 2009/136/EC. Thus, the provider only has a duty to offer an option to refuse the use of cookies under the Czech law. Interestingly, the explanatory note of the amending act states that the opt-in principle is in fact introduced, which might lead to confusion of providers and users.

In order to prevent unintended operational breaches of EU law, The Office for Personal Data Protection issued guidance stating that the law should be interpreted in the light of European provisions (http://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=1853&n=cookies-prechod-z-principu-opt-out-na-opt-in&query=cookie&p1=1099), so that the opt-in principle should be applied despite the fact that there is not such specific Czech statutory obligation.

b. Czech statutory law does not differ between various categories of cookies or devices.
| 6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)? |

| Czech law does not require explicit informed consent for the use of cookies, it only provides for a duty to inform the user about the use of cookies (which duty, however, is not specified in any greater detail). |
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The exception is implemented in the art. 89 para. 3 of the Electronic Communications Act by its literal translation. As described in the answer to question 5, Czech law does not recognize specific types of cookies. The Office for Personal Data Protection has not issued any official opinion / guidance on the issue, nor are there any judicial or administration decisions so far.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, Art.s, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The manner of informing users about the use of cookies reflects the fact that neither opt-in nor any rigorous rules apply. Typically, users are informed about them only in a form of a small print notice placed at the very bottom of a website that works as a link to broader information (that actually nobody really clicks on).

Below picture shows a typical situation of information on cookies demonstrated on a popular Czech news website aktualne.cz – there is a link (highlighted in red) marked just “cookies” that leads to a page with contains a notice on the fact that cookies are used. However, even that website does not provide for any plain explanation as to what cookies are – this is only partly done in further documents linked from there that contain privacy policy and “general contractual terms” (although no contracts are actually made between the provider of the news server and its regular users).
No Czech statistics as to the use, typical forms or perception of cookies were discovered.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

<table>
<thead>
<tr>
<th>a. The Office for Personal Data Protection issued one opinion and one article focused on discussed topics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cookies: transfer from the opt-out to the opt-in principle. This is an article from the website informing about the opt-in principle regarding the the use of cookies. Available in Czech: <a href="http://www.uou.cz/vismo/zobraz_dok.asp?id_org=200144&amp;id_ktg=1853&amp;n=cookies-prechod-z-principu-opt-out-na-opt-in&amp;query=cookie">http://www.uou.cz/vismo/zobraz_dok.asp?id_org=200144&amp;id_ktg=1853&amp;n=cookies-prechod-z-principu-opt-out-na-opt-in&amp;query=cookie</a></td>
</tr>
<tr>
<td>b. No relevant case-law was identified.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. It is relatively difficult to formulate a solid opinion with regards to rules that did not have an opportunity to settle down in regular practice. The lack of activity of the Office for Personal Data Protection does not provide for cases that could illustrate the practical application of the rules. Practical absence of sanctioned misconducts also leads to a lack of court case-law which might illustrate that either privacy problems are not properly tackled by the new regulatory regime or that there are no actual problems at all. As to particular elements of privacy protection, it seems to us unreasonably obtrusive to require their specific consent for the use of cookies. In that respect, the Czech omission as to the statutory requirement of opt-in seems paradoxically reasonable. On the other hand, a lack of particular rules and enforcement activities as to the compulsory informing of users with regards to what cookies are and how are they used makes the Czech implementation of these privacy protective measures practically insignificant (in fact, providers were only obliged to include one more category into the grey small-print, in which users are not interested).

b. In general, we think that a more pragmatic approach to statutory obligations together with rules providing for enhanced institutional activity of the DPAs might help. In particular, less attention should be paid to specific opt-in requirements, while more regulatory efforts should probably be put into the improvement of consumer awareness. As to the institutional activity, it is in a number of European countries (incl. the Czech Republic) quite difficult to motivate the local DPA to fully engage in truly problematic issues that are often complex and complicated. Instead of that, it seems that minor issues of only little practical significance are actually dealt with. If the private sector or even entrepreneurial initiatives would be given an opportunity to actively enforce privacy protective provisions e.g. on the basis of class actions, we would probably only rarely see major services being in evident breach even with basic and clearly formulated rules.

---

C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Electronic Communications Act art. 90 para. 1 defines traffic data as: “Any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof.”

As was stated in question 1 of section B, the word “message” is an equivalent for the Directive’s term “communication,” so the Czech legal definition literally matches the wording of the European regulatory framework.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

<table>
<thead>
<tr>
<th>General requirements for data and privacy security in electronic communications services are laid down in Art. 88 of the Electronic Communications Act (see question no. 7 of section A of this report). Art. 90 of the Electronic Communications Act defines the main rules regarding the processing of traffic data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“(1) Traffic data mean any data processed for the purposes of the transmission of a message via the electronic communications network or for the billing thereof.</td>
</tr>
<tr>
<td>(2) The undertaking providing a public communications network or publicly available electronic communications service who processes and stores traffic data, including the appropriate location data relating to a user or subscriber, shall erase such data, or render them anonymous, once they are no longer needed for message transmission, except as provided in paragraphs 3 to 6. The obligation of the legal entity or natural person providing a public communications network or a publicly available electronic communications service to maintain operating and location data according to Art. 97 shall remain unaffected.</td>
</tr>
<tr>
<td>(3) The undertaking providing a public communications network or a publicly available electronic communications service shall store operating data for services provided to subscribers or users until such time as disputes pursuant to Art. 129 paragraph 3 have been resolved, or until the end of the period during which the billing of the price or the provision of the electronic communications service can be legally challenged or the payment thereof collected.</td>
</tr>
<tr>
<td>(4) The undertaking providing a public communications network or a publicly available electronic communications service may only process operating data required for the billing of the cost of services provided to subscribers or users for access to the end of the period during which the payment may be collected.</td>
</tr>
<tr>
<td>(5) Undertakings providing a public communications network or a publicly available electronic communications service may mutually exchange data relating to the provision of such services, including data on subscribers being connected, in order to ensure connection and access to the network, mutual billing and the identification of any abuse of the network and the electronic communications services. Abuse of the electronic communications service means consistent late payment of the billed cost pursuant to Art. 64, or the making of malicious or annoying calls.</td>
</tr>
<tr>
<td>(6) For the purposes of marketing the electronic communications services or for the provision of value-added services, the undertaking providing publicly available electronic communications service may only process the data referred to in paragraph 1 above to the extent and for the period as needed for such services or such marketing, as far as the subscriber or user to whom the data relate gave a prior consent thereto. The subscriber or user may withdraw his consent with the processing of traffic data at any time.</td>
</tr>
<tr>
<td>(7) A value-added service means any service for which it is necessary to process traffic data – or location data other than those of traffic nature – beyond what is needed for the transmission of a message or for the billing thereof.</td>
</tr>
</tbody>
</table>
(8) The undertaking providing publicly available electronic communications service shall inform the concerned subscriber or user about the traffic data being processed and about the time for which such data may be processed for the purposes referred to in paragraphs 3 to 5. For the purposes referred to in paragraph 6, the undertaking shall so inform the subscriber or user to whom the data apply still before obtaining such a subscriber’s or user’s consent.

(9) The undertaking providing a public communications network and the undertaking providing publicly available electronic communications service shall ensure that the traffic data processing according to Subsections 2 to 6 is restricted to

a) the persons who were authorised to that effect by the that undertaking and who are responsible for the billing or operation management, for customer inquiries, fraud identification, electronic communications services marketing, or who provide value-added services; and

b) the extent essential for the activities referred to in Clause a) above.”

The Czech transposition matches the terms used in the ePrivacy Directive without any major textual differences.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th><strong>Pursuant to Art. 90, para. 2 of the Electronic Communications Act traffic data must be deleted or anonymised if they are not necessary for the purpose of communication transition, with exemptions listed in paras. 3 to 6 of the same Article (see also question 2 of this section.)</strong></th>
</tr>
</thead>
</table>

### 4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

One case was noted where general information rights were successfully enforced against a mobile communications operator. In this case, a user successfully asked for access to traffic data (it also concerned location data), which were stored on his account by the operator. This case was used as a basis for the issuance of guidelines by the Office for Personal Data Protection No. 6/2013 where traffic data are explicitly counted among personal data that fall under information rights ([http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9737](http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9737)).

The persistent problem, however, is that provision of such data might be subject to a payment by the data subject, whereas recent pricing policies of providers are quite extensive. This was already criticised by a couple independent journalists and might be a subject to further review by the Czech DPA.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Traffic data together with location data represent a highly problematic issue in Czech law, mostly due to the Data Retention Directive. That, however, falls outside of the scope of this report.

As to specific issues related to the ePrivacy Directive, we would probably point out the distinction between providers of electronic communications and providers of information society services. While there are specific protective rules applicable on the first, the latter fall only under the scope of general duties arising from the legal regulatory framework protecting personal data. This, however, does not bring any significant problems or confusions as to practical enforcement of the protection of personal data with regards to processing of traffic data by providers of various services.

On the other hand, we noted quite some confusion as to what arrangements on processing of traffic data might be included in consumer contracts. In that respect, there is not much in the Electronic Communications Act which is relevant and there are no rules at all (except general consumer protection) with regards to services of information society. In that respect, we would welcome particular contractual rules or guidelines preventing providers from including overly extensive processing clauses into their service contracts that regularly give them much broader possibilities with regards to consumer traffic data compared to those implied by the statutory law.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The term “location data” is defined in art. 91, para. 1 of the Electronic Communications Act, as: “Any data that are processed within the electronic communications network or by an electronic communications service that define the geographical location of the terminal equipment of a user of publicly available electronic communications service.”

The definition matches the ePrivacy directive definition.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

The legal requirements for the lawful processing of location data are defined in art. 91 of the Electronic Communications Act.

“(1) Location data mean any data that are processed within the electronic communications network or by an electronic communications service that that define the geographical location of the terminal equipment of a user of publicly available electronic communications service.

(2) If the undertaking providing a public communications network or publicly available electronic communications service performs the processing of location data other than those of traffic nature, which data have a bearing on the user or subscriber, such an undertaking shall render such data anonymous or gain the user’s or subscriber’s consent to the processing of such data to the extent and for the period as needed for the provision of value-added services. Before gaining the consent, the undertaking shall inform the concerned user or subscriber about the type of location data to be processed other than those of operating nature, about the purpose and length of the processing and whether the data are to be made available to a third party for the provision of value-added services. The user and subscriber may withdraw his consent with the processing at any time.

(3) If the user or subscriber gave his consent to the processing of location data other than those of traffic nature, the undertaking providing a public communications network or publicly available electronic communications service shall offer the user or subscriber the option to temporarily refuse the processing of the data in accordance with Subsection 2 above for every connection to the network or for every message transfer. Such an option shall be provided free of charge and with the application of simple facilities.

(4) The undertaking providing a public communications network, the undertaking providing publicly available electronic communications service and the undertaking providing value-added services shall ensure that the data referred to in Subsections 2 and 3 are only processed by persons duly authorised and entitled to that effect by a internal technical and organisational regulations within the meaning of Section 88 Subsection 1 Clause b) and that the processing is restricted to the extent essential for such activities.”

The terms of the definition do not deviate from the Directive. As to third parties, there are no specific provisions, as the scope of the Electronic Communications Act only covers providers of services of electronic communications. Operations with these data conducted by third parties are regulated by general provisions of the Personal Data Protection Act (i.e. there apply general rules regarding consent, contracted processing, transfers etc.).
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

| **Art. 91 para. 2 of the Electronic Communications Act** establishes a duty to delete or anonymise location data, unless the user (data subject) gives informed consent to processing. This consent can be withdrawn any time and even temporarily (para. 3 of the same article). (See question 2 of this section.) |
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. The Office for Personal Data Protection issued an opinion which clarifies certain aspects of the relation between the Electronic Communications Act and the Personal Data Protection Act.

In Opinion No. 6/2013 on providing of information about Traffic and Location data processed by providers of electronic communication services (in Czech: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9737), the Office states that the data subject has a right to information in accordance with the Personal Data Protection Act (generally matching directive 95/46/EC) about processed data even in cases, when there are processed traffic and location data for the purpose of data retention (based on Directive 2006/24/EC). This opinion, however, does not include any guidance as to whether the data subject is also entitled to receive information about whether her data were requested by the Police or other state bodies.

The Office for Personal Data Protection was more concerned with the Data Retention directive and its implementation, which was quite turbulent, and the general provisions concerning traffic and location data were out of its sight.

The Czech Telecommunication Office has not issued any guidance, or cases decisions. On the website of the CTO statistics can be found of traffic and location data which were handed over to the Police forces. It is a duty of an operator to provide such information to the CTO.

b. We have noted no relevant case-law apart from the judgement of the Constitutional Court of the Czech Republic from 22\textsuperscript{nd} March 2011 (Pl. ÚS 24/10-1). In this judgment, the Constitutional Court quashed the data retention provisions (at the moment, a new data retention statutory regime is already in force).
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The answer on this point should be similar to the previous part, because location data have the same regulatory regime as traffic data.
### E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in Art. 13 of the ePrivacy Directive) please describe:

   a. the scope and substance of your national implementation

   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

| a. | The provisions concerning unsolicited direct marketing communications are implemented in articles 7 and 8 of the Certain Information Society Services Act. Paragraph 1 of Art. 7 states that commercial communication can be disseminated by electronic means only when they adhere to the requirements of the Certain Information Society Services Act. “Commercial communication” is defined in Art. 2 under f) as “all forms of communication, including advertisement and a challenge to visit a webpage, dedicated to a direct or indirect support of sale of goods or services, or image of undertaking of a person who is a businessman or who executes a regulated activity.” |
| b. | The word ‘marketing’ is not used in the implementation. Instead of that the term ‘commercial communications’ is used. This is due to the fact that “marketing” is not a word of Czech origin and its use would be contrary to the language principles of Czech legislation. Paragraph 2 of Art. 7 of the Certain Information Society Services Act does not specify kinds of electronic communications as does the Art. 13 (1) of the ePrivacy Directive. This is due to the technological neutrality of these provisions (see question 4 in this section of the report). Paragraph 2 of the Art. 7: “Electronic contact details can be used for the purpose of dissemination of commercial communications via electronic mail only in relation to users, who provided prior consent.” |
| | Art. 13 (2) of the ePrivacy directive is implemented very similarly in Art. 7 paragraph 3 of the Certain Information Society Services Act. Art. 13 (3) of ePrivacy directive isn’t expressly implemented, however, the purpose of this provision is achieved by setting the scope of the provisions and Art. 7 paragraph 1 in particular (see first part of this question). Art. 13 (4) of the ePrivacy Directive is implemented very similarly in Art. 7 paragraph 4 of the Certain Information Society Services Act. Since the definition of user includes both natural and legal persons, Art. 13 (5) of the ePrivacy Directive is fulfilled. |
Pursuant to art. 13 (6) dissemination of unsolicited marketing information is regarded as an administrative offence, so individuals might file petitions to the Czech DPA, but they formally act only in case of information about illegal activity (not as individual claims). This is typical for administrative offences, i.e. that authorities act upon their own initiative, whereas individual petitions formally act only as information that may induce administrative investigation.

There are no other specific provisions regarding direct individual claims, but general possibilities of individuals and corporations to defend upon standard instruments of private law. In the case of business units (corporate or non-corporate), it is possible to use direct claims based on unfair competition. In case of individuals, it is possible to defend using privacy protective provisions of the Civil Code.

A fine, that can be imposed upon a perpetrator of sending an illegal unsolicited commercial communications, can be at maximum 100 000 for a natural person (art. 10a of the Certain Information Society Services Act) and 10 000 000 for a legal person (art. 11 of the Certain Information Society Services Act). There is neither any standard scheme for remedies claimed individually upon the rules of unfair competition or privacy nor any case-law that would enable us to determine standard level of damages.

A rather specific issue arises in case of commercial communications by specifically regulated professionals (e.g. solicitors, architects etc.). Art. 8 of the Certain Information Society Services Act allows such actions under the condition that requirements laid down in Art. 7 of the Certain Information Society Services Act and of rules of the specific association are met. Art. 8 reads:

“(1) Persons exercising a regulated profession may, using electronic means, within activities that are subject to the regulated profession, disseminate commercial communications, in compliance with Section 7 and in compliance with the relevant rules issued by commercial, professional and consumer associations, governing in particular the independence, dignity, honour of the profession, and fairness towards customers.

(2) When disseminating commercial communications, using electronic means, within activities that are subject to a regulated profession, persons exercising a regulated profession who are not members of professional self-governing chambers established by statute shall proceed in accordance with Section 7.

(3) Commercial communications from persons exercising a regulated profession must contain the name of the professional self-governing chamber established by statute with which the person exercising a regulated profession is registered, a reference to the professional rules applied in the member state of the European Union in which the person exercising a regulated profession is established, and the manner of permanent access to information about the relevant professional self-governing chamber established by statute which the person exercising a regulated profession is a member of.”

Art. 10 paragraph 1 letter b) of the Certain Information Society Services Act provides for the establishment of the authority of respective self-governing bodies (e.g. Czech Bar Association, Czech Chamber of Architects etc.) over compliance control and enforcement of the aforementioned provisions. This makes sending unsolicited marketing communication of specifically regulated professionals distinct from other forms of unsolicited marketing.

Lex specialis to both aforementioned regulatory regimes concerns the use of data that are being
processed as a matter of creation of telecommunication directories. These provisions affect providers of services of electronic communications and are included in Art. 66, 95 and 96 of the Electronic Communications Act. These provisions read as follows:

Art. 66:
“(1) The undertaking that allocates telephone numbers to the subscribers shall, if so requested by the person providing the publicly available directory enquiry services or providing the subscriber directories, deliver to such a person or entity the available subscriber personal and identification data to the extent specified in Section 41 Subsection 5 above, except for the information and data about the subscribers who refused to have their information published in the directory. The undertaking that allocates telephone numbers to the subscribers shall deliver such information and data in the agreed format and under equal abn fair conditions and at prices, which are cost-oriented and non-discriminatory. The submitting party shall always indicate, if such is the case, that the subscriber expressed his wish not to be contacted for marketing purposes.

(2) For all the end users of the public telephone network, the undertaking providing the public telephone network shall enable access to the operator services and at least to one directory enquiry service, the latter service covering the telephone numbers of the subscribers to all the undertakings providing publicly available telephone service.”

Art. 95 on Subscriber Directories:
“(1) Anybody gathering subscribers’ personal data in order to issue a subscriber directory, which is to serve for seeking detailed contact information about persons on the basis of their names and, if applicable, an essential minimum amount of other identifying elements, shall:
a) inform the subscribers concerned free of charge before inclusion of their data in the directory about the purpose of the printed or electronic directory of subscribers, which is to be available to the public either directly or through the subscriber directory inquiry services, as well as about other possibilities of use, based on the searching functions contained in the directory’s electronic versions;
b) obtain beforehand the consent of the subscribers with making their personal data public and ensure that the subscribers have an opportunity to determine which of their personal data from the range or information relevant for the directory purposes, as defined by the directory publisher, are to be included in the public directory; further, it must be ensured that the subscribers are able to verify such information and ask corrections or removal of such information. At the same time, the person gathering such information must ensure that the subscribers can indicate with their personal information that they do not wish to be contacted for marketing purposes. Non-inclusion in the public directory of subscribers, the verifications, corrections and removals of information from the directory and the information about the subscriber’s wish not to be contacted for marketing purposes shall be free of charge.

(2) If the purpose of the public directory is other than seeking detailed contact information about person on the basis of its name and, if applicable, an essential minimum amount of other identifying elements, anybody intending to issue such a subscriber directory must first ask for further consent of the subscribers concerned.”

Art. 96:
“(1) It is prohibited to offer through the electronic communications networks or services any marketing advertising or any other method of offering goods or services to the subscribers who
noted in the public directory of subscribers in accordance with Section 95 Subsection 1 Clause b) or Section 95 Subsection 2 that they do not wish to be contacted for such purposes.

(2) It is prohibited to use the electronic communications networks or services for direct marketing through automated dialling systems with no human involvement (automated dialling systems), fax machines or electronic mail, unless the affected subscriber consented to that in advance.

(3) The undertaking that provides for an inquiry service for subscribers’ numbers or other similar data, is prohibited to provide for data that are not included in the public directory.

(4) The provisions of Sections 95 and 96 shall apply, mutatis mutandis, to the information about subscribers who are legal entities.

(5) Provider of services of electronic communications, whose commercial interests are damaged by breaches of obligations laid down in paragraphs 1 to 4 is entitled to claim judicial protection on behalf of its subscribers, whose rights were violated by such breaches. This does not affect the possibility of an individual subscriber to claim these rights individually.”

The aforementioned provisions basically provide for an opt-in regime with regard to the inclusion of contact information in public directories of electronic communications. The opt-out mechanism applies in case of exclusion of these contact details from the possibility of being used for marketing purposes. Although the Electronic Communications Act regulates a broad variety of services of electronic communications, these provisions practically regulate only telephone contact details (i.e. public telephone directories). As the use of these directories not popular anymore, these provisions have almost lost their significance.

The only exception that might be of crucial importance is laid down under paragraph 2. As no reference is made to the directories, this provision generally prohibits the use of electronic communications networks and services for unsolicited direct marketing incl. if this is done by e-mail. Moreover, this provision does not only apply to providers of services or networks of electronic communications, but to all businesses that use these services, as the sanction provisions laid down in Art. 118 apply to “legal entities and private entrepreneurs”. As a result, it is possible for the Czech Telecommunications Authority to directly sanction spamming, whereas the maximum fine could be up to 20 mil. CZK (this is double of the maximum fine that can be imposed by the Czech DPA upon the Act No. 480/2004 Sb.) It is not entirely clear to the rapporteurs whether this dichotomy is intentional or accidental. In any case, no investigations or sanctions for spamming by the Czech Telecommunication Office were reported so far.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Art. 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

| Please see answer 1b of this section. |
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

| Art. 7 paragraph 3 of the Certain Information Society Services Act is a direct implementation of art. 13(2) of the Directive. The exception is formulated the same way as in the Directive. |
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Electronic mail is defined in Art. 2 under b) of the Certain Information Society Services Act as: “a text, voice, sound or image message sent over a public electronic communication network which may be stored in the network or in the user’s terminal equipment until it is collected by the user.”
This definition covers all kinds of messages including e/mail, MMS/SMS/text messages, banners, instant messaging newsfeeds, social media outreach, and others. The Czech law is technologically neutral in this matter, so it does not distinguish between them. This definition is in its content comparable to ‘electronic mail’ as is defined in the ePrivacy directive.

There are specific provisions in the Electronic Communications Act that regulate the use of direct marketing tools using information from public directories of electronic communications (see question 1).
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. The Office for Personal Data Protection is quite active in this matter. There is a huge section dedicated to unsolicited commercial communications on the website of the Office (in Czech: [http://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=1493&n=nevyzadana-obchodni-sdeleni&p1=1493](http://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=1493&n=nevyzadana-obchodni-sdeleni&p1=1493)). Users can also use a web form to make a complaint and then they can check online what the status is of their complaint.

Guidance on the consent to receive commercial communication was published by the Office for Personal Data Protection in the form of Opinion no. 5/2012 (available in Czech: [http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9719](http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9719)).

The decision-making practice of the Personal Data Protection Office is, however, quite problematic. The Office receives an enormous number of complaints, so it tends to investigate them vaguely and in most cases decides on formal criteria. Only a few cases end up in significant fines (see for instance a ruling of 21st of March 2014 where a spammer was fined by 480,000 CZK – approx. 18,000 EUR). [http://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=9362&n=ulozeni-pokuty-spolecnosti-emarketing-cz&query=obchodni(sd%20sd%C4%9Blen%C3%AD)](http://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=9362&n=ulozeni-pokuty-spolecnosti-emarketing-cz&query=obchodni(sd%20sd%C4%9Blen%C3%AD)). Moreover, most of spammers are acting outside of the Czech jurisdiction, so there is no actual possibility for the Office to reach them (and there is no possibility for the Office to approach ISPs with e.g. blocking or filtering orders either).

b. We noted no decisions where individuals would take legal actions against spamming. This might be mainly due to the fact that it is quite complicated to actually identify a spammer and to discover solid evidence as to the harmful effect of spamming (actual harm forms in these cases substantial ground for private law remedies).
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Although preventive rules against spamming might have some preventive effect, the overall impact of the anti-spam legislation is hugely disputable. It established a quite substantial workload for the Czech DPA, but the resulting outcome does not look very impressive. It is practically impossible to tackle spam of foreign origin (whereas this is most frequently the case) and it is also quite easy to avoid sanctions even in the case of spamming within the Czech Republic by taking simple practical measures (e.g. by pretending that marketing communication is in fact individual viral sharing of some interesting news). Consequently, the law is incomparably less efficient than technical measures like spam filters – the fact that there is no significant amount of originally Czech spam that would represent regular marketing communication (e.g. offering regular goods or services) might also show that this marketing practice is not efficient from the business point of view any more.

In that respect, we believe it might help if the DPA would have competences to order filtering against ISPs or if specific individual causes of action were established in order to promote self-defence of those who are targeted by spamming (e.g. class actions or specifically designed statutory damages). As spam acts not just as a carrier of marketing information but hugely as a carrier of security threats, we believe the newly developed Czech and EU regulatory framework on network security might be of help.
COUNTRY REPORT
GERMANY

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Prof. Dr. Nikolaus Forgó & Christian Hawellek // Institute for Legal Informatics // Leibniz University Hanover

Date: 25.08.2014
Contents

Part 1: Management summary .............................................................................................................. 3
Part 2: Answers to the questionnaire .................................................................................................. 5
Part 1: Management summary

The transposition of the ePrivacy Directive into German law can be summarized as follows:

- The provisions with regard to the scope of the Directive have been transposed mainly through amendment of part VII of the German telecommunications code with the exception of Art. 5(3) (transposed through § 15 III Telemediengesetz (Law on Services of the Information Society)) and Art. 13 (transposed through § 7 II and III UWG (Law against unfair competition)).

- The majority of provisions appear to have been transposed fairly accurately, with the exception of Art. 13, regarding which German law provides for an opt-out only, which has led to confusion regarding the question whether the directive could override the German provisions in this particular point. That apart, transposition of Art. 5 II remains somewhat unclear. Otherwise, there are a couple of minor discrepancies in which German data protection law is stricter than the directive, e.g. through extending the scope of protection against unsolicited communications to legal persons or through extending the need to comply with data protection rules to providers of non-public telecommunications services.

- An important observation, is the fact that the directive when being transposed had to be integrated into a set of already existing rules with a very similar scope. Thus, the transposition has led to some confusion by altering an existing system of legal provisions. Questions that came up included the extent to which previous court decisions on the very same subject-matter can be used as guidelines post implementation of the directive. Also certain disturbances in the existing systematic set of rules, which - according to the data protection authority - lead to difficulties in interpretation. This begins, as the authority has stated, with issues related to translation into German, which may lead to a different wording where the same wording (as previously used) would appear appropriate; or vice versa to identical wording, where different terms would be needed (as the German legal system, being a relatively strictly positivist legal system tends to assume a distinct legal concept behind different legal terms).

- Moreover, those provisions of the directive that were transposed into the telecommunications code also systematically overlap with existing law. This becomes quite evident when looking at § 96 TKG (traffic data) and § 98 TKG (location data), regarding which sentences transposing European law and sentences of genuine German legislation alternate. While this does not necessarily cause any issues regarding transposition, it at least holds a certain potential of causing questions regarding interpretation of the law.

- Location data has largely lost significance in context of telecommunications services, as these days location data is collected via GPS and processed in smart phones, and therefore used for telemedia services (services of the information society, such as Google Maps), which renders the telecommunications code inapplicable. However, there is no corresponding law on usage of location data outside telecommunications services, which creates a lacuna in this respect (only the general rules apply).
- Competencies of enforcement are split between the Federal Data Protection Authority (BFDI, in charge of telecommunications services in total, and telemedia services of the Federal Authorities), the 16 data protection authorities of the German Lands (in charge of privacy related issues regarding all other telemedia services) and Bundesnetzagentur (German Federal Networks Regulation Authority, in charge of enforcement of the entire telecommunications code, including privacy related provisions). While the co-operation between BFDI and Bundesnetzagentur appears to run smoothly and rules are quite clear (privacy assessment through BFDI, enforcement through Bundesnetzagentur), the division of competencies is more critical regarding BFDI and the data protection authorities of the Lands. While in theory the law is clear (the latter being responsible for telemedia services), the persisting practical difficulties regarding finding a clear distinction between telecommunications services and telemedia services have an impact on the practical division of competencies, which still needs to be solved.

- Whereas compliance with telecommunications privacy law appears to be monitored quite well, provisions on cookies (transposed in telemedia privacy law) appear not to have been monitored to a similar degree until this point in time. While there are isolated cases addressing the issue, in general the subject of cookies has not yet been addressed a lot, except for the discussion around the question whether Germany has transposed Art. 5 III sufficiently. The latter debate, however, has not yet, as it appears, led to a clear outcome either.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into German law in the code against unfair competition jointly with those provisions laid down in the ecommerce directive. While these are not enforced by a particular authority, competitors, consumer protection societies and consumers themselves with respective rights to challenge breaches (consumers only if directly affected) have been provided with the necessary rights to seek enforcement in front of court.
Part 2: Answers to the questionnaire
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC was mainly transposed into German federal law by part 7 section 2 (as well as section 1) of the German Telecommunications Law (Telekommunikationsgesetz).
- The provisions with regard to unsolicited communications were transposed through modifying § 7 UWG (Gesetz gegen den unlauteren Wettbewerb; law against unfair competition).
- Some of the directive’s provisions have not been transposed explicitly; the explanatory report of the respective draft laws does not explicitly mention that a transposition was considered unnecessary due to existing law being considered sufficient, although that is the likely reason.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
| Art. 2 (Definitions) | a) “user” -> § 3 Nr. 14 TKG  
                        b) “traffic data” -> § 3 Nr. 30TKG (n.b. different wording!)  
                        c) “location data” -> § 3 Nr. 19 TKG  
                        d) “communication”; in the German wording of the directive translated as “Nachricht” (literally “message”): § 2 I Nr. 4 UWG  
                        e) Deleted from directive  
                        f) “consent” -> there is no particular transposition in telecommunications law or otherwise. Art. 2  
                        h) 95/46/EC has not been transposed literally, however, § 4a BDSG (General Data Protection Regulation) | http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html |
<table>
<thead>
<tr>
<th>Protection Code, applicable wherever no rules being more specific exist, contains rules on consent which together with the general principles of German law should cover what is laid down in Art. 2 h) 95/46/EC (which is referred to by Art. 2 f) 2002/58/EC) at least implicitly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>g) “value added service” -&gt; § 3 Nr. 5 TKG</td>
</tr>
<tr>
<td>h) “electronic mail” -&gt; apparently not transposed</td>
</tr>
<tr>
<td>i) “personal data breach” -&gt; § 3 Nr. 30a TKG</td>
</tr>
</tbody>
</table>

| Art. 3 (Scope) | § 91 TKG, whereas the German scope is not limited to publicly available telecommunication services, but includes also those which are not publicly available | http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html |

| Art. 5.1 (Confidentiality) | The German constitution constitutes a distinct fundamental right to telecommunications privacy (Art. 10 Grundgesetz), being complementary to the more general fundamental right to informational self-determination (data protection). As a result, German statutory law needs to transpose both independently. Consequently, telecommunications privacy is (and has always been) protected through distinct provisions in telecommunications law, which | http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html |
are also suitable to transpose Art. 5.1. These are § 88 TKG on general level, and more specifically § 89 TKG regarding the prohibition of all forms of interception and § 90 TKG concerning the prohibition of disguised telecommunications devices suitable for surveillance purposes. Both provisions allow exceptions through specific laws, in particular referring to authorities entrusted with public safety and national security (transposing the reference of Art. 5 I to Art. 15 I 2002/58/EC).

| Art. 5.2 (Business exception) | Not directly transposed. To which extent exceptions as laid down under Art. 5 II 2002/58/EC could be established under the rule of German law appears not totally clear and depends on the precise interpretation of Art. 5 II. Should sub-section II seek to constitute an exception to the rule of sub-section I, this would mean that sub-section II would (as does sub-section I) address cases, in which third parties (other than the users) would access/store telecommunications without prior consent of the users and beyond the cases referred to in Art. 15 (public security). |
Given that telecommunications privacy is a distinct fundamental right in Germany, that would be legitimate only - if at all - under very strict preconditions, and it appears difficult to think of a scenario in which such rule would be proportionate.

However, it appears more likely that Art. 5 II does not seek to constitute an exception to subsection I, but rather to clarify that subsection I does not cover cases, in which a user himself would record the telecommunications. This interpretation appears more likely in the light of possible scenarios (in which one of the communicating parties seeks to document the transaction initiated through telecommunications) and is supported by recital (23) referring to 95/46/EC.

Under the rule of German law such cases would not affect the fundamental right to telecommunications privacy at all, but fall under the general data protection framework.

Still, distinction between (real-time) speech or other content is needed, as in the former case any recording without obtaining prior consent of the speaker speaking not in public is prohibited by § 201 StGB (German Criminal Code). In all
cases, such scenarios are governed by the general data protection rules.

<table>
<thead>
<tr>
<th>Article</th>
<th>Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Legislator considered existing rules laid down in § 12 Telemediengesetz sufficient, which has been confirmed by the European Commission. The German data protection authority has however criticised the transposition, pointing out that § 15 III Telemediengesetz was applicable as <em>lex specialis</em>, which constitutes an opt-out (only). This has not however caused any legislative action as it was argued that further observation on the development on a European level would be sufficient and appropriate.</td>
<td><a href="http://www.gesetze-im-internet.de/tmg/BJNR017910007.html">http://www.gesetze-im-internet.de/tmg/BJNR017910007.html</a></td>
</tr>
</tbody>
</table>
| Art. 9 (Other location data) | Art. 9 I -> § 98 I TKG (together with additional rules and with extended scope)  
Art. 9 II -> § 98 II TKG  
| Art. 13 (Unsolicited communications) | Art. 13 I -> § 7 II Nr. 3 UWG (referring to ‘marketing’ in general without adding ‘direct’ other than the directive);  
Art. 13 II -> § 7 III UWG;  
Art. 13 III -> § 7 II Nr. 1 and 2 UWG; Nr. 2 laying down specific | http://www.gesetze-im-internet.de/uwg_2004/BJNR141400004.html  
rules for non-automated telephone calls (opt-in required) and Nr. 1 laying down rules for means of distance selling, which are not regulated in Nr. 2 and Nr. 3.

Art. 13 IV -> § 7 II Nr. 4 UWG and § 95 II TKG (for service providers only)

Art. 13 V: most of the interdictions laid down in § 7 UWG protect legal and natural persons likewise; this includes all interdiction based upon the directive. § 7 II Nr. 2 UWG makes a distinction between consumers (natural persons not acting professionally, § 13 BGB) and traders (other natural and legal persons, § 14 BGB); Nr. 1 only applies to consumers

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit</td>
<td>German Federal Data Protection Authority</td>
<td>All provisions transposed in telecommunications law (as well as general data protection law) (s. § 115 I TKG; Beck-</td>
<td><a href="http://www.bfdi.bund.de/DE/Home/homepage_node.html">http://www.bfdi.bund.de/DE/Home/homepage_node.html</a></td>
</tr>
<tr>
<td>Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen</td>
<td>German Authority for Networks</td>
<td>The entirety of provisions in telecommunication law; including those related to data protection and transposing the directive (joint responsibility with data protection authority) (s. § 115 IV TKG; Beck-TKG-Komm)</td>
<td><a href="http://www.bundesnetzagentur.de/cln_1411/DE/Home/home_node.html">http://www.bundesnetzagentur.de/cln_1411/DE/Home/home_node.html</a></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Landesbeauftragte für den Datenschutz</td>
<td>Data Protection Commissioners of the German Lands</td>
<td>§ 15 TMG, which is supposed to transpose Art. 5 III 202/58/EC</td>
<td>Each of the 16 German Lands holds an autonomous data protection authority with respective territorial competences; URLs for some of these authorities are e.g.:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.baden-wuerttemberg.datenschutz.de/">http://www.baden-wuerttemberg.datenschutz.de/</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.datenschutz-bayern.de/">https://www.datenschutz-bayern.de/</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.datenschutz-hamburg.de/">https://www.datenschutz-hamburg.de/</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.ldi.nrw.de/">https://www.ldi.nrw.de/</a></td>
</tr>
</tbody>
</table>

Explanation:
- Bundesnetzagentur is in charge of supervising the entire Telecommunications Code’s application; BFDI has extra-ordinary responsibility for part VII (data protection) only, which covers the transposition of the directive. Regarding this section, both authorities share responsibility and may
both work in parallel or co-operate, depending on the case.

- The provisions with regard to unsolicited direct marketing communications, transposed in § 7 UWG, allow through § 8 UWG legal actions (correction (for the past) and omission (for the future)) to be taken by
  - Competitors (§ 8 III Nr. 1 UWG)
  - Certain umbrella associations the members of which are enterprises active on the same market and at least partly affected by the action of the enterprise violating the rules laid down in § 7 UWG (§ 8 III Nr. 2 UWG)
  - Qualified organisations proving to be enlisted in the lists mentioned in § 4 UKlaG (organisations representing consumers’ interests in terms of consumer protection) or the European Commission’s list according to Art. 4 of directive 98/27/EC
  - The Chambers of Industry and Commerce
  - Implicitly through interpretation: each consumer positively affected by such violation in a specific case through the general clauses in civil code, which are: § 1004 BGB (omission) and § 823 II BGB (damages)

- Consequently, conformity of the aforementioned provisions on unsolicited direct marketing is not supervised by a central authority in most cases, but through legal actions (warning letters and further legal steps) taken either by the legal subjects directly affected by the violations (competitors or consumers) or by the aforementioned umbrella associations representing them

- An exception to the above is the enforcement measures taken by Bundesnetzagentur on the basis § 67 TKG, which comprise unsolicited phone calls and faxes (as a sub-case of misuse of numbers). It was stated that currently around 80 employees are working in that field. However, according to Bundesnetzagentur this does not comprise unsolicited communications through any other mean, such as email, which is not regulated by the sub-chapter on (misuse of) numbers.

- Another exception of the aforementioned applies for telecommunications service providers, for which § 95 II TKG applies regarding direct marketing. The compliance with this provision is supervised by both Bundesnetzagentur and BFDI.

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

**Networks:**

Art. 2 (a) 2002/21/EC:

> “electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

§ 3 Nr. 27 TKG:

> "telecommunications network" means the entirety of transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

⇒ Wording and scope are identical.

Art. 2 (d) 2002/21/EC

> “public communications network” means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points;

§ 3 Nr. 16a TKG:

> “public telecommunications network” means a telecommunications network, that entirely or mainly serves providing telecommunications services to the public, which allow transmission of information between network termination points;

⇒ Wording and scope are identical.

**Services:**

§ 3 Nr. 24 TKG:

> "telecommunications services" means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting;

Art. 2 (c) 2002/21/EC:
“electronic communications service” means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

The difference in wording generally does not result in different application as the exclusion of the services mentioned in Art. 1 (c) 2002/21/EC was transposed through German media law and regarding information society services through § 1 TMG. However, practice has shown significant difficulties in applying a strict distinction between telecommunications services and other services.

Providers:

Art. 3 2002/58/EC
This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

§ 3 Nr. 6 TKG:
"service provider" means a person who, on a wholly or partly commercial basis,
a) provides a telecommunications service, or
b) contributes to the provision of such service;

§ 3 Nr. 10 TKG:
"commercial provision of telecommunications services" means telecommunications offered to third parties on a sustained basis, with or without profit-making intent;

§ 91 TKG
(1) This sections governs the protection of personal data of subscribers and users of telecommunications regarding collection and use of such data by enterprises and persons providing telecommunications services commercially in telecommunications networks, including public telecommunications networks supporting data collection and identification devices, or contributing to such provision. Data of an identified or identifiable legal person or partnership, to the extent that they have the ability to acquire rights or to commit to legal claims, which is protected by the telecommunications secret (§ 88 TKG), are equal to personal data.
(2) With regards to closed user groups of public bodies of the German Lands this section applies under the condition that instead of the Federal Data Protection Code the respective Data Protection code of the respective Land respectively shall apply.

The German transposition includes - unlike the directive - non-publicly available telecommunications services, albeit these need to be “commercially” provided, which means offering these to third parties on a sustained basis, with or without profit-making intent. This, again, limits the scope, as thereby all cases of one-time or “random” provision of telecommunications services (e.g. house phones) is excluded. Included are, however, all services
within hotels or companies, which is a wider scope than the one of the directive.

As to protection of legal persons, Art. 1 l 2 2002/58/EC requires protection of their legitimate interests, without providing further details. Regarding the German transposition protection includes, but is limited to the telecommunications secret (§ 88 TKG), which is protected by a distinct fundamental right (Art. 10 GG) and which comprises content and all conditions of telecommunications (e.g. user communicating, time stamp, etc.), in particular traffic data.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

VoIP is considered telephony and as such clearly falls under the scope of the implementing legislation.

Webmail, which in theory could also be seen as a service of the information society (hereafter: SoIS), is unanimously considered a telecommunications service, which makes it fall within the scope of the implementing legislation. There are voices arguing that a webmail service consisting of a mailbox that is accessible via a webbrowser was not a telecommunications service, but a telemedia service (service of the information society). The reasoning in general is that such service (virtual post box) provides access to information, but does not transmit information. Such reasoning is however not convincing, not only because both the recitals of the directive and the explanatory report on German law clearly regard email services as telecommunications services, but also because if webmail was a telemedia service, that would not per se exclude it being a telecommunications service as well – such a service can be of dual nature, which leaves telecommunications data protection law applicable.

The distinction between telecommunications services and telemedia services is pretty much the same as outlined for Belgian law and reflects the same distinction on European level. However, regarding the services in questions here, the applicability of telecommunications data protection law (transposing the ePrivacy Directive) is widely assumed and not challenged.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

| There are no explicit rules on the territorial scope of the telecommunications code. There is a general understanding (also applied by Bundesnetzagentur) that the supervisory authority of Bundesnetzagentur is limited to services which are provided in Germany, regardless of whether or not an establishment exists on German territory; which means Bundesnetzagentur has no competences regarding any services provided outside Germany. Oppositely, § 1 V BDSG (General Data Protection Code) in transposition of Art. 4 95/46/EC provides for the principle of location of establishment, rendering German (general) data protection law inapplicable if a controller had an establishment in another member state, but not in Germany. Obviously, this creates a discrepancy in those cases, in which telecommunications services are provided in Germany without maintaining an establishment in Germany. BDSG is subsidiary to TKG, which means § 1 V BDSG can only be applied to the extent to which TKG does not provide for any specific rules on applicability; however, that does not necessarily mean that the lack of explicit rules automatically results in a (subsidiary) applicability of § 1 V BDSG, if an implicit applicability of TKG on all services provided in Germany without any regard to the existence of an establishment is assumed. This becomes more complex as directive 2002/58/EC does not contain any such rule as laid down in Art. 4 95/46/EC and does not mention Art. 4 in the list of provisions of 95/46/EC to be applied on telecommunications services, which is laid down in Art. 15 2002/58/EC, while emphasising the complementary nature of the latter directive in relation to the former directive in Art. 1 No. 2 2002/58/EC. In particular, recital (10) states: “In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.” This allows an interpretation which would render Art. 4 95/46/EC applicable despite not being mentioned explicitly by Art. 15 2002/58/EC. In that case, German telecommunications would need to be interpreted in conformity with European law thus that § 1 V BDSG (transposing Art. 4 95/46/EC) would apply also on those (more specific and therefore primarily applicable) rules on data protection, which are not laid down in (subsidiary applicable) BDSG, but in transposition of 20002/58/EC laid down in TKG. That would limit the competence of Bundesnetzagentur to take measures against telecommunications services which are compliant with German law to those services, the providers of which hold an establishment in Germany. This could easily become relevant in those cases in which German law is stricter than the rules laid down in 2002/58/EC, e.g. regarding traffic data. However, as outlined initially, Bundesnetzagentur considers itself competent in all cases, regardless of the existence of an establishment. Practically, however, cases with cross-border impact are extremely rare, which has been stated both by the head of department for telecommunications privacy at German Federal Data Protection Authority and by the head of department for telecommunications privacy at Bundesnetzagentur,
due to foreign providers holding local subsidiary companies in Germany (such as Vodafone), and German providers holding subsidiary companies in foreign countries, in which they are active. There have been few cases with cross-border impact in the b2b-sector.

In summary, it appears desirable to clarify the issues outlined above on a European level in order to avoid gaps in supervisory competencies.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a.
   b. BFDI organises non-public meetings on a regular basis with stakeholders in order to create common positions on application of law where appropriate. The outcomes and any guidance issued are not publicly available.

   b. BFDI has published a couple of documents providing guidance on particular legal issues, such as location data, VoIP, data retention, location data, traffic data and so on. They do not particularly aim at explaining the scope of the notions, but are rather tailored to inform the public.

   http://www.bfdi.bund.de/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Telekommunikation_node.html

   A comprehensive brochure (addressing the public) on telecommunications data protection can be found here:

   http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO5_September_2013.pdf?__blob=publicationFile

   This, again, is not primarily designed to establish a coherent line of scope of application, but addressing the wide public on a general level.

   b. § 3 Nr. 27 TKG (telecommunications network): there are a few cases explicitly referring to this provision. The scope of this definition is however not specified beyond what is laid down by law. It does not appear like this definition has been challenged in front of court. Cases are, e.g.: VG Köln, Urteil vom 05.09.2007 - 21 K 3395/06; BVerwG, Urteil vom 27. 1. 2010 - 6 C 22/08 (VG Köln) // neither deals with data protection related issues, however.

   There seems to be no case law addressing § 3 Nr. 16a TKG (public telecommunications network).

   § 3 Nr. 24 TKG (telecommunications service): the provision is constantly being applied, but without any further information on how to interpret it.

   AG Bonn, Urteil vom 5.7.2007 - 9 C 177/07; temporary storing of IP-addresses;
   BGH, Urt. v. 14. 6. 2012 – III ZR 227/11 (LG Verden ); providing i.a. (though very briefly) criteria on how to distinguish between telecommunication services and
telecommunications-based services in context of transfer of traffic data for billing purposes. The rules laid down for telecommunication services regarding transfer of traffic-data shall apply likewise on telecommunications-based services to provide for an equal level of protection.

§ 3 Nr. 6 TKG (Service Provider): OVG Berlin-Brandenburg, Beschluss vom 2.12.2009 - OVG 11 S 32.09 (VG Berlin) (rechtskräftig): A web-hosting provider, who offers inclusion of email services, which need to be configured by the client, is not a telecommunications service provider and therefore does not have to comply with the provisions on data retention (which were declared void by the constitutional court, since then).
7. What is your individual view of:
a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

| a. The distinction between telecommunications services and telemedia services (services of the information society) still causes significant issues of correct classification, both in theory and in practice. This triggers not only issues regarding applicable law, but also regarding competencies of authorities, as these depend on exactly this classification. These issues persist to this day. The issues become more complex when services become more complex. This becomes apparent when considering social networks. As it would be impossible to assess their nature as such, a split into the different services forming the social network in total needs to be undertaken. However, even then process of uploading content to the board of a member is of dual nature: the upload should be considered a telecommunications service, the subsequent display (making available) a telemedia service (SoIS).

The second major issue results from the fact that telecommunications data protection law has a history of almost 20 years in Germany, thereby several traditions and subtle balance systems in the codified law. The partial harmonisation through European Law has caused several issues as a non-literal transposition makes it unclear, whether the provision in questions transposes European law, whereas a literal transposition may cause – and has caused – strong unwanted side-effects on the application of the existing provisions as the original system of interlinking provisions and definitions had been disturbed. To this day the telecommunications code remains in some points confusing, as it clearly shows the parallel development both on a national and on the European level, both of which tend to be overlapping, but historically not being based upon identical concepts. This applies in particular where technical and legal terms deviate, because generally the German legal systems as a strictly positivist system requires precisely one term for one subject/functionality/legal concept to address. Using deviating terms is likely to cause confusion whether the legislator seeks to express the different nature of the two legal concepts, whereas in many cases, the reason may lie in simple fact that historically the terms have been used and shaped differently in the directives and in national laws.

b. As to the disturbance caused by European harmonisation this clearly is a side-effect which has to be accepted in exchange of the merits of European harmonisation. It appears from our perspective not unlikely that these side-effects will cease to exist over time, be it through advancing European harmonisation, or through case law. On the contrary, the distinction between telecommunications services and SoIS to this day does not appear to have brought more merits but to have caused unwanted issues. In particular the split of competences resulting from it does create at times an obstacle in efficient application of the provisions transposing the directive. |
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The principle of confidentiality didn’t have to be transposed as in Germany telecommunications, privacy has been a distinct fundamental right since the founding of the Federal Republic, which means that this fundamental right is both more powerful and richer in tradition and jurisdiction than concepts of data protection. A particular reference to telecommunications privacy is provided by § 88 TKG which provides for the details and scope of the telecommunication secrecy: The provision provides for a detailed outline of the scope of telecommunications privacy, referring also to the circumstances surrounding telecommunications, which can be seen as a – possibly a bit outdated – way of referring to traffic data. “Communications” as such is not defined by this provision, which, however, does not appear necessary, because “telecommunications” as such is legally defined in § 3 (quoted above in this study). Apart from the provisions quoted below, § 206 Strafgesetzbuch (German Criminal Code) sanctions certain cases of violation of telecommunication privacy as criminal offence. An important detail of the legal term “communications” in the context of these provisions is the fact that it is commonly understood to cover only content in transmission, not, however, content about to be transmitted by the sender, or already having been received by the person meant to receive it, which includes receiving devices and virtual post-boxed. What is protected therefore is e.g. the email in transmission, not the draft on the computer of the sender or the received email in the post-box provided by the email service provider (which, however, could be challenged in situations when such email storage might be cloud storage).

§ 88
Privacy of Telecommunications
(1) The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts.
(2) Every service provider shall be obliged to maintain telecommunications privacy. The obligation to maintain privacy also applies after the end of the activity through which such commitment arose.
(3) All persons with obligations according to subsection (2) shall be prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems. Knowledge of facts which are subject to telecommunications privacy may be used solely for the purpose referred to in sentence 1. Use of such knowledge for other purposes, in particular, passing it on to other parties, shall be permitted only insofar as provided for by this Act or any other legal provision and reference is made expressly to telecommunications activities. The reporting requirement according to section 138 of the Penal Code shall have priority.
(4) Where the telecommunications system is located on board a ship or an aircraft, the obligation to maintain privacy does not apply in relation to the captain or his second in command.
§ 89 Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy

Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others.

§ 90 Misuse of Transmitting Equipment

(1) It shall be prohibited to own, manufacture, market, import or otherwise introduce in the area of application of this Act transmitting equipment which, by its form, purports to be another object or is disguised under an object of daily use and, due to such circumstances, is particularly suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection. The prohibition on owning such transmitting equipment does not apply to any person obtaining or acquiring actual control of transmitting equipment

1. as an executive body, as a member of an executive body, as a legal representative or as a partner entitled to represent a person authorised under subsection(2);
2. from another or for another person authorised under subsection(2) if and for as long as he has to comply by virtue of service or employment relations with the directives given by the other party concerning exercise of the actual control of the transmitting equipment, or exercises actual control by virtue of a court order or an order from a public authority;
3. as a bailiff or an enforcement officer in enforcement proceedings;
4. temporarily, from a person authorised under subsection (2), for the purpose of safe custody or non-commercial conveyance to an authorised person;
5. for conveyance or storage for business purposes only;
6. by finding, provided that such person hands over the equipment without undue delay to the loser, the owner, any other party entitled to acquire the equipment or the office responsible for taking delivery of the lost property report;
7. causa mortis, provided that such person gives the transmitting equipment to an authorised person without undue delay or renders it permanently unusable; or
8. which has been rendered permanently unusable by the removal of a major component, provided that such person gives notice in writing to the Regulatory Authority of the acquisition without undue delay, stating his particulars, the type of equipment, its trademark and any manufacturing number given on the equipment, and presents prima facie evidence that the equipment has been acquired for collection purposes only.

(2) The supreme federal and state authorities with competence shall allow exceptions where these are required in the public interest, in particular for public safety reasons. Subsection (1) sentence 1 does not apply insofar as the Federal Office of Economics and Export Control (BAFA) has authorised export of the transmitting equipment.

(3) It shall be prohibited to advertise, in public or in communications intended for a relatively large group of persons, transmitting equipment by indicating that the equipment is suitable for intercepting the non-publicly spoken words of another person without his detection or for taking pictures of another person without his detection.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

It appears that this provision has not been transposed. However, it cannot be ruled out that there was no intention to transpose this provision in order to not establish such exemption and have a stricter data protection regime in Germany (2002/58/EC is considered to set a minimum standard, but not providing for full harmonisation). The explanatory report to the law implementing 2002/58/EC in telecommunications code makes no reference at all to Art. 5 II, which makes it hard to evaluate to which extent a possible non-transposition has been on purpose or not.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Exemptions from the confidentiality principle which is a Fundamental Right in Germany, cannot be constituted by case law (except a constitutional ruling on the scope of the fundamental right).

Exemptions by law can be provided under certain pre-conditions, and are manifold in the field of homeland security. Section 3 of Chapter 7 (privacy) of the *telecommunications code* covers the measures service providers have to take in order to enable surveillance for homeland security purposes. The provisions entitling authorities to conduct these surveillance measures are laid down in the respective codes governing the measures by these authorities. These are the Police Codes of the 16 German Lands regarding preventive measures of the police, Bundeskriminalamtgesetz for the Federal Criminal Police Office, Bundespolizeitgesetz for Federal Police, G10 Gesetz for the Intelligence Services, Strafprozessordnung (*Criminal Procedure Code*) for criminal investigation and prosecution (repressive measures) through the police and state prosecution. Their entirety is so vast that it appears impossible to display all these provisions here. Mostly, wire-tapping of telephony is concerned. Legally questioned was the method of wire-tapping using Trojan horse software to re-route telecommunications before encryption (so-called Quellen-TKÜ).
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   • Whether the interception of MAC addresses would entail breach of confidentiality;
   • Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   • Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The answer to the first question depends on the interpretation of the question. The *criminal code* constitutes offences (e.g. § 202b StGB, interception of data), which address (also) automated interception (sniffer-software, etc.). These transpose the cybercrime convention (albeit some of them being older and dating back to 1986), which means they are widely the same as in most CoE states.

The general data protection rules do not distinguish between automated and non-automated breaches, but refer only to automated decision-making (which supposedly is not meant here).

Interception of mac-addresses in context of telecommunications is a breach of telecommunications privacy, as mac addresses as well as IP addresses identify the devices of sender and receiver, both of which are traffic data.

The non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality as any content (as well as the headers) is protected by the fundamental right to telecommunications privacy and the provisions based upon it. Interception of telecommunications as a criminal offence does not require this communication to be encrypted, either.

The German legislation does not distinguish between content of the communications and other data relating to communications (i.e. traffic data) as long as the data is in transmission (all covered by the fundamental right to telecommunications privacy).

However, from the end of transmission onwards content data is protected by the fundamental right to informational self-determination (data protection) “only”, whereas meta-data such as traffic data remains to be protected by the telecommunications secret.

b. German law does not know particularities in terms of telecommunications being “electronic” or “private” in this sense (except TV or radio-broadcasts which address the public and therefore are not “private”). Otherwise, all telecommunications are considered “private” and as such protected, regardless of the fact whether or not it they are electronic. The only exception is § 202b StGB referred to above, which constitutes that intercepting data from a non-public (hence: private) transmission is a criminal offence. “Non-public” refers to the transmission not being meant to address the public (thereby excluding broadcasts); whereas the data being transmitted through a public telecommunications network and not being encrypted does non render such transmission “public”. Moreover, this applies for all data, not being limited to personal data.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

| a. The use of spyware is prohibited by the criminal code; §§ 202a, 202b and in particular § 202c (prohibiting acquiring, creating, selling, making available on so forth of malware, including spyware). Art. 5 III 2002/58/EC is considered to be transposed by §§ 12, 13 Telemediengesetz (n.b. the critics of BFDI referred to above, considering § 15 III TMG overriding § 12 TMG, as the former is lex specialis; causing the issue that § 15 III TMG provides for an opt-out (only)). |
| § 12 TMG General Rules |
| (1) The service provider shall collect and use personal data for providing telemedia to the extent that this law or another law addressing telemedia services explicitly allow for it, or if the user has consented. |
| § 13 II TMG: |
| (...) |
| (2) consent can be declared by electronic means, if the service provider ensures that |
| 1. the user gives consent knowingly and unmistakably, |
| 2. consent is being protocolled, |
| 3. the user is being enabled to access the content of their declaration of content at any time and |
| 4. the user is enabled to withdraw consent at any time for the future. |
| § 15 TMG Utilisation Data |
| (1) The service provider shall be entitled to collect and use personal data of the service’s users only to the extent necessary to enable and invoice the use of telemedia (utilisation data). |
| Utilisation data is in particular |
| 1. any characteristics to identify the user of the service, |
| 2. any details on beginning and end of usage, and |
| 3. details on content/services used by the user. |
| (2) The service provider shall be entitled to link a user’s utilisation data sets regarding the use of different telemedia to the extent necessary for billing purposes. |
| (3) For the purposes of advertising, market research or in order to improve the service design based upon existing needs, the service provider may create utilisation profiles linked to pseudonyms, if the user does not opt-out. The service provider shall refer the user to his right to opt out pursuant to Sub-section 13 No. 1. Such profiles shall not be linked to any data on the identity of user. |
| (4) The service provider shall be entitled to use utilisation data beyond the session’s termination only if necessary for invoicing the recipient of the service (invoicing data). The service provider is entitled to keep the data if blocked (rendered temporarily inaccessible – comment of the translator) in order to meet retention periods laid down by law or contractual obligation. |
| [...] |
b. **§ 15 TMG** does not distinguish between different types of cookies. However, the retention and use of any utilisation data are restricted by sub-section 4 to billing purposes and contractual obligation. Such contractual obligations may be rooted in the agreement to use the service, which may require certain information to be stored longer than one particular session. That apart, data usage in any case is possible through the user’s consent, which can be obtained through a privacy policy (§ 12 I and II TMG).
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Legal requirements of informed consent regarding the use of telemedia services (SoIS) are laid down in § 13 TMG, which provides for the ranges of information to be provided and formal details regarding electronic consent; and which is backed up by §§4 and 4a BDSG.

There is no requirement to use pop-up screens or consent bars; however § 12 I TMG in conjunction with § 13 II Nr. 1 TMG can be read as requiring an opt-in. However, that particular provision would not apply on cookies, because § 15 III TMG explicitly provides for an opt-out being sufficient, which overrides § 13 II TMG by the former being the more specific provision.

Cookies which are technically needed in order to enable service provision can be used without the need of consent at all (§ 15 I TMG, see translation above).

There are no particular rules applying to cookies regarding the information which needs to be provided beyond the rules applying for all telemedia services laid down in §§ 12, 13 TMG (and which were more specific than the rules laid down in general data protection laws, which applies subsidiary)

These rules do not distinguish between mobile devices and other devices. In that regard, no particularities regarding mobile devices are apparent

Setting up of cookies before/without the user having given consent is definitely possible to the extent provided for by § 15 I TMG (cookies needed for billing or technical purposes (to enable the service)). Otherwise, the user would need to be given the opportunity to opt out. By the wording of the law (see translation above) it is not entirely clear, whether this opportunity needs to be given before loading the page at all, or whether it would be sufficient to provide the possibility to opt out once the page has been loaded. “If the user doesn’t opt-out” both implies that using cookies is legal as long as the user has not taken action to prevent it; whereas, obviously, this requires that such option exists.
How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

i) To the extent to which the sole transmission of a communication is concerned, it appears that this would be a telecommunications service (and not a telemedia service), which would render the provisions on cookies generally inapplicable (§ 1 TMG, or, if a “mixed” service “§ 12 III TMG; both which rule out the application of § 15 I – VII TMG inapplicable).

ii) § 15 I TMG provides for usage of utilisation data (including cookies) which are technically required to provide the service to the user being legitimate without any further requirements.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

It does not appear that this particular issue has met specific attention yet. As the German law provides for an opt-out only, the question of obtaining consent is handled differently. Some services explicitly ask for consent (nike.de; http://help-de-eu.nike.com/app/answers/detail/a_id/16755/~/datenschutz--und-cookie-richtlinie), other inform about using cookies in their privacy policy (e.g. the website of the German Federal Ministry for Science and Research, http://www.bmbf.de/de/7540.php ). Zalando.de uses a banner stating that the provider assumes consent to using cookies, if the user continues to use the website.

The subject of cookies appears sporadically in the activity reports of the data protection authorities, but mainly with a focus on the unclear legal situation, or through reporting that the issue has been discussed in a working party or similar. As to a case of enforcement in Hamburg see next question.

Statistics on blocking cookies in Germany:

9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

| a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases) |
| b. national courts through rendering of case law |

| a. Data Protection Commissioner of the Land Schleswig-Holstein on Cooking Warning System: |
| Data protection commissioner of the Land Bavaria on datr-cookie used by facebook (p. 30): |
| Data protection commissioner of the Land Hamburg on the case “hamburg.de”, the website of the city of Hamburg which had used cookies in a way considered illegitimate by the authority: |

https://www.datenschutzzentrum.de/selbstdatenschutz/p3p/p3p_ie6_2.htm

In general it does not appear as if the matter of cookies has triggered intense discussion on the substantial level, except the public debate mentioned earlier on whether or not § 15 III TMG would be sufficient to transpose the directive.

b. There are not many recent cases regarding cookies.

LG Berlin, Urteil vom 19.11.2013 - 15 O 402/12; general terms and conditions on cookies breaching the rule of pseudonymous use of telemedia services and thereby being void.

VG Schleswig, Urteil vom 09.10.2013 - 8 A 218/11; on the particular cookies „datr-cookie“ and “c-user cookie” used on facebook pages.

An old case dating back to the year 2000 was AG Ulm, Urteil vom 29. 10. 1999 - 2 C 1038/99 (rechtskräftig): an internet service provider offering a virtual mall to online shop providers may declare the contract with such online shop providers void if these are using cookies not needed for the service they are providing.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Yes, albeit the fact that the German legislation is not entirely coherent with the EU legislation seems to have produces quite some confusion on the market as it remains unclear whether the German legislation providing for an opt-out only is overruled by the directive which might be applied directly, should one assume the German transposition being insufficient and the further pre-conditions for direct application of the directive being given.</td>
</tr>
<tr>
<td>b.</td>
<td>A problem might be enforcement, already in terms of capacities of the authorities. This, however, does not necessarily appear to be an issue which can be solved by amending the law.</td>
</tr>
</tbody>
</table>
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 3 nr. 30 TKG defines traffic data as “data collected, processed or used in the provision of a telecommunications service”</td>
</tr>
<tr>
<td>§ 3 Nr. 24 TKG defines &quot;telecommunications services&quot; as “means services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting;”</td>
</tr>
<tr>
<td>§ 96 TKG legitimates collection and use of traffic data i.a. for “for setup and maintenance of the telecommunications connection and for billing purposes.”</td>
</tr>
<tr>
<td>This does not, other than the directive, exclude broadcasting.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

§ 96 Traffic Data

(1) The service provider may collect and use the following traffic data to the extent required for the purposes set out in this Chapter—
   1. the number or other identification of the lines in question or of the terminal, personal authorisation codes, additionally the card number when customer cards are used, additionally the location data when mobile handsets are used;
   2. the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
   3. the telecommunications service used by the user;
   4. the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
   5. any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

This traffic data may be used only to the extent that it is necessary for the purposes laid down in sentence 1, in other codified provisions or to establish further telecommunications connections. Otherwise traffic data needs to be deleted immediately by the service provider.

(2) Any collection or use of traffic data exceeding the allowances laid down in sub-section 1 is prohibited.

(3) The service provider may use subscriber-related traffic data used by the provider of a publicly available telecommunications service for the purpose of marketing telecommunications services, shaping telecommunications services to suit the needs of the market or for the provision of value added services for the duration necessary only where the data subject has given his consent to such use. The data of the called party are to be made anonymous without undue delay. Traffic data relating to the destination number may be used by the service provider for the purpose referred to in sentence 1 only with the consent of the called party. In such case, the called party data are to be made anonymous without undue delay.

(4) When obtaining consent, the service provider is to inform the subscriber of the data types which are to be processed for the purposes referred to in subsection (3) sentence 1 and of the storage duration. Additionally, the subscriber’s attention is to be drawn to the possibility of withdrawing his consent at any time.

Art. 6 2002/58/EC:
1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

⇒ This sub-section is transposed by sub-section I of § 96 TKG at the end and in particular by sub-section II.
2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

   ➔ § 97 TKG, establishing a maximum period of 6 months for storing the data (unless the subscriber would challenge the invoice, in which case the data may be kept until the matter has been settled) and requiring to extract all data needed for billing immediate and to delete all other data.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

   ➔ § 96 III TKG

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

   ➔ § 96 IV TKG.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

   ➔ § 97 I in conjunction with §§ 88, 93, 95, 96, 97, 99, 100 TKG.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

   This follows from the general procedure rules to use evidence in front of court.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Any traffic data not collected for the purposes laid down in § 96 I 1 TKG are to be deleted immediately after connection termination (§ 96 I 3 TKG). Any traffic data collected for the purposes laid down in § 96 I 1 TKG are to be deleted immediately, if no longer needed for these purposes (§ 96 I 2 TKG).

Any data not needed for billing purposes is to be deleted immediately after connection termination, any billing data may be kept up to six month, unless the subscriber challenges the invoice, in which case the data may be kept until the matter has been settled, § 97 III TKG.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

BGH, Urt. v. 7. 2. 2013 – III ZR 200/11 (LG Deggendorf); Supreme Court: cession of claims does not legitimise transfer of traffic data.

BGH, Urt. v. 13. 1. 2011 – III ZR 146/10 (OLG Frankfurt a. M.); Supreme Court on the pre-conditions for storing IP-addresses for billing purposes.

OLG Düsseldorf, Beschluss vom 7.3.2013 - I-20 W 121/12, I-20 W 5/13 (LG Düsseldorf) (rechtsskräftig); no obligation for internet service providers to store IP addresses to inform copyright-holders claiming an infringement at a later point in time.

Still under the rule of the former version of § 96 TKG the supreme court has ruled that IP addresses have to be deleted, once the connection has been terminated (that was a flat rate model which didn’t require this data for billing purposes); BGH Az. III ZR 40/06.

BGH, Urteil vom 13. 1. 2011 - 3 StR 332/10 (LG Hannover) is a case in which the Supreme Court ruled on the legitimacy of using mobile phones’ traffic data in criminal proceedings. That particular case concerned traffic data which was stored longer than necessary by the provider in order to meet the requirements set up by the former rules on data retention. While these rules had been declared void by the constitutional court in 2010, the constitutional court previously had issued a provisional order in 2008 setting up strict requirements for usage of traffic data in criminal proceedings which was kept for data retention only. The data in question was transferred to the prosecutors between the provisional order of 2008 and the final ruling of 2010. That triggered the question of whether such evidence was excluded from the proceedings or not. The supreme court reasoned that, although the law legitimating data retention was declared void subsequently and thereby needs to be considered void ex tunc, the provisional order of 2008 is as such – as all ruling of the constitutional court – of legislative virtue and replaces law. As the strict pre-conditions for using traffic data in criminal proceedings had been met and as the data stemmed from the period between the provisional order and the final ruling, bringing such evidence was not excluded, but legitimate.

// Guidelines on traffic data issues by BFDI (Federal German Data Protection Authority) and Bundesnetzagentur (Federal Networks Regulation Authority) jointly: http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenZumSpeichernVonVerkehrsdaten.pdf?__blob=publicationFile
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Yes, these rules appear to be clear and set a high standard of privacy protection.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

§ 3 Nr. 19 TKG defines location data as “any data that is collected or used in a telecommunications network or by a telecommunications service and which determine the location of the device of a user of a publicly available telecommunications service.”

Art. 2 (c) 2002/58/EC:

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

There appears to be no deviation between the two definitions.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Art. 9 2002/58/EC Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

§ 98 TKG Location Data

(1) Location data relating to users of public telecommunications networks or publicly available telecommunications services may be processed only when they have been made anonymous or with the consent of the subscriber to the extent and for the duration necessary for the provision of value added services. In such case the provider of a value added service shall inform the user about each detection of location of the mobile device by a text message to the mobile device which has the location of which has been detected. This does not apply if the location is only displayed on the mobile device the location data of which has been detected. If location data of a mobile device shall be processed for a value added service which include transmission of location data of a mobile device to another subscriber or to any third party non being provider of a value added service, the subscriber is required in deviation of § 94 to express their consent explicitly, separately and in writing towards the provider of the value added service. In this case the obligation laid down in sentence 2 applies to the provider of the value added service accordingly. The provider of a value added service shall use the neccessary inventory data to meet the obligation laid down in sentence 2. The subscriber shall inform his co-users of all such consent given. Consent may be withdrawn at any time.

(2) Where the consent of the subscriber to the processing of location data has been obtained, the
subscriber shall continue to have the possibility, using a simple means and free of charge, of
temporarily refusing the processing of such data for each connection to the network or for each
transmission of a communication.

(3) In respect of calls to the emergency call number "112", to telephone numbers determined in the
ordinance as provided for under § 108(2) and to the telephone number "124124", the service
provider shall ensure that the transmission of location data is not ruled out on a per-call or a per-
line basis.

(4) Processing of location data other than traffic data in accordance with paragraphs 1 and 2
must be restricted to persons acting under the authority of the provider of the public
communications network or publicly available communications service or of the third party
providing the value added service, and must be restricted to what is necessary for the purposes of
providing the value added service.

As can be seen from the comparison displayed above, most of Art. 9 2002/58/EC has been
transposed almost literally, with the exception of sentence 2. Whether the obligation to inform
about the kind of data collected, the purposes of processing and the possible transfer to third
parties follows the general data protection rules - which supposedly was the reason why the
legislator did non literally transpose this particular sentence from Art. 9 in § 98 TKG, can to some
extent be challenged. While the requirement to inform about the purposes of collecting and
processing location data explicitly is laid down in the rules on informed consent in §§ 4, 4a BDSG,
these provisions require only informing about the categories of possible receivers of such data,
whether the directive at least allows an interpretation which would require to inform about the
receiving parties explicitly. Informing about the type of data beeing processed and the duration of
processing are not mentioned explicitly in §§ 4, 4a BDSG, although it can be well reasoned that at
least implicitly these provisions require the provider to (also) inform in that regard. However. a
more literal transposition of the directive possibly might have been more helpful in order to avoid
legal disagreements and diverging interpretation of the national rules, where the directive
provides a clear framework. Anyway, of course the national law has to be interpreted in
accordance with the directive, which should - in theory - lead to absolute synchronism.

That apart, the German legislation provides for a couple of additional rules, such as the
requirement to inform co-users of a mobile device. The rules on emergency calls transpose Art. 10
b) of the directive.

§ 98 I 1 TKG does not specify any categories of controllers, meaning that whoever collects of
processes location data of user of public telecommunications networks or publicly available
telecommunications services, it bound to comply with this provision. Consequently, by its wording
it applies on any third party harvesting data (e.g. when downloading applicatons).
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

| Location data, just as laid down in the directive, needs to be anonymised, if the user has not given consent to the particular use of the data. It needs to be deleted, once it is no longer needed for providing the value added service (except the user would have consented to any secondary use). In particular, the general data protection rules require any data, which is no longer needed for the purposes it was collected for originally, to be deleted. |
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>a. BFDI on location data:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.bfdi.bund.de/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/LocationBasedServices.html?nn=409870">http://www.bfdi.bund.de/DE/Themen/KommunikationsdiensteMedien/Telekommunikation/Artikel/LocationBasedServices.html?nn=409870</a></td>
<td></td>
</tr>
</tbody>
</table>

The document explains on an abstract level addressing the general, uninformed public the nature of location data, the fact that such data is being created frequently through ordinary use of mobile phones (without the need to subscribe to particular services) and the legislative rules applicable. Moreover, it emphasises that these rules apply only to data that was collected in telecommunications networks, whereas the provisions remain inapplicable to location data collected through GPS devices (e.g. in smart phones) which are being used in telemedia services only (e.g. google maps). In such case there are no rules but the general data protection rules applicable, which leave a certain gap regarding location data collected in that way.

b. It does not appear that there has been any case-law on location data relevant for this study.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The rules on location data appear to be very clear and consistent to achieve the aims for which they were introduced. One exception might be the lack of a literal transposition of Art. 9 I 2 2002/58/EG, because - although the same follows from the general rules - it might have been clearer and more appropriate to repeat these conditions in the telecommunications code in § 98 TKG.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

§ 7 UWG (Gesetz gegen den unlauteren Wettbewerb; Law against unfair competition)
Undue Inconveniences

(1) Any commercial action, which results in any undue inconvenience of another market player, is illegal. This applies in particular to any marketing, despite the market player approached noticeably does not wish for such advertisement.
(2) An undue inconvenience always needs to be assumed
   1. regarding any marketing using any means of commercial communication suitable for distance selling and not mentioned under No. 2. or 3., through the use of which a consumer is being persistently approached although noticeably not wishing for such advertisement;
   2. regarding marketing through a telephone call to a consumer without their previously given explicit consent or to any other market player without at least their presumable consent,
   3. regarding any marketing through using an automated calling system, a fax or electronic post, without explicit consent previously given by the addressee, or
   4. regarding marketing through a message,
      a) regarding which the identity of the sender, on behalf of which the message is being transferred, is being disguised or concealed or
      b) which is breaching § 6 I Telemediengesetz or through which the addressee is being asked to visit a website, which is in breach of that provision, or
      c) regarding which a valid address is lacking, to which the addressee can point a request to stop such messages, without resulting in any communications costs other than the base rate.
(3) Notwithstanding sub-section 2 No. 3 an undue inconvenience cannot be assumed for any marketing through electronic posts, if
   1. a trader has collected the electronic post address of a client in context of selling a good or a service,
   2. the trader is using the address for direct marketing for similar goods or services offered by themselves,
the client has not opted out and
4. the client is being informed clearly and distinctly while collecting and during each use of this address that they can object the use at any time, without any costs occurring other than the base rate.

Art. 13 2002/58/EC

1. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

⇒ transposed by § 7 II Nr. 3 UWG; German law requires explicit consent; “automated communication systems” other than calling systems are not mentioned, German law is not limited to “direct” marketing.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

⇒ transposed by § 7 III UWG; German law refers to “traders” as used in the consumer protection directive, German law does not refer to 95/46/EC or the transposition of it; German law does not require objection being free of charge, but only free of any additional charge (meaning that a call to object does not need to be toll free, but shall not exceed the base rate); German law does not refer to “an easy manner”

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

⇒ Such unsolicited communications “not being allowed” follows directly from the wording of the transpositions of sub-sections I and II; thereby from the wording of § 7 II Nr. 3 UWG and §7 III UWG. Germany has chosen to stick with the opt-in procedure regarding telephone calls to consumers; whereas for any other market players a presumed consent is sufficient (§ 7 II N2. UWG); for other means of distance selling § 7 II Nr. 1 UWG applies; providing for an opt-out procedure in all cases not mentioned under Nr. 2 (telephone calls) and Nr. 3 (all cases of Art. 13 I 2002/58/EC).

Measures to ensure the prohibition of unsolicited communications are e.g. penalties laid down in

1 Ohly, in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, § 7 Rn. 8.
4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

§ 7 II Nr. 4 UWG; transposes this paragraph almost verbatim (though systematically slightly differently as the second case and the fourth case are grouped as both are referring to the same provision). The norm also refers (obviously to the German transposition of Art. 6 2000/31/EC (§ 6 I TMG) and not to the directive itself. It also repeats the obligation to provide means to send a request that such communication should cease which do not cause any cost exceeding the base rate.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

Legal persons and natural persons not being consumers are protected through § 7 I, II Nr. 3 and 4 UWG; which means that all provisions transposing the directive apply to both natural and legal persons who are addressees of unsolicited communications.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.

§ 20 I UWG (only applying for breaches of § 7 II Nr. 3 UWG), and the rights to claim damages and omission laid down in § 8 UWG for competitors and consumer protection organizations; and following from the general rules of civil law (§ 823 BGB and § 1004 BGB) for consumers directly affected.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Art. 13 I is transposed by § 7 I, II Nr. 3 UWG.

(1) Any commercial action, which results in any undue inconvenience of another market player, is illegal. This applies in particular to any marketing, despite the market player approached noticeably does not wish for such advertisement.

(2) An undue inconvenience always needs to be assumed [...]

3. regarding any marketing through using an automated calling system, a fax or electronic post, without explicit consent previously given by the addressee [...]

German law requires explicit consent; “automated communication systems” other than calling systems are not mentioned, German law is not limited to “direct” marketing.

Regarding Art. 13 III Germany has chosen to stick with the opt-in procedure regarding telephone calls to consumers; whereas for any other market players a presumed consent is sufficient (§ 7 II N2. UWG); for other means of distance selling § 7 II Nr. 1 UWG applies; providing for an opt-out procedure in all cases not mentioned under Nr. 2 (telephone calls) and Nr. 3 (all cases of Art. 13 I 2002/58/EC).

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

1. The opt-out mechanism provided for in Art. 13 II (➔ § 7 II Nr. 3, III UWG).

2. The opt-out mechanism for all means of distance selling which are not mentioned by Art. 13 I 2002/58/EC and which are not telephone calls.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

There is a certain distinction, but only a relatively rough one: All means (automated calling machines, fax and email) which are regulated by Art. 13 I 2002/58/EC are regulated distinctly in German Law as well (§ 7 II Nr. 3 UWG). That apart, telephone calls are regulated distinctly in § 7 II Nr. 2 UWG. That apart, there is not technology specific regulation such as addressing social media or instant messaging explicitly or exclusively.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. There is no national enforcement authority in charge of unsolicited communications (except for cases regarding unsolicited communications by telecommunications service providers, regarding which there are no specific guidelines)

b. BGH - Urteil vom 12.09.2013 - I ZR 208/1; a company providing the service to send recommending emails to a third party for users of its website is legally equally responsible as if these emails were sent by the company itself.

BGH, Urteil vom 25.10.2012 - I ZR 169/10; consent to telephone calls for direct marketing can be obtained through general terms and conditions, if - and only if - the user is informed sufficiently about the fact that her consent covers such phone calls and also about the nature of such calls and the companies which are entitled to call.

BGH - Urteil vom 10.02.2011 - I ZR 164/09; German law providing for an opt-in regarding unsolicited calls does not breach law of the European Union; consent requires comprehensive documentation for each consumer.

BGH: Beschluss vom 10.12.2009 - I ZR 201/07; direct marketing through email requires explicit or implicit consent, whereas the mere assumption of consent is not sufficient; a car trader offering to contact him through email does not mean he implicitly consents to receiving any other mail than those concerning car trades.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The rules appear to be clear from the legal point of view; and does the case law. A practical issue occurs with enforcement: spam from outside the EU is frequent and hard to fight by legal means; spam violating the rule to clearly refer to the author makes it difficult for consumers to take any legal action. That apart, in most cases costs and efforts of taking legal actions in general may hinder consumers to take any legal steps against spam.
COUNTRY REPORT

DENMARK

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Andrej Savin, Copenhagen Business School

Date: 18 August 2014
Contents

Part 1: Management summary ................................................................. 3
Part 2: Answers to the questionnaire ....................................................... 4
Management summary for Denmark:

- The ePrivacy Directive has been implemented in Denmark through a range of legislative instruments, beginning with the Act on Electronic Communications and Services but leading into more important Executive Order on Provision of Electronic Services and the Cookie Order. This structure could be confusing for outsiders as it involves several acts, all of which are concerned not just with one but with several directives. The use of ministerial orders can be explained by the need to introduce flexibility into the fast-changing area, but avoiding a lengthy and complicated full legislative process.

- The scope of the legislation leaves no surprises. In terms of Article 3, the Directive applies to all services that target Denmark. In terms of Article 5, it applies to services which are established in Denmark. The implementation in terms of the networks, services or providers is largely following the Directive. The guidelines to the implementing Provision Order give a comprehensive explanation of the key terms and how they may be applied in practice.

- Art. 5.3 of the Directive has been the subject of a special ministerial order (the Cookie Order) which has, in turn, been followed by comprehensive and practically-oriented Guidelines. The latter take cognizance of the many different types of cookies and address them (even though the legislation itself does not). The enforcing authority (Danish Business Authority) emphasized that location data is not limited to cookies and that the reality of electronic life may have overtaken the legislation.

- Traffic and location data have been implemented in line with what is required in the Directive. Although the wording is occasionally different, it follows the general direction and the spirit of the Directive.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been implemented in the Market Practices Act. The regime chosen is the strict opt-in regime for emails, automated calling and the fax machines with the possibility to use other means of communication only if the users have not placed themselves on the opt-out list. Guidelines have been published on the website of the Consumer Ombudsman.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)


- The Act is complemented by ministerial orders (Executive Orders). These are specifically called for in Articles 3, 4, 5, 8, 9, 61 and 81 of the Act on Electronic Communications and Services.

- The actual implementation of the ePrivacy Directive is to be found in these ministerial orders as the Act concerns itself with other general telecommunications and electronic commerce issues. In fact, the Act implements a range of different EU Directives, among which are the Access Directive, the Framework Directive, the Universal Service Directive, the Authorisation Directive and others.

- The complete list of all the acts that implement the Directive (Consolidated law, the Act and executive orders with interpretative Guidelines) can be found on: [https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058](https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058)

  - The general provisions of the ePrivacy Directive (other than the ones mentioned below) are to be found in the Executive Order on the Provision of Electronic Communications Networks and Services (Executive Order No. 713 of 23 June 2011), [https://www.retsinformation.dk/Forms/R0710.aspx?id=137773](https://www.retsinformation.dk/Forms/R0710.aspx?id=137773), unofficial English version at [https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf](https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf), hereafter “the Provision Order”.

  - The provisions concerning cookies are to be found in the Executive Order on Information and Consent Required in Case of Storing or Accessing Information in End-User Terminal Equipment, (Executive Order No. 1148 of 9 December 2011), [https://www.retsinformation.dk/Forms/R0710.aspx?id=139279](https://www.retsinformation.dk/Forms/R0710.aspx?id=139279), unofficial English version at [https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf](https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf), hereafter “the Cookie Order”.

- The provisions on unsolicited marketing have been implemented in the Marketing Practices Act (Act
All of the laws (the Act and the executive orders) have been in existence prior to the changes required in the 2009 EU telecoms reform. Consequently, the older versions of the above acts can also be found at: [https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058](https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058)

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed in Danish law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2 (Definitions)</td>
<td>Article 2 of the Electronic Communications Act, Article 2 of the Provision Order and Article 2 of the Cookie Order.</td>
<td><a href="https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058">https://www.retsinformation.dk/Forms/R0900.aspx?s30=32002L0058</a></td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
<td>Article 1 of the Provision Order, Article 1 of the Cookie Order (for scope) and Article 2 of the Provision Order and Article 2 of the Cookie Order (for definitions)</td>
<td><a href="https://www.retsinformation.dk/Forms/R0710.aspx?id=137773">https://www.retsinformation.dk/Forms/R0710.aspx?id=137773</a>, Unofficial English version at <a href="https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf">https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf</a></td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>The general legal basis is found in Articles 7 to 9 of the Electronic Communications Act but the specific implementation is in Articles 23 and 24 of the Provision Order.</td>
<td><a href="https://www.retsinformation.dk/Forms/R0710.aspx?id=137773">https://www.retsinformation.dk/Forms/R0710.aspx?id=137773</a>, Unofficial English version at <a href="https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf">https://erhvervsstyrelsen.dk/sites/default/files/media/udbudsbekendtgorelsen-engelsk-udgave.pdf</a></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>The general legal basis is found in Articles 7 to 9 of the Electronic Communications Act but the specific implementation is in Articles 23 and 24 of the Provision Order.</td>
<td><a href="https://www.retsinformation.dk/Forms/R0710.aspx?id=139279">https://www.retsinformation.dk/Forms/R0710.aspx?id=139279</a>, Unofficial English version at <a href="https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf">https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf</a></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Article 3 of the Cookie Order</td>
<td><a href="https://www.retsinformation.dk/Forms/R0710.aspx?id=139279">https://www.retsinformation.dk/Forms/R0710.aspx?id=139279</a></td>
</tr>
<tr>
<td>Full name of the authority</td>
<td>English translation of the short name</td>
<td>The part or provision(s) it supervises</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Erhvervsstyrelsen</td>
<td>Danish Business Authority</td>
<td>All provisions except the ones specifically listed below</td>
</tr>
<tr>
<td>Datatilsynet</td>
<td>Data Protection Authority</td>
<td>General data protection</td>
</tr>
<tr>
<td>Teleklagenævnet</td>
<td>The Telecommunications Complaints Board</td>
<td>Telecommunications side of the ePrivacy Directive, namely complaints relating to telecoms violations. This will mostly affect corporate players and the government</td>
</tr>
<tr>
<td>Forbrugerombudsmanden</td>
<td>Danish Consumer Ombudsman</td>
<td>Consumers complaints of general and specific nature, unsolicited communications</td>
</tr>
<tr>
<td>Konkurrence- og Forbrugerstyrelsen</td>
<td>Danish Competition and Consumer Authority</td>
<td>Unsolicited Communications</td>
</tr>
</tbody>
</table>

2. An enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

Explanation:
- *Erhvervstyrelen* is the main authority named in the Electronic Communications Act and, therefore, the main authority in charge of the ePrivacy Directive. This area used to fall under the competence of an authority called *IT- og Telestyrelen* (IT and Telecommunications Authority) but this body, along with some others, have been merged into the present one. A section within the Authority now deals with IT issues and is called *Tele og Internet* (Telecoms and Internet).
- The Data Protection Authority maintains its general competence over breach of data protection laws. In cases where a breach of the ePrivacy Directive also constitutes a breach of general data protection laws, this authority will maintain its competence.
- The telecommunications complaints board will have the authority to hear complaints in cases where breaches of the ePrivacy Directive primarily concern telecommunications issues.
- The Consumer Ombudsman has the general capacity to protect consumers, particularly in cases concerning Marketing Practices Act violations.
- The Danish Competition and Consumer Authority has the competence to monitor various aspects concerning competition law but also general consumer protection.
- The competence seems, therefore, to be split between a number of authorities. There is insufficient case-law to confirm which authority is dominant.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The Act defines electronic communication **networks** in Article 2(4) as “Any form of radio frequency or cable based telecommunications infrastructure used for handling electronic communications services.” Public electronic communications networks are those which are “made available to a number of end-users or providers of electronic communications” if those are not specified in advance. Public pay telephony as well as broadcasting by any antenna equipment, digital or analogue, are excluded. (See Guidelines to Provision Order, http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf, page 4). On-demand and over-the-net TV and telephony are, therefore, included although doubts exist over cases where TV is bundled with the Internet and provided through the broadband line.

The Act defines **electronic communication services** in Article 2(7) as those “consisting wholly or mainly in electronic conveyance of communications in the form of sound, images, text or combinations thereof, by means of radio or telecommunications techniques, between network termination points, including two-way and one-way communications.” Public electronic communication services are defined in Article 2(8) as those “made available to a number of end-users or providers of electronic communications networks or services who have not been specified in advance.” Article 2(9) defines information and content services as those “to which other end-users get access via electronic communications networks or services on the basis of an individual request.”

Article 2 of the Provision Order defines “prepaid electronic communications services” as services where the end-user, “via purchase of a card or electronic communications services comparable therewith, prepays the combined service, including the current usage.” Value-added services are defined as those which require “the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.”

**Providers** are defined in Article 2 of the Act as “any person who makes products, electronic communications networks or services governed by this Act available to other parties on a commercial basis.” Commercial providers are defined in the same article as those who “for commercial purposes, offers products or electronic communications networks or services governed by this Act as its main service or as a non-accessory part of its business.”

In general, Danish legislation contains straightforward definitions of the three terms in question, occasionally providing more detail (as is the case for ‘services’). These definitions are in line with other relevant legal frameworks (e.g. with regard to general electronic commerce).
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

No straightforward answer can be given to this question.

The wording itself makes no specific mention of any VoIP, webmail or location based services. It can be inferred from the general definitions (given under the answer to question 3 above) as well as from the context of the Provision Order (in particular, the passages on location data) that such services do fall within the scope of the implementation. There is, in any case, nothing explicit in the text that would prevent from being considered such and, indirectly, through the Provision Order, one can conclude that any non-antenna and non-payphone sending of signals is covered.

It is worth remarking that the legislative competence in the area seems to be mixed. While telecommunications services are subject to one legislative regime, electronic commerce falls under another and audio-visual services under yet another regime. This may create uncertainty as to whether one, two or all three apply to the three situations outlined in the question. This has not yet been resolved in Danish practice.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

<table>
<thead>
<tr>
<th><strong>The answer to this question is not straightforward.</strong> The Act does not contain provisions on its territorial scope and the same is true for the Executive Orders that implement the ePrivacy Directive. The generic language of the Act would seem to suggest that it applies in all situations where services are provided on Danish territory, irrespective of the nature of the provider, its corporate seat, ownership structure, etc. The general supervisory/enforcement authority of the Danish agencies confirms this.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The state of confusion in this area has been confirmed in 2009 when Data Protection Agency began exploring its authority over Facebook (see <a href="http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook.pdf">http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook.pdf</a>). The Agency reiterated that “the Working Party is of the opinion that the national law of the Member State where the user’s personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk.” Somewhat surprisingly, it asked Facebook whether it considered itself a data controller within the meaning of the Data Protection Directive and asked it to appoint a representative for Denmark. This debate has not been brought to a conclusion and the state of suspense remains.</strong></td>
</tr>
<tr>
<td><strong>The correct way to interpret the provisions would be to consider that electronic services offered on the Danish territory are covered. In that sense, at least theoretically speaking, a service provider from another country, irrespective of whether this is a EU country or not, would fall under the territorial scope of the Danish laws in all cases where the service is accessed. The Danish Business Authority, however, emphasized that Article 5 only applies to businesses established in Denmark.</strong></td>
</tr>
<tr>
<td><strong>No cases have been reported involving an extraterritorial element. It is worth noting that, due to harmonization, intra-EU cases are unlikely to raise serious differences.</strong></td>
</tr>
</tbody>
</table>
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. No official guidance exists on the Electronic Communications Act. With regard to the Provision Order official guidelines exist: Vejledning til udbudsbekendtgørelsen, of 1 October 2012, available at [http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf](http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf) (in Danish). In this ‘order’, the authorities explain that some of the laws in the area apply to businesses only while other mainly to consumers. Rather than elaborate on this, they refer to the Telecommunications Law. No further definitions or clarifications are given on networks, services or providers, except one:

The Guidelines (page 6) specifically mention cases where the provision of internet services is packaged with radio and TV provision. This often the case in Europe, where a package containing broadband, internet or regular telephony and cable or internet TV is bundled together and offered at a discount. In those situations, the radio and TV distribution part of the service will be treated as antenna-provided TV and will be taken out of the scope of these laws, even though the Internet itself will be in.

b. No information exists on this.
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically
      consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

a. Danish telecommunications and electronic services providers suffer from the same
   uncertainties arising out of convergence of technologies that affect other EU states. With
   regard to the scope, there is an obvious lack of clarity as to what the rules apply to (content
   or services) and in what situations. This is addressed neither in the legal texts themselves
   nor in the guidelines. Furthermore, the territorial scope (Danish vs EU vs non-EU providers)
   is left undefined.

   With regard to clarity, the main legal texts cover various EU directives and refer to
   executive orders extensively. As a consequence, the implementation of a particular EU
   directive in this area is often to be found in multiple documents. This is difficult to follow
   and work with. On the other hand, the guidelines (the Provision Order Guidelines and the
   Cookie Order guidelines) are written clearly and comprehensively.

b. While it is not likely that the enforcement method and the use of ministerial orders will be
   changed, it would be possible to issue further guidelines on the issues above. In this
   context. Most important here may be the clarification of territorial scope.
B. Confidentiality obligations

<table>
<thead>
<tr>
<th>1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The implementation of this provision is split between several acts.</td>
</tr>
<tr>
<td>The general framework is to be found in Articles 7 to 9 of the Act. These articles, under the title “Secrecy of electronic communications, information security, processing of personal data, assistance for interception etc.” provides a general legal framework for information security. Article 7 provides that owners of electronic communication services shall not “be entitled without authorisation to disclose or utilise information about other persons’ use of the network or the service or the content thereof that comes to their knowledge in connection with the provision of electronic communications networks or services.” Furthermore they must take measures to ensure that information about other persons’ use of the network is not available to unauthorized persons. Article 152 of the Danish Penal Code covers any violations of this provision. Article 8(1), however, delegates the creation of rules for “minimum requirements for information security and processing” for providers to the Minister for Science, Technology and Innovation. Article 8(2) delegates the creation of the rules for “natural and legal persons’ storing of information on end-users’ terminal equipment” and access to this information to the same Ministry.</td>
</tr>
<tr>
<td>Ministerial Order No. 988 of 28 September 2006 (available only in Danish at <a href="https://www.retsinformation.dk/Forms/R0710.aspx?id=2445">https://www.retsinformation.dk/Forms/R0710.aspx?id=2445</a>), known as “the Logging Order”, was enacted in pursuit of the Data Retention Directive. As such, it modifies the implementation of ePrivacy Directive in its area of applicability. It is not clear what will happen with this law following the recent declaration of invalidity of the Data Protection Directive by the CJEU.</td>
</tr>
<tr>
<td>Articles 23 and 24 of the Provision Order, entitled “Processing of traffic and location data” specifically require erasure or anonymization of traffic and location data and only allow it in specifically defined cases or upon user’s consent.</td>
</tr>
</tbody>
</table>
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Article 23 of the Provision Order permits processing “for the purposes of subscriber billing and interconnection payments.” Such storing is permitted “only up to the end of the period during which the bill may lawfully be challenged or payment pursued”. This, however, implements Article 6, not 5(2). There does not seem to be a direct implementation of Article 5(2) in Danish legislation. No other elaboration on the subject is offered in any of the other implementation documents.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Article 10 of the Act obliges providers to arrange the equipment in a manner, which will enable the police to access the information about traffic and to access historical data and, as the text of the Act calls it: “forward-looking data”, to intercept and observe, provided that any such action is in compliance with Parts 71 and 74 of the Administration of Justice Act.

Further exceptions are provided in the Provision Order, which in Article 23(1) refers to Article 786(4) of the Administration of Justice Act, and Article 24(1), which refers to Article 791 of the Administration of Justice Act. The former allows police access to confidential information as part of an ongoing investigation. Such requests are limited to the general rules on injunctions for securing evidence in criminal matters. The latter deals with the evidence already in police hands and confirms an obligation to destroy it where it is no longer needed.

This issue is also directly related to the Danish implementation of the Data Retention Directive, which can be found in the Logging Order. This implementation predates the actual Directive by some 4 years. The Danish law goes well over and above what is required in the Data Retention Directive. Session logging includes more internet packets than required and more information concerning sources and IP address being collected, with the retention limit for data being one year. While this represents a “public policy” exception, and therefore only one part of the question examined here, it is worth noting that this issues is both difficult and controversial.

A specific exception exists in relation to marketing electronic communication services (Provision Order, Art 24(3)). This is only possible with prior consent.
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

<table>
<thead>
<tr>
<th>a. Danish legislation does not specifically address automated breaches. The issues mentioned in the question are not expressly addressed anywhere in the implementing framework.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. None other than the legislation already mentioned above.</td>
</tr>
</tbody>
</table>
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Article 3 of the Cookie Order entails a detailed transposition of Article 5.3 of the Directive. It provides that “Natural or legal persons may not store information, or gain access to information already stored, in an end-user’s terminal equipment, or let a third party store information or gain access to information, if the end-user has not consented.” The user’s consent shall only be valid upon presentation of comprehensive information. This is the case if:

1) it appears in a clear, precise and easily understood language or similar picture writing,
2) it contains details of the purpose of the storing of, or access to information, in the end-user’s terminal equipment,
3) it contains details that identify any natural or legal person arranging the storing of, or access to, the information,
4) it contains a readily accessible means by which the end-user to will be able to refuse consent or withdraw consent to storing of or access to information, as well as clear, precise and easily understood guidance on how the end-user should make use thereof, and
5) it is immediately available to the end-user by being communicated fully and clearly to the end-user. In addition, when storing of information or access to information takes place through an information and content service, information to end-users must be directly and clearly marked and be accessible at all times for the end-user on the information and content service in question.”

b. The abovementioned provision itself does not distinguish between types of cookies. The Guidelines to the Cookie Order, however, in Section 2 provides a very detailed overview of which technologies are covered. Emphasizing that the rules are technology neutral, the guidelines stipulates that the Order covers similar technologies, including storing and access of information from USB keys, CDs, CD-ROMs, external hard drives, etc. Not only classic html cookies but any type of cookies, including Flash cookies, Web storage in HTML5, JavaScript or Microsoft Silverlight. Cookies of different life spans are all covered. First party cookies and third party cookies are separately mentioned. Session cookies and persistent cookies are both covered.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Consent is defined in Article 2(1) No. 8 of the Cookie Order as “any freely given, specific and informed indication of the end user’s wishes by which the end-user confirms its agreement to information being stored, or access to stored information being gained” in the end-user equipment. This definition implies a real choice but this does not mean that the in any other situation, the service provider should provide website functionality without cookies. In other words, it is legal to employ a “take-it-or-leave-it” scenario, where rejection of cookies leads to inability to use the website.

Consent, as should be clear from the five requirements outlined in the answer to question 5 above, must be presented in clear and easy to understand language. The purpose of the storing must be explained and the details of the person storing must be available. The refusal of consent must be made easy. All of the information must be made available “immediately”, “fully” and “clearly”. The Cookie Guidelines emphasize that the information may be layered but the essential information must be available at once. The Guidelines say that such “essential” information concern “all purposes of cookies and similar technologies” and “who is using cookies and similar technologies”.

An indication of the user’s wishes can be done by either ticking a box, clicking a button or filling a form or by actively using of a service where it must be clear that there is storing of information. The Cookie guidelines emphasize, in the case of the latter, that it is not merely enough that the site stores tells the user that cookies are used but it must be possible that continued action (e.g. clicking) will trigger their use.

The Guidelines explain that some websites place cookies even before consent is obtained (e.g. for statistical purposes of counting the number of hits a site gets). The legal status of these is not clear and the Danish Business Authority is not enforcing the rules in the absence of official clarification from the Commission.

There is nothing specific on mobile devices although the Guidelines offer examples which are specific to these devices (and even include pictures of an iPhone). This means only that the Agency is aware of the specific nature of mobile communications; the rules itself do not vary.

The Guidelines address the problem of third party cookies, which are stored through the main sites (e.g. various adverts on a web page provided by a newspaper). These third party sites embed their content on the main sites. The Guidelines demonstrate how the consent issue can be resolved by using different technical solutions.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

<table>
<thead>
<tr>
<th>Article 4(1) of the Cookie Order allows storing of cookies and similar technologies if the storing is 1) for the sole purpose of carrying out the transmission of the communication over an electronic communications network or 2) storing of or access to information is necessary in order for the service provider of an information society service explicitly requested by the end-user to provide this service. The language here is consistent with the requirement of the ePrivacy Directive. The Cookie Guidelines spell these out as: cookies used when connecting to the Internet (for the first) and cookies ensuring the functionality of a service requested (for the second).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 4(2) says that storing is allowed where such storing is a technical precondition for being able to provide a service:</td>
</tr>
<tr>
<td>“Storing of or access to information in an end-user’s terminal equipment is necessary, cf. subsection (1), no. 2, if such storing of or access to information is a technical precondition for being able to provide a service operating in accordance with the purpose of the service.”</td>
</tr>
<tr>
<td>The Guidelines provide examples of electronic shopping baskets, log-in situations, authentication cookies, etc. as examples of exemptions.</td>
</tr>
</tbody>
</table>
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

<table>
<thead>
<tr>
<th>The Danish Business Authority has confirmed on several occasions that, while general compliance exists, there are wide compliance discrepancies between companies and that no company complies 100%. Based on a sample of 50 companies taken in 2013, the Authority found that 48 out of 50 sites informed the users on cookies. 78% had good navigation practices compared to 36% 8 months earlier. (See <a href="http://www.atomic.dk/nyheder/overholdelse/danske-hjemmesider-overholder-ikke-nye-cookieregler/801692066">http://www.atomic.dk/nyheder/overholdelse/danske-hjemmesider-overholder-ikke-nye-cookieregler/801692066</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In practice, most Danish companies use a simple prompt/pop-up banner, which can be ignored. In other words, it is normally possible to simply continue using the site without actually clicking on it. It is not clear whether cookies are, in such situations, actually placed but the evidence suggests that, in some cases at least, they are. A minority of prompts provide detailed information, with dedicated areas of the site explaining the mechanism in plain language. The majority of companies use very reduced information. Some companies still use the old model where no specific information is provided in advance.</td>
</tr>
</tbody>
</table>
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

| a. Very detailed assistance is provided in the Cookie Order guidelines ([http://erhvervsstyrelsen.dk/file/253400/cookie-exec-order-guidelines-english-version.pdf](http://erhvervsstyrelsen.dk/file/253400/cookie-exec-order-guidelines-english-version.pdf)) These are published by the Danish Business Authority, which has the main enforcement responsibility. The Guidelines address the Order article-by-article, frequently providing practical examples. The Guidelines have a separate Technical Guide, which describes a five-step process for compliance with the cookie rules. For each of the steps (identifying web property, checking if cookies are set, giving information, removing unwanted cookies, obtaining consent), a detailed explanation is provided (including illustrations).

| b. No cases have been rendered yet. |
10. What is your individual view of:
a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

a. It seems that general awareness of the basic requirements of the ePrivacy directive as amended in 2009 exists both in the corporate world and with customers. However, both providers and users are publicly voicing complaints. The former because of the impracticality of the extra burden, the latter because of little or no real gain.

Anecdotal evidence suggests that Danish consumers are comparatively well-informed in matters of Internet safety and electronic commerce. The broadband penetration and speeds as well as other parameters are comparatively high. Consumers rely on public ranking systems (such as Trustpilot) and on- and off line consumer information rather than on cookie alerts. An average consumer may or may not feel that a website is safe, not on the basis of cookie prompts but on the basis of other parameters such as location of the site, its “look and feel” and the nature of the business. The author of this national report, in conversation with ordinary Danes, has yet to find one who claimed that the new rules had benefited them. Most people ignore the prompt, unless it is impossible to proceed with the site. In most situations, this is not the case. On the other hand, the relatively extensive system of consumer protection (which exists since prior to 2002) and keeps being widely used.

In summary, the 2009 reform is seen locally as being somewhat bureaucratic and lacking in real effect. It is worth emphasizing that this is particularly true after Edward Snowden revelations of 2013 and a number of high-profile pirate attacks. While most users and businesses realize that reinforcing security regarding data storage and collection is of importance, the belief is that the present measures only touch the surface.

It is this author’s belief that the new rules (i.e. the 2009 reform) have had little or no material effect in practice and that true changes may be achieved elsewhere.

b. It is likely that the problems do not lie in the legal instruments themselves but in practicalities of Internet operation. One improvement relatively easily achieved is increased coherence at EU level between the three directives (Data Protection – ePrivacy – Data Retention). As already suggested, the Danish legislation is split between several instruments. It is not impossible to bring more coherence into this framework.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Traffic data is defined in the Provision Order as “data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.”

This definition does not appear to be in any way different from the one in the Directive.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

<table>
<thead>
<tr>
<th>Article 23(1) of the Provision Order requires that traffic data be erased or anonymized where data are no longer necessary for transmitting communication. The exceptions are laid down in the Administration of Justice Act.</th>
</tr>
</thead>
<tbody>
<tr>
<td>As per Article 23(2), it is permitted to process and store traffic data for the purposes of subscriber billing and interconnection payments but only up to the end of the period during which the bill may lawfully be challenged or payment pursued.</td>
</tr>
<tr>
<td>As per Article 23(3) processing traffic data regarding subscribers or users for the purpose of marketing electronic communications services or for the provision of value added services, is permitted provided that the user has consented prior to the processing but only to the extent and necessary for such services or marketing. In such cases, users must have the option of withdrawing their consent.</td>
</tr>
<tr>
<td>Article 23(4) further requires that providers inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in subsections (2) and (3). Where data are processed for the purposes mentioned in subsection (3), information shall be given prior to obtaining consent.</td>
</tr>
<tr>
<td>The overview of the above provisions confirms that the requirements for lawful processing have not been clearly spelled out but set in negative terms only – in the form of prohibition of certain actions.</td>
</tr>
<tr>
<td>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</td>
</tr>
<tr>
<td>---</td>
</tr>
</tbody>
</table>

Article 23(1) of the Provision Order requires that traffic data be erased or anonymized “where data are no longer necessary for transmitting communication”. The exceptions are contained in the Administration of Justice Act. The latter, as indicated above, goes wider than the moribund Data Retention Directive.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

| No such cases have been reported by the Danish Business Authority and the author is not aware of any relevant judicial case law. |
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| The rules seem to be straightforward. The requirement for anonymization of traffic data is clear. |
| A problem may be in the lack of evidence on the extent to which traffic data is really anonymized. |
| The problems may lie in the data retention rules and this is on the government side, not on the corporate side. The Danish government has recently confirmed that there is no need to significantly revise the retention laws (see [http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/](http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/)) |
| This is the position that remains controversial in both business and consumer circles. |
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
</table>

Location data are defined in article 2 of the Provision Order as “Data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a public electronic communications service.”

This definition does not seem to be different from the provided in the Directive.
| 2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications? |

Pursuant to Article 24 of the Provision Order, location data can only be processed when it has been made anonymous or “when the subscriber or user has consented to the processing”. In the latter case, only to the extent and duration necessary “for providing a value added service”.

Providers processing location data must inform the subscribers or users, “prior to obtaining their consent, of the type of location data other than traffic data which will be processed.” Furthermore, providers must inform the subscribers of the “purposes and duration of the data processing” and if the data will be transmitted to a third party “for the purpose of providing a value added service”.

Where the user’s consent had been obtained, the user must continue to have the option of by “using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication”.

The processing of data must be “restricted to persons employed by or acting under the authority of the provider of the network or service or of the third party providing the value added service”.

The implementation does not contain discrepancies with the ePrivacy Directive and appears to be straightforward.

It is not clear from the text of the Order whether third parties who harvest data are covered. A strict reading would suggest so, in which cases the anonymization and consent requirements would apply to them in the same manner as they apply to any other provider. The Provision Guidelines do not address this point.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

The general requirement of Article 24(1) allows processing if data are anonymised. This is one of the two requirements, the other being informed consent. No other mention of anonymisation is made.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong></td>
<td>The Guidelines for the Provision Order have been issued on 1 October 2012: “Vejledning til udbudsbekendtgørelsen” Danish version on <a href="http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf">http://erhvervsstyrelsen.dk/file/279079/vejledning-udbud-bkg.pdf</a>, no English translation exists. The Guidelines were published by the Danish Business Authority, the same one that issued Cookie Guidelines. The Guidelines take an article-by-article approach, are over 60 pages long and fairly comprehensive. The text is mostly clear and understandable to non-experts, although fewer examples have been given than in Cookie Guidelines. Two appendices have been provided in the Guidelines. The first concerns the requirements for contract content re Article 9 (Common terms for commercial provisions of electronic communication networks and services to end-users). The second concerns information given to consumers in cases of prepaid electronic services.</td>
</tr>
<tr>
<td><strong>b.</strong></td>
<td>No cases exist on this issue.</td>
</tr>
</tbody>
</table>
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The rules are relatively straightforward and follow the letter and spirit of the ePrivacy Directive. It is difficult to assess the effectiveness of these rules'. The reports of abuses of location data are widespread. A significant number of these relate to harvesting of such data by third parties. Neither the European nor the national legal framework has a clear answer to this challenge. The author of this report feels that, although the rules may be clear and logically consistent, they are not successfully targeting the problem which would require a rehaul of the entire data protection system and would also need technological and societal solutions entirely independent of any legal intervention. In other words, the law is a necessary but not sufficient precondition for eliminating the problem.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.


   Article 6 covers unsolicited communications:

   (1) A trader must not approach anyone by means of electronic mail, an automated calling system or facsimile machine with a view to the sale of products, real property, other property, labour and services unless the party concerned has requested him to do so.

   (2) Notwithstanding subsection (1), a trader that has received a customer’s electronic contact details in connection with the sale of products or services may market his own similar products or services to that customer by electronic mail, provided that the customer has the option, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in the event of subsequent communications.

   (3) A trader must not approach a specific natural person using other means of remote communication with a view to sales as referred to in subsection (1) if the person concerned has declined such communications from the trader, if it may be seen from a list prepared each quarter by the Central Office of Personal Registration (CPR) that the person concerned has declined communications for such marketing purposes, or if the trader, by consulting the CPR, has become aware that the person concerned has declined such communications. Telephone communications are also subject to the regulations governing unsolicited communications in the Act on Certain Consumer Agreements.

   (4) Subsection (3) does not apply if the person in question has previously requested the communication from the trader.

   (5) The first time a trader makes a communication as referred to in subsection (3) with a specific natural person who is not on the CPR list, the trader shall inform him clearly and comprehensibly of his right to decline communications from the trader as referred to in subsection (3). At the same time, the person concerned shall be offered an easy manner of declining such communications.

   (6) No payment may be requested for receiving or noting information to the effect that a request under subsection (1) is being revoked or that communications as referred to in subsection (3) are being declined.

   (7) The Minister for Business and Growth may lay down more detailed regulations governing the trader’s duty to provide information under subsection (5) and duty to offer an opportunity to decline communications as referred to in subsection (3).
This is the opt-in regime, which is expressed in somewhat clearer terms than in Article 13 of the ePrivacy Directive. Overall, the implementation follows the spirit of the Directive. The overall idea is that no unsolicited communication by email, fax or auto-calling machines can be sent unless the user had requested it (paragraph 1). The exception (paragraph 2) is for traders that already have information from previous transactions and would like to use it again. They can do so, provided the users can opt out at any point before the initial transaction or after the subsequent advertising. A trader must not pursue consumers who have already opted out or have put their names on the official opt-out registers with other means of unsolicited communications than in paragraph 1 (paragraph 3), although this is not the case if a person had already previously requested info from the trader (paragraph 4). In cases where the person is not in an opt-out register, it is necessary for a trader to explain the options available to the natural person to decline communications (paragraph 5).

b. The system introduced is the opt-in system with relatively detailed explanations given to the customers and a reduced number of options for the trader. The language used is more detailed and more precise than that in the ePrivacy Directive, although the spirit is followed. The main principle is that consumers must opt in.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

For electronic mail, automated calling systems or facsimile machine, as per Article 6 of the Marketing Practices Act, the requirements are different than the Directive, depending on three situations:

- Marketing is allowed where the user requests it (or has in the past for some other product or service in the same company)
- Marketing is allowed where the user is not on the opt-out list and initiates the transaction and the marketing is not by email, fax or auto-calling systems
- Marketing is forbidden for users on the opt-out list

This is a more precise definition than the one provided in the Directive, but it is fully within what Article 13(3) allows.
<table>
<thead>
<tr>
<th><strong>3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, pursuant to Article 6 of the Marketing Practices Act, a) where the consumer had already contacted the seller in case of a previous transaction and b) where the consumer initiates the transaction.</td>
</tr>
</tbody>
</table>
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The law applies to all methods of unsolicited communication, without discrimination, i.e. it is technology neutral. The specific opt-in regime, however, is only in force for emails, auto-calling machines and faxes. The other methods are under a strict opt-out in the sense that a placing of a name on the Register will always have the result of prohibiting unsolicited communication, in respect of any method.

No other distinction is made in the law.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

| a. Unlike general provision of electronic services and cookies, there are no official guidelines, other than those provided on the internet. These guidelines are provided on the website of the Consumer Ombudsman: [http://www.forbrugerombudsmanden.dk/Sager-og-praksis/Markedsfoeringsloven/Markedsfoeringsloven-i-praksis](http://www.forbrugerombudsmanden.dk/Sager-og-praksis/Markedsfoeringsloven/Markedsfoeringsloven-i-praksis), English version on [http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act](http://www.consumerombudsman.dk/Regulatory-framework/Danish-Marketing-Practices-Act). The Ombudsman also provides other guides on the same page, such as information on how to lodge a complaint: [http://www.consumerombudsman.dk/About-us/complaintprocedure](http://www.consumerombudsman.dk/About-us/complaintprocedure). The information is clear and detailed but is geared towards non-experts. |
| b. No case-law exists in this area. |
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

<table>
<thead>
<tr>
<th>The rules are clear, well-written and effective. The number of complaints to the authorities over unsolicited advertising is low and the awareness of the rules and their effect both in the general population and on providers is high.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of the different areas addressed in the ePrivacy Directive, this is probably the most effective one.</td>
</tr>
</tbody>
</table>
COUNTRY REPORT

Republic of Estonia

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Urmas Kukk, Kraavi & Partners

Date: 18th of August 2014
Contents

Part 1: Management summary ................................................................. 3
Part 2: Answers to the Questionnaire .......................................................... 5
Part 1: Management summary

- The provisions with regard to the scope of the ePrivacy Directive have been transposed partly into the Electronic Communications Act (01.01.2005, transposition of ePrivacy Directive requirements (partly) came in to force 25.05.2011) and into the Information Society Service Act (01.05.2004) year. At the same time it is wrong to say that the ePrivacy Directive has not been fully transposed into the Estonian legislation. According to the structure of the Estonian legislation, the question has to be solved by a general rule if there is no special rule. In this case, if the Electronic Communications Act or the Information Society Service Act do not prescribe how personal data must be processed, then the data processor has to follow the provisions of the Personal Data Protection Act.

- Articles 3, 5(1), 6, 9, and 13 have been more or less literally transposed into Estonian law and has been satisfactorily included in the Electronic Communications Act and into the Information Society Service Act.

- Article 5(3) of the ePrivacy Directive (about “cookies” etc.) has not been transposed into Estonian law expressis verbis. However the gaining of access to information stored in the terminal equipment of a subscriber might lead to information which allows the subscriber to be identified directly or indirectly. In this case the person who gains access to the information is obliged to follow the personal data processing rules which are defined in the Personal Data Protection Act (08.07.1996) year.

- Regardless how the ePrivacy Directive requirements have been transposed into Estonian legislation (see previous point), the application of Article 5(3) of the ePrivacy Directive, is not followed in practice. Webpage visitors are not notified about the usage of cookies and are not asked for permission to store information on their terminal equipment.

- As of June 2014 Ministry of Economic Affairs and Communications has begun the procedure to amend the Information Society Service Act. This amendment will transpose into the Estonian law Article 5(3) of the ePrivacy Directive.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into Estonian law and Estonian Data Protection Inspectorate supervises the requirements of the law.

**Personal remark**

Putting the text of the Article 5(3) of the ePrivacy Directive into simple form it is obvious that this provision is refers to a form of spying without the consent of the terminal equipment owner. At the same time it is not clear if the person who gains access to information receives personal information or not. If yes, there is a violation of the privacy of the subscriber, if not, there is no violation of the privacy. Therefore the wording of the article 5(3) is not clear and confusing. The
Article 5(3) could be amended as follows: “/---/ the storing of information or the gaining of access to information already stored, in the terminal equipment of a subscriber or user, regardless if this information allows identification of the physical person or not, is only allowed... /---/”
Part 2: Answers to the Questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC has been (partly) transposed into Estonian legislation by the Electronic Communication Act from 1st of January 2005
- The general rule for the personal data protection is the Personal Data Protection Act from 8th of July 1996

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 3 (Scope)</td>
<td>Electronic Communication Act §1 (1)</td>
<td><a href="https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv">https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv</a></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Electronic Communication Act §102 (4)</td>
<td><a href="https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv">https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv</a></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Not (yet) transposed</td>
<td></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Electronic Communication Act §§105 and 106</td>
<td><a href="https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv">https://www.riigiteataja.ee/akt/129062014019?leiaKehtiv</a></td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- the full name in your national language
- the English translation of the short name
- the part or the provision(s) of the ePrivacy Directive it supervises
- URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
</table>

Explanation:
- The Estonian Technical Survailance Authority is the state supervisory authority for the provisions transposing the ePrivacy Directive which have been inserted into the Electronic Communications Act (except §103¹ Use of electronic contact details for direct marketing)

- The Estonian Data Protection Inspectorate is the state supervisory authority for personal data processing and protection and the provisions transposing the ePrivacy Directive art. 13 which have been inserted into the Electronic Communications Act §103¹ Use of electronic contact details for direct marketing
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

**networks** §2 8) of the Electronic Communication Act defines **electronic communications network** as a transmission system including switching equipment and other support systems for the transmission or conveyance of signals by way of a cable or by radio, optical or other electromagnetic means. Electronic communications networks include also the satellite network, telephone network, data communication network, mobile telephone network, broadcasting network, cable network and electric cable system, if used for the transmission or conveyance of signals, regardless of the nature of information transmitted over such networks.

This is not different from the ePrivacy Directive.

**services** §2 6) of the Electronic Communication Act defines **electronic communications service** as a service which consists wholly or mainly in transmission or conveyance of signals over the electronic communications network under the agreed conditions. Network services are also electronic communications services.

The difference from the ePrivacy Directive lies in the provision that a network service, where the service provider only enables the equipment for the transmission or conveyance of signals, is also counted as electronic communications service.

**Providers** §2 5) of the Electronic Communication Act defines **electronic communications undertaking** as a person who provides publicly available electronic communications services to the end-user or to another provider of publicly available electronic communications services.

The definition is not so detailed in the ePrivacy Directive but covers all the activities (establishment, operation, control or making available) described therein.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

<table>
<thead>
<tr>
<th>Services such as VoIP, webmail etc. fall within the scope of the Information Society Services Act.:</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 1. Purpose of the Act</td>
</tr>
<tr>
<td>(1) This Act provides the requirements for information society service providers, the organisation of supervision and the liability for the violation of this Act.</td>
</tr>
<tr>
<td>§ 2. Definitions</td>
</tr>
<tr>
<td>1) “Information society services” are services provided in the form of economic or professional activities at the direct request of a recipient of the services, without the parties being simultaneously present at the same location, and such services involve the processing, storage or transmission of information by electronic means intended for the digital processing and storage of data. Information society services must be entirely transmitted, conveyed and received by electronic means of communication. Services provided by means of fax or telephone call and television or radio services are not information society services.</td>
</tr>
</tbody>
</table>
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The legislation can affect operators outside of Estonia as follows:

1. Electronic Communications Act: §111(5) The data specified in subsections (2) and (3) of this section shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia:
   1) the requests and information provided for in § 112 of this Act;
   2) the log files specified in subsection 113 (5) and the applications provided for in subsection 113 (6) of this Act;
   3) the single requests provided for in § 114 of this Act.

Subsection (2) states the data which must be preserved by the telephone or mobile telephone service providers and subsection (3) states the data which must be preserved by the Internet service providers.

2. Information Society Services Act: §3 (1) Information society services provided through a place of business located in Estonia shall meet the requirements arising from Estonian law regardless of the Member State of the European Union or Member State of the European Economic Area in which the service is provided.

(2) The provision, in Estonia, of services belonging to the co-ordinated field through a place of business located in a Member State of the European Union or Member State of the European Economic Area are not subject to restriction, except in the case and to the extent justified for the protection of morality, public order, national security, public health and consumer rights.

3. Personal Data Protection Act: §7 (6) A processor of personal data operating outside of the European Union who uses equipment located in Estonia for processing personal data is required to appoint a representative located in Estonia.
There are no cases where Estonian national law has been applied to a foreign entity but under these provisions, it would do so where their business was provided in Estonia.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. There is no guidance issued by the Estonian Data Protection Inspectorate nor the Estonian Technical Surveillance Authority on the definitions described in subsection 3.

   b. There are no court cases in Estonia with regard to the interpretation of the definitions described in subsection 3.

   In the question of the Internet service providers liability on publication of insulting comments, the Estonian Supreme Court in case no 3-2-1-43-09 stated that the service provider together with the person who actually wrote the insulting comment is defined as the ‘publisher’ and was therefore responsible for damage caused by the publication.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. In Estonia the Personal Data Protection Act deals with privacy, personal data processing and personal data protection regardless of the environment (electronic or physical). Therefore there is no need to make exceptions for data processors in one area of business so that an electronic service provider has more obligations than a data processor in other areas. (By the Electronic Communication Act §1021 (2) In the event of personal data breach (regardless of whether the breach is electronic or physical)*, a communications undertaking is required to notify the Data Protection Inspectorate thereof at the earliest opportunity. Other data processors do not have such obligation.)

b. As the electronic environment does not create a new law, it is reasonable to merge the both the Data Protection Directive and the ePrivacy Directive.

*Expert’s remark
B. Confidentiality obligations

<table>
<thead>
<tr>
<th>1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Communication Act §102 (1) A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, it must maintain the confidentiality of: 1) information concerning specific details related to the use of communications services; 2) the content and format of messages transmitted over the communications network; 3) information concerning the time and manner of transmission of messages.</td>
</tr>
<tr>
<td>There is no definition of “communications” under Estonian legislation.</td>
</tr>
<tr>
<td>2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations</td>
</tr>
<tr>
<td>This is transposed in Estonian law with the same effect.</td>
</tr>
<tr>
<td>According to the Electronic Communication Act §102 (4) the undertaking has a right to collect and process, without the consent of a subscriber, information whose processing is necessary for the purposes of recording the transactions made in the course of business and for other business-related exchange of information. In addition, a communications undertaking has a right to store or process information without the consent of a subscriber if the sole purpose thereof is the provision of services over the communications network, or if it is necessary for the provision, upon a direct request of the subscriber, of information society services within the meaning of the Information Society Services Act.</td>
</tr>
</tbody>
</table>
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

According to the Electronic Communication Act §111¹ certain data is required to be preserved:

(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:
   1) the number of the caller and the subscriber’s name and address;
   2) the number of the recipient and the subscriber’s name and address;
   3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialed and the subscriber’s name and address;
   4) the date and time of the beginning and end of the call;
   5) the telephone or mobile telephone service used;
   6) the international mobile subscriber identity (IMSI) of the caller and the recipient;
   7) the international mobile equipment identity (IMEI) of the caller and the recipient;
   8) the cell ID at the time of setting up the call;
   9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;
   10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

(3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data:
   1) the user IDs allocated by the communications undertaking;
   2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;
   3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
   4) the user ID or telephone number of the intended recipient of an Internet telephony call;
   5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;
   6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID;
   7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;
   8) the Internet service used in the case of electronic mail and Internet telephony services;
   9) the number of the caller in the case of dial-up Internet access;
   10) the digital subscriber line (DSL) or other end point of the originator of the communication.

Under (11) of same paragraph this information is allowed to be forwarded to:
   1) an investigative body, a surveillance agency, the Prosecutor’s Office or a court pursuant to the Code of Criminal Procedure;
   2) a security authority;
   3) the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure;

¹ See Electronic Communication Act §111.
4) the Financial Supervision Authority pursuant to the Securities Market Act;
5) a court pursuant to the Code of Civil Procedure;
6) a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act.
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

<table>
<thead>
<tr>
<th>a. The Estonian legislation does not distinguish between breaches of confidentiality with or without human involvement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. There is no separate legislation with regard to the protection of private electronic communications.</td>
</tr>
</tbody>
</table>
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

| a. | There is no regulation in the Estonian law on cookies and spyware. However, as of June 2014 the Ministry of Economic Affairs and Communications has begun the procedure to amend the Information Society Service Act. This amendment will transpose Article 5(3) of the ePrivacy Directive into the Estonian law. The proposed amendment states:
   §11¹ (1) The service provider can store the information or provide access to the information already stored in the terminal equipment of the service user only with the consent of the service user.
   §12 (3) The Data Protection Inspectorate supervises the compliance with the requirement in §11¹ of this Act. |
| b. | There is no distinction in the Estonian law between types of cookies and between the type of device. The proposed amendments will not make distinctions. |
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

The informed consent is implemented into Personal Data Protection Act:

§ 12. Consent of data subject for processing of personal data

(1) The declaration of intention of a data subject whereby the person permits the processing of his or her personal data (hereinafter consent) is valid only if it is based on the free will of the data subject. The consent shall clearly determine the data for the processing of which permission is given, the purpose of the processing of the data and the persons to whom communication of the data is permitted, the conditions for communicating the data to third persons and the rights of the data subject concerning further processing of his or her personal data. Silence or inactivity shall not be deemed to be a consent. Consent may be partial and conditional.

(2) Consent shall be given in a format which can be reproduced in writing unless adherence to such formality is not possible due to a specific manner of data processing. If the consent is given together with another declaration of intention, the consent of the person must be clearly distinguishable.

Informed consent is required only if where the information identifies, or allows identification of, the user in question. There is no special requirement in the law to use pop-up screens or consent bars.

As mentioned previously there is no distinction in the Estonian law between types of cookies and between the type of device.
7. How are the exceptions to the informed consent rule implemented in national law?
Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The exceptions to the informed consent are imposed by the §14 of the Personal Data Protection Act:
(1) Processing of personal data is permitted without the consent of a data subject if the personal data are to be processed:
1) on the basis of law;
2) for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;
3) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;
4) for performance of a contract entered into with the data subject or for ensuring the performance of such contract unless the data to be processed are sensitive personal data.

(2) Communication of personal data or granting access to personal data to third persons for the purposes of processing is permitted without the consent of the data subject:
1) if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;
2) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;
3) if the third person requests information obtained or created in the process of performance of public duties provided by an Act or legislation issued on the basis thereof and the data requested do not contain any sensitive personal data and access to it has not been restricted for any other reasons.

(3) Surveillance equipment transmitting or recording personal data may be used for the protection of persons or property only if this does not excessively damage the legitimate interests of the data subject and the collected data are used exclusively for the purpose for it is collected. In such case, the consent of the data subject is substituted by sufficiently clear communication of the fact of the use of the surveillance equipment and of the name and contact details of the processor of the data. This requirement does not extend to the use of surveillance equipment by state agencies on the bases and pursuant to the procedure provided by law.

As mentioned previously there is no distinction in the Estonian law between types of cookies and the Personal Data Protection Act is applicable only if where the information identifies, or allows identification of, the user in question.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The cookie provisions have not been transposed into Estonian law and as such there is no compliance and enforcement of cookie rules by the Data Protection Inspectorate or Technical Surveillance Authority.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There is no guidance on cookies.</td>
</tr>
<tr>
<td>b.</td>
<td>There are no court cases on cookies.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The protection of privacy against cookies lies solely with the end users. The state institutions do not inform their webpage users about the cookies they use. The state portal eesti.ee does not give the option to accept or reject cookies.

   b. For improvements it is essential that Estonia adopts the provisions of Directives 2002/58 and 2009/136 expressis verbis into domestic law and provides the necessary resources to the Technical Surveillance Authority and the Data Protection Inspectorate for effective supervision of these rules.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no clear definition of “traffic data” in Estonian law.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

The legal requirements for the lawful processing of traffic data are provided in the Electronic Communications Act:

§104 A communications undertaking may process the information provided for in subsection 102 (1) of this Act without the subscriber's consent if is necessary for billing the subscriber, including for the determination and calculation of interconnection charges.

§102 (1) (1) A communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber; above all, it must maintain the confidentiality of:

1) information concerning specific details related to the use of communications services;
2) the content and format of messages transmitted over the communications network;
3) information concerning the time and manner of transmission of messages.

(2) The information specified in subsection (1) of this section may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons, except in the cases specified in §§ 112, 113 and 114 of this Act. A subscriber has the right to withdraw his or her consent at any time.

As mentioned above there is no clear definition of “traffic data” in Estonian law.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

The legal requirements to anonymise or delete traffic data are provided in the Electronic Communication Act:

§106 (2) Communications undertakings and persons duly authorised thereby are required to delete or render anonymous the data provided for in subsection 102 (1) of this Act and in §§ 103 and 105 of this Act within one calendar month after the need to store such data ceases to exist or the purpose of processing such data has been achieved. The data provided for in § 104 of this Act must be deleted or rendered anonymous immediately when one year has passed from payment for the communications services prescribed in the communications services contract or payment of the arrears by the subscriber.

(3) The data specified in subsections 111¹ (2) and (3) of this Act and requests submitted and information given pursuant to § 112 must be deleted immediately after the expiry of the term specified in subsection 111¹ (4).
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

| There are no cases involving traffic data rules. |
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Personal Data Protection Act is for the data processors in every sector therefore everyone (in case of violation of privacy) can rely on provisions of this act. The Electronic Communications Act and Information Society Service Act provide additional, more detailed obligations to the service providers.
## D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no clear definition of “location data” in Estonian law.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

The legal requirements for lawful processing are provided in the Electronic Communication Act: § 105. Processing of location data of subscribers

1. A communications undertaking has the right to process subscribers’ location data, the processing of which is not provided for in § 104 (See section C2) or § 111 (See section B3) of this Act, only if such data are rendered anonymous prior to processing.

2. A communications undertaking may also process, with the consent of the subscriber, the data provided for in subsection (1) of this section to provide other services in the process of using the communications services to an extent and during the term necessary for processing and without rendering the data anonymous.

3. Before obtaining the consent of a subscriber, a communications undertaking is required to inform the subscriber of the data it wishes to use for the provision of the service, the purpose and term of using such data and whether such data are forwarded to third persons for the purposes of providing the service. A subscriber has the right to withdraw his or her consent at any time.

4. A subscriber who has granted consent for the processing of the data provided for in subsection (1) of this section must have an opportunity to temporarily refuse, free of charge and in an easy manner, the processing of the data in the part of establishment of a connection or transmission of information as indicated by the subscriber.

5. A communications undertaking may process the data provided for in subsection (1) of this subsection without the subscriber’s consent for the purposes of informing the subscriber promptly of an event which endangers the subscriber’s life or health and providing instructions about safe conduct, whereas such information is forwarded to the communications undertaking by the Police and Border Guard Board or a rescue service agency.

There are no differences provided in the Directive, except subsection (5) which is not included in the Directive.

§111¹ (1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts:

6) determining of the location of the terminal equipment.

This provision does not apply to third parties.
<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location data must be anonymised.</td>
</tr>
<tr>
<td>The legal requirements for lawful processing are provided in the Electronic Communication Act: §105 (1) A communications undertaking has the right to process subscribers' location data, the processing of which is not provided for in § 104 or § 111 of this Act, only if such data is rendered anonymous prior to processing.</td>
</tr>
</tbody>
</table>
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There are no guidelines or cases on the interpretation on “location data rules” by the Data Protection Inspectorate. The Data Protection Inspectorate issued guidelines for personal data processing in employment relations. Furthermore in chapter 3.5. surveillance is briefly touched on in terms of using GPS equipment as a surveillance tool, for example, when keeping a logbook of the use of a personal car for professional journeys.</td>
</tr>
<tr>
<td>b.</td>
<td>There are no court cases where location data rules have been applied.</td>
</tr>
</tbody>
</table>
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| The rules are clear, logically consistent and appropriate but it is difficult to evaluate the effectiveness of the rules due to the lack of supervision. |
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. The legal requirements for lawful processing are provided in the Electronic Communication Act: §103\(^1\) (1) The use of electronic contact details of a subscriber or user of communications services, who is a natural person, for direct marketing is allowed only with the person’s prior consent. The consent must comply with the conditions provided for in § 12 of the Personal Data Protection Act (below).

   Personal Data Protection Act §12: Consent of data subject for processing of personal data
   (1) The declaration of intention of a data subject whereby the person permits the processing of his or her personal data (hereinafter consent) is valid only if it is based on the free will of the data subject. The consent shall clearly determine the data for the processing of which permission is given, the purpose of the processing of the data and the persons to whom communication of the data is permitted, the conditions for communicating the data to third persons and the rights of the data subject concerning further processing of his or her personal data. Silence or inactivity shall not be deemed to be a consent. Consent may be partial and conditional.
   (2) Consent shall be given in a format which can be reproduced in writing unless adherence to such formality is not possible due to a specific manner of data processing. If the consent is given together with another declaration of intention, the consent of the person must be clearly distinguishable.
   (3) Before obtaining a data subject’s consent for the processing of personal data, the processor of personal data shall notify the data subject of the name of the processor of the personal data or his or her representative, and of the address and other contact details of the processor of the personal data. If the personal data are to be processed by the chief processor and authorised processor then the name of the chief processor and authorised processor or the representatives thereof and the address and other contact details of the chief processor and authorised processor shall be communicated or made available.
   (4) For processing sensitive personal data, the person must be explained that the data to be processed is sensitive personal data and the data subject’s consent shall be obtained in a format which can be reproduced in writing.
   (5) A data subject has the right to prohibit, at all times, the processing of data concerning him or her for the purposes of research of consumer habits or direct marketing, and communication of data to third persons who intend to use such data for the research of consumer habits or direct marketing.
   (6) The consent of a data subject shall remain valid during the lifetime of the data subject and for thirty years after the death of the data subject unless the data subject has decided otherwise.
   (7) Consent may be withdrawn by the data subject at any time. Withdrawal of consent has no retroactive effect. The provisions of the General Principles of the Civil Code Act concerning declaration of intention shall additionally apply to consent.
   (8) In the case of a dispute it shall be presumed that the data subject has not granted consent for the processing of his or her personal data. The burden of proof of the consent of a data subject lies...
on the processor of personal data.

b. §103¹ of the Electronic Communication Act is more detailed than Article 13 of the ePrivacy Directive and despite using the term “direct marketing” instead of “unsolicited communication”, the regulation provided in §103¹ is in line with Article 13 of the ePrivacy Directive. However, §103¹ narrows the area of restrictions because the restrictions are limited only to the use of electronic contact details. This is probably caused by the fact that there has never been a wide use of automatic calling machines or faxes for the purpose of direct marketing in Estonia.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The legal requirements for the lawful processing are provided in the Electronic Communication Act: §103(2) The use of electronic contact details of a subscriber or user of communications services, who is a legal person, for direct marketing is allowed if:

1) upon use of contact details, a clear and distinct opportunity is given to refuse such use of contact details free of charge and in an easy manner;
2) the person is allowed to exercise its right to refuse over an electronic communications network.
(3) If a person obtains the electronic contact details of a buyer, who is a natural or legal person, in connection with selling a product or providing a service, such contact details may still be used, regardless of the provisions of subsection (1) of this section, for direct marketing of its similar products to the buyer if:

1) the buyer is given, upon the initial collection of electronic contact details, a clear and distinct opportunity to refuse such use of its contact details free of charge and in an easy manner;
2) the buyer is given, each time when its electronic contact details are used for direct marketing, a clear and distinct opportunity to refuse such use of its contact details free of charge and in an easy manner;
3) the buyer is allowed to exercise its right to refuse over an electronic communications network.
(4) It is prohibited to use electronic contact details for direct marketing if:
1) the person on whose behalf the information is communicated cannot be identified;
2) the communicated information does not include any such instruction or information allowing the user of communications services, subscriber or buyer to exercise its right to refuse.
3) the communicated information does not comply with the requirements provided for in subsection 5 (2) of the Information Society Services Act;
4) the communicated information encourages people to visit websites where information is provided which does not comply with the requirements referred to in clause 3) of this subsection;
5) the user of communications services, subscriber or buyer has refused the use of electronic contact details of the person for direct marketing.
(5) The burden of proof of the consent specified in subsection (1) of this section rests with the person on whose behalf direct marketing is conducted.
(6) The provisions of this section do not apply to multi-party voice calls in real time.

There are no differences in the ePrivacy Directive except for subsections (5) and (6). The ePrivacy Directive does not specify whose obligation it is to prove the presence of consent and it does not exclude real time multi-party voice calls.

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

There are no exceptions to the opt-in consent for the physical person.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Estonian legislation does not distinguish different between communication channels.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

It is explained in the guideline that direct marketing does not only consist of providing information on goods and services. Direct marketing also includes offers made to spread ideas (political ads, etc.) and information given by charity organisations to promote their activities. There are also suggestions in the guideline on how to receive correct consent from the consumer and how to differentiate between the e-mail address of a legal person and a natural person. The consumer is given suggestions on how to avoid search engines that gather e-mail addresses. Finally, the liability for breaking the rules of direct marketing is explained.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b. There are no court cases on unsolicited communications or direct marketing.</td>
<td></td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

<table>
<thead>
<tr>
<th>The rules of unsolicited direct marketing are complex and effective if the physical person is careful and does not tick every box when making a contract with an information society service provider or seller.</th>
</tr>
</thead>
<tbody>
<tr>
<td>However, some of the entities use phone calls for direct marketing and in this case the phone numbers list they use may be generated by software, rather than using the customer list of a service provider, where the phone number differs from the previous one by only one digit.</td>
</tr>
</tbody>
</table>
COUNTRY REPORT

Greece

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Dr. Eleni Kosta, time.lex CVBA

Date: 14.09.2014
Contents

Part 1: Management summary ........................................................................................................................................3
Part 2: Answers to the questionnaire ..................................................................................................................................5
Part 1: Management summary

Management Summary

Important issues relating to the transposition of the ePrivacy Directive into Greek law can be the following:

- The competences between ADAE and HDPA are not very distinct. The HDPA has clearly expressed the opinion that the competence of ADAE not only on the secrecy of communications (which covers the content of a communication), but also on the confidentiality of communications, is overreaching the material scope of the competences that should be assigned to ADAE. However, in practice the two authorities are collaborating with each other when relevant cases appear.

- According to the European definition a “electronic communications service” consist wholly or mainly of the transmission of signals to electronic communications networks. However the Greek legislator requires that such a service consists wholly or partially of the transmission of signals to electronic communications networks, broadening the scope of electronic communications services.

- The current implementation of the ePrivacy Directive leaves a lot of open issues in relation to transnational cases; for instance situations where the provider is established outside Greece, although they are incurring a breach of confidentiality of communications to a Greek citizen. This issue should be looked into, especially in view of the adoption of the General Data Protection Regulation.

- Greece has done an almost literal implementation of Art. 5(3) of the ePrivacy Directive. According to the HDPA, the consent of the user or the subscriber can be provided via the website of the website provider via adequate measures, e.g. pop-up windows. The acceptance of cookies can be realised at once for all cookies installed by the same information society service provider. Alternatively, consent can also be provided via special settings of the web browser or other application. However, the guidelines included in the Greek law and published by the HDPA do not seem sufficient to ensure a harmonised and seamless implementation in practice.

- The choice of the Greek legislator to consider “passwords” as traffic data explicitly in the definition of traffic data is questionable.

- With regard to unsolicited communications, although the ePrivacy Directive refers to both subscribers and users, the Greek law refers only to subscribers. Moreover, when it comes to subscribers, although the Directive applies only to natural persons (see Art. 13(5) ePrivacy Directive), the Greek provisions on unsolicited communications apply also to subscribers that are legal persons, as explicitly mentioned in Art. 11(7) of Law 3471/2006, as amended.

- The introduction of an opt-out regime for the realisation of unsolicited communications with human intervention (calls), requires that the subscriber states to the provider of the publicly available electronic communications service that they do not wish to accept such communications in general; the provider must enter these statements in a special subscriber directory, which shall be at the subscriber’s disposal, free of charge. A problem that has arisen in practice is that these no unified directory, which makes consultation of the directories and consequently the application of the provision in practice very difficult. This is an issue that the HDPA is currently looking into.

- Art 11(5) of Law 3471/2006 introduced an obligation for providers of electronic communications services to take suitable measures for the prevention of unsolicited communications. Although this provision is in accordance with Article 13(3) of the ePrivacy Directive, the Greek legislator introduced the additional requirement that the suitable measures will be “defined by a common act of the DPA and ADAE”. This provision created problems in practice as the common act has not been issued yet and the providers –via a literal translation of the provision- are not required to take the necessary and adequate measures for the prevention of unsolicited communications, before the issuing of the act.
Management Summary

- While the HDPA has suggested best practices for the provision of consent via SMS in its Guidance 2/2011, in practice the major problem is that it is difficult to include the information necessary for the efficient application of an opt-out procedure.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC has been transposed into the Greek legislation via Law 3471/2006, Protection of personal data and privacy in the electronic communications sector and amendment of law 2472/1997, GG A’ 113/28.06.2006, unofficial translation in Greek by the DPA at [http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_203471_06EN.PDF](http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_203471_06EN.PDF). [ΝΟΜΟΣ 3471/2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997, ΦΕΚ 133/Α’/28.6.2006. The official law as published in the Government Gazette can be found here: [http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEbA_BZxkczbHdtvSoC1rl85CIBV551lg7tII9LGd kf53Ulxxx942CdyqzSQYNuqAGCF0lf9Hl6hq6ZkZV96Fi8-MH3D3yFzoT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM](http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEbA_BZxkczbHdtvSoC1rl85CIBV551lg7tII9LGd kf53Ulxxx942CdyqzSQYNuqAGCF0lf9Hl6hq6ZkZV96Fi8-MH3D3yFzoT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM), while an unofficial consolidated version is available in Greek at [http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHEISA%20PROSOPIKA%20DEDOMENA%20%CE%9D3471%20_06.PDF](http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHEISA%20PROSOPIKA%20DEDOMENA%20%CE%9D3471%20_06.PDF).

- Following the 2009 amendments of the European Regulatory Framework for Electronic Communications, the Greek legislator amended its legal framework by Law 4070/2012: Law 4070/2012, Regulations on electronic communications, transport and public works, GG A’ 28/10.04.2012 [Νόμος 4070/2012 Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις, ΦΕΚ Α’ 82/10.04.2012, available only in Greek at [http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEbA_BZxkczbHdtvSoC1rl85CIBV551lg7tII9LGd kf53Ulxxx942CdyqzSQYNuqAGCF0lf9Hl6qSytmEKhLwnFsngj5A5WiLuVnRwO1oKqSe4BIOTspEWYhszf8P8UqWb_zFijLdLEuyXy6QwDnl7MK0f5CBFUuv1_Z2IMKfvm4ZFaV1ZC](http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEbA_BZxkczbHdtvSoC1rl85CIBV551lg7tII9LGd kf53Ulxxx942CdyqzSQYNuqAGCF0lf9Hl6qSytmEKhLwnFsngj5A5WiLuVnRwO1oKqSe4BIOTspEWYhszf8P8UqWb_zFijLdLEuyXy6QwDnl7MK0f5CBFUuv1_Z2IMKfvm4ZFaV1ZC)].

- Law 3917/2011, which implemented the Data Retention Directive, amended a few provisions of Law 3471/2006: Law 3917/2011 Retention of data that are generated or processed in connection with the provision of publicly available electronic communications services or public communications networks, use of surveillance systems via obtaining or recording sound or image at public areas and relative provisions, GG A’ 22/21.02.2011 [Νόμος 3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων]
επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε
dημόσιους χώρους και συναφείς διατάξεις, ΦΕΚ Α’ 22/21.02.2011, available online in Greek at
http://www.et.gr/idocs-
nph/search/pdfViewerForm.html?args=5C7QrtC22wFYAfDx4L2Gd3tvSoCrl8fYWINrQqHftl9LG
dkF53Ulxsx942CdyqxSQYNuqAGCF0fF9Hl6hq6ZkZV96Fls4vX0wZ4DJE72C9POpV8pFNovXD8GPZtu
uZocvHjkZM].

- Art. 10 of Law 2225/1994, as amended, foresees with regard to unsolicited communication that
for such communication the provisions of Art 11 of Law 3471/2006 apply (for which reason no
reference to Law 2225/1994 will be made in this report).

Concordance table
<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
| Art. 2 (Definitions) | Art. 2, Law 3471/2006 | http://www.et.gr/idocs-
nph/search/pdfViewerForm.html?args=
5C7QrtC22wEbA_BZxkczbHdtvSoCrl85
CIBV551l7tlIl9LGdkF53Ulxsx942CdyqxS
QYNuqAGCF0fF9Hl6hq6ZkZV96Fl8 -
MH3D3yF2oT0FlhRXx0L5ofQf5zUm_6w
6Vgvm9aXM |
| Art. 3 (Scope) | Art. 3, Law 3471/2006 | http://www.et.gr/idocs-
nph/search/pdfViewerForm.html?args=
5C7QrtC22wEbA_BZxkczbHdtvSoCrl85
CIBV551l7tlIl9LGdkF53Ulxsx942CdyqxS
QYNuqAGCF0fF9Hl6hq6ZkZV96Fl8 -
MH3D3yF2oT0FlhRXx0L5ofQf5zUm_6w
6Vgvm9aXM |
| Art. 169, Law 4070/2012, which amended Art. 3 Law 3471/2006 | | http://www.et.gr/idocs-
nph/search/pdfViewerForm.html?args=
5C7QrtC22wEbA_BZxkczbHdtvSoCrl85
CIBV551l7tlIl9LGdkF53Ulxsx942CdyqxS
QYNuqAGCF0fF9Hl6hq6YtMQEKEHLwnF
qmgISA5WlsuV-
Rw01oQqSe4B1QTSpEWYhszF8P8UqW_b_zFijLdEuyYx6QwDni7MK0fSCBFUv_1_Z
2lMKFvmm42FaV1ZC |
| Art. 5.1 (Confidentiality) | Art. 4(1), 4(2) and 4(4), Law 3471/2006 | http://www.et.gr/idocs-
nph/search/pdfViewerForm.html?args=
5C7QrtC22wEbA_BZxkczbHdtvSoCrl85
CIBV551l7tlIl9LGdkF53Ulxsx942CdyqxS
QYNuqAGCF0fF9Hl6hq6ZkZV96Fl8 -
MH3D3yF2oT0FlhRXx0L5ofQf5zUm_6w |

- Art. 10 of Law 2225/1994, as amended, foresees with regard to unsolicited communication that
for such communication the provisions of Art 11 of Law 3471/2006 apply (for which reason no
reference to Law 2225/1994 will be made in this report).
| Art. 5.2 (Business exception) | Art. 4(3), Law 3471/2006 | http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrL85CIBV551Jg7tl9LGdkF53UXsx942CdyqX5QYNuqAGCF0fB9Hl6q6ZkZV96F18-MH3D3vF2oT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM |
| Art. 5.3 (Cookies) | Art. 170, Law 4070/2012, which amended Art. 4(5) of Law 3471/2006 | http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrL85CIBV551Jg7tl9LGdkF53UXsx942CdyqX5QYNuqAGCF0fB9Hl6q6ZkZV96F18-MH3D3vF2oT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM |
| Art. 6 (Traffic data) | Art. 171(2), Law 4070/2012, which amended Art. 6(1), 6(2), 6(3) and 6(6), Law 3471/2006 | http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrL85CIBV551Jg7tl9LGdkF53UXsx942CdyqX5QYNuqAGCF0fB9Hl6q6ZkZV96F18-MH3D3vF2oT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM |
| Art. 171(1), Law 4070/2012, which amended Art 5, Law 3471/2006 (which contains general provisions for the processing of personal data, including traffic and location data) | http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrL85CIBV551Jg7tl9LGdkF53UXsx942CdyqX5QYNuqAGCF0fB9Hl6q6ZkZV96F18-MH3D3vF2oT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM |
| Art. 9 (Other location data) | Art. 171(2), Law 4070/2012, which amended Art. 6(4), Law 3471/2006 | http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrL85CIBV551Jg7tl9LGdkF53UXsx942CdyqX5QYNuqAGCF0fB9Hl6q6ZkZV96F18-MH3D3vF2oT0FihRXx0L5ofQf5zUm_6w6Vgvm9aXM |
Art. 171(1), Law 4070/2012, which amended Art 5, Law 3471/2006 (which contains general provisions for the processing of personal data, including traffic and location data)

http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrl85CIBV551lg7tIl9LdkF53Ulxxs942CdyqX5QYNuqAGCF0lfB9Hl6q5YtMqEhLwBFmgJSA5WIsluV-nRwO1oKqSe4BIOTSpEWYhszF8P8UqWb_zFijLdLEujYx6QwDnl7MK0fSCBFUv1_Z2IMKfvm4ZFaV1ZC

Art. 13 (Unsolicited communications) Art. 11, Law 3471/2006

http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wWYAFdDx4L2G3dtvSoClrL8fYWlnRQQhFl9LdKf53Ulxxs942CdyqX5QYNuqAGCF0lfB9Hl6q6ZkZV96F18_MH3D3yF2oT0fhRx0L5ofQf5zU6m_6Vgy9aXM

Art. 16, Law 3917/2011, which amended Art. 11(1) and 11(2), Law 3471/2006

http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wFYAfDx4L2G3dtvSoClrL8fYWlnRQQhFl9LdKf53Ulxxs942CdyqX5QYNuqAGCF0lfB9Hl6q6ZkZV96FIs4vX0wZ4DJE7ZC9PQpV8pFNovXD8GPZtuvZocvHjkZM.

Art. 172, Law 4070/2012, which amended Art. 11(3)-11(8) of Law 3471/2006

http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wEba_BZxkczbHdtvSoClrl85CIBV551lg7tIl9LdkF53Ulxxs942CdyqX5QYNuqAGCF0lfB9Hl6q5YtMqEhLwBFmgJSA5WIsluV-nRwO1oKqSe4BIOTSpEWYhszF8P8UqWb_zFijLdLEujYx6QwDnl7MK0fSCBFUv1_Z2IMKfvm4ZFaV1ZC
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
   a. the full name in your national language
   b. the English translation of the short name
   c. the part or the provision(s) of the ePrivacy Directive it supervises
   d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it is supervising</th>
<th>the URL linking to its website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hellenic Data Protection Authority</td>
<td>HDPA</td>
<td>All provisions transposed in Law 3471/2006, as amended</td>
<td><a href="http://www.dpa.gr">www.dpa.gr</a></td>
</tr>
<tr>
<td>Hellenic Authority for Communication Security and Privacy</td>
<td>ADAE</td>
<td>According to Law 3115/2003 ADAE has the power a) to issue regulations regarding the assurance of the confidentiality of communications, b) to perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service, c) to hold hearings of the aforementioned entities, d) to investigate relevant complaints from members of the public and e) to collect relevant information using special investigative powers.</td>
<td><a href="http://www.adae.gr">www.adae.gr</a></td>
</tr>
<tr>
<td>Hellenic Telecommunications and Post Commission</td>
<td>EETT</td>
<td>EETT is the National Regulatory Authority, which supervises and regulates the</td>
<td><a href="http://www.eett.gr">www.eett.gr</a></td>
</tr>
</tbody>
</table>
telecommunications as well as the postal services market. It collaborates with HDPA and ADAE on ePrivacy related issues, but is not directly assigned with the supervision of the implementation of Law 3471/2006.

Explanation:

- The English website of ADAE refers to itself as “the Hellenic Authority for Communication Security and Privacy” (ADAE). However, the literal translation is Hellenic Authority for Communication Secrecy (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών).

- In relation to cases relating to the national implementation of the ePrivacy Directive that cover both internal and external elements of a communication, both Authorities (ADAE and HDPA) may have responsibility: The competences of the two Authorities are not always very distinct. In the 2006 Annual Report of the HDPA commented on the position that EETT is responsible for the security of communications at the level of physical security of the providers of electronic communications, while ADAE is responsible for the security of communications towards the aforementioned providers as well as the data controller who transmits data via networks, such as banks, hospitals etc, and HDPA is responsible for the protection of personal data of network users. The HDPA found that such an approach limits the protection of personal data to confidentiality issues and took the position that the distinction of competences between the three authorities is as follows:
  a) EETT is responsible for ensuring the integrity and availability of communication infrastructures, via which publicly available electronic communications are offered, especially as regards physical safety and to the extent that it is adequate for commercial networks.
  b) ADAE is responsible for the supervision of the procedures of legal interception and the protection of secrecy of communications, which are realised via publicly available electronic communications services and not in the context of private corporate networks and this only in regards of security relating to the confidentiality of communication.
  c) HDPA is responsible for the security of information and communications (network and IT infrastructures) of data controllers (organisations, services, and public and private sector companies) that create, collect, communicate and process personal data. HDPA is responsible for subscriber or user data, to the extent that the security of the technological infrastructure of publicly available electronic communications services relates to such data, and in any case after the end of the communication, i.e. during the stage of storing and further processing data. To the extent that ADAE imposes measures to safeguard the communications secrecy, especially during the communication phase, the two authorities
(HDPA and ADAE) should collaborate with each other to the extent that the measures relate to the protection of private life and personal data.\(^1\)

In the 2007 Annual Report the HDPA confirmed the position that the distinction between the safeguarding of the secrecy of a telephone communication (part of confidentiality) and the overall security of a telephone communication is neither clear nor necessarily useful.\(^2\) The HDPA has clearly expressed the opinion that the competence of ADAE not only on the secrecy of communications (which covers the content of a communication), but also on the confidentiality of communications, is overreaching the material scope of the competences that should be assigned to ADAE.\(^3\) However, in practice the two authorities are collaborating with each other when relevant cases appear.


3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Art. 2(6) of Law 4070/2012 defines *public communications network* as the network of electronic communications, which is used, in whole or mainly, for the provision of electronic communications services available to the public which support the transfer of information between network termination points.

Art. 2(7) of Law 4070/2012 defines *public telephone network* as the network of electronic communications that is used for the provision of telephone services available to the public. It supports the transfer of voice communications between termination points, as well as other forms of communication, such as fax and data.

Art. 2(8) of Law 4070/2012 defines *electronic communications services available to the public* as electronic communications services that are provided to the public.

Art. 2(9) of Law 4070/2012 defines *telephone service available to the public or public telephone service* as service available to the public for the creation and direct or indirect receiving of national calls or national and international calls via number or numbers that exist in national or international numbering plans.

Art. 2(17) of Law 4070/2012 defines *electronic communications network* as transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, as well as cable television networks, irrespective of the type of information conveyed.

Art. 2(30) of Law 4070/2012 defines *provision of electronic services network* as the establishment, control and making available of such a network.

Art. 2(31) of Law 4070/2012 defines *electronic services network provider* as an establishment that consists of, functions, controls or avails of electronic communications network.

Art. 2(49) of Law 4070/2012 defines *electronic communications services* as services normally provided for remuneration which consist wholly or partially in the conveyance of signals on electronic communications networks, including telecommunications services, and transmission services in networks used for broadcasting. Electronic communications services do not include services providing, or exercising editorial control over content transmitted using electronic communications networks and services and information society services, as defined in Article 2 Paragraph 2 of Presidential Decree 39/2001 (Α’28), as amended, which do not consist wholly or partially in the conveyance of signals on electronic communications networks.

However, Law 3471/2006 on the protection of privacy and data protection contains *different definitions for the terms “electronic communications services”, “public communications network” and “publicly available electronic communications services”*. 
More specifically Art. 2(8) of Law 3471/2006 defines “electronic communications services”: Any services normally provided for remuneration which consist wholly or partially in the conveyance of signals on electronic communications networks, including telecommunications services, and transmission services in networks used for broadcasting. Electronic communications services do not include services providing, or exercising editorial control over content transmitted using electronic communications networks and services and information society services, as defined in Article 2 Paragraph 2 of Presidential Decree 39/2001 (A’28), as amended, which do not consist wholly or partially in the conveyance of signals on electronic communications networks. Short messages (SMS), multimedia messages (MMS) and other similar applications are included in this definition. (The last sentence of Art 2(8) was added via Art. 168(1)(c) of Law 4070/2012 and differentiates the definition of Law 3671/2006 from the definition of electronic communications services in Law 4070/2012).

Art. 2(9) of Law 3471/2006 defines “public communications network”: Any electronic communications network used, fully or mainly, for the provision of publicly available electronic communications services. The definition of Public communications network of Law 4070/2012 requires that the networks “support the transfer of information between network termination points”. Most likely the Greek legislator did not update the definition in Law 3471/2006 in order to match the amended definition of public communications network, as introduced in Directive 2009/140/EC and implemented in the Greek legislation via Law 4070/2012.

Art. 2(10) of Law 3471/2006 defines “publicly available electronic communications services”: Any electronic communications services provided to the public.

According to the European definition a “electronic communications service” consist wholly or mainly of the transmission of signals to electronic communications networks. However the Greek legislator requires that such a service consists wholly or partially of the transmission of signals to electronic communications networks, broadening the scope of electronic communications services.

Moreover one should also keep in mind that the data or activities addressed by the provisions of the ePrivacy Directive involve the processing of personal data. As such the scope of these provisions is also determined by the (scope of the) Greek data protection law and in particular by the provision transposing Art. 4 of Directive 95/46/EC.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

| The answer to this question entirely depends on whether or not these services “consist wholly or partially in the conveyance of signals on electronic communications networks”, as defined in Art. 2(8) of Law 3471/2006. The Greek law does not require that the services consist “wholly or mainly” in the conveyance of signals on electronic communications networks, but it is sufficient that the service “partially” consists of such conveyance. Therefore it may be easier under Greek law to claim that services such as VoIP, webmail and location based services fall under the scope of Law 3471/2006. Although the HDPA has not dealt with cases dealing with specific types of providers such as webmail or VoIP ones, it takes the position that while it is clear that webmail services will fall under the scope of Law 3471/2006, the VoIP services will most likely be considered as content services and will remain outside the protective ambit of the law.

Furthermore, broadcasting services (and services provided by the information society, which are more content-oriented than transport-oriented) are – naturally – also excluded. |
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

Law 3471/2006 specifies its material scope of application in Art 3. Although the territorial scope is not specified in Law 3471/2006, Art 3(2) states that “Law 2472/1997 (GGB 50A), as effective and the laws in execution of Art. 19 of the Constitution, as effective, shall apply to all matters in connection with the provision of electronic communications services that are not regulated explicitly by the present law”. Article 3(3) of Law 2472/1997 states that “The present law shall apply to any processing of personal data, provided that such processing is carried out:

a) by a Controller or a Processor established in Greek Territory or in a place where Greek law applies by virtue of public international law.

b) by a Controller who is not established in the territory of a member-state of the European Union or of a member of the European Economic Area (EEA) but in a third country and who, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the Greek territory, unless such equipment is used only for purposes of transit through such territory. In this case, the Controller must designate in writing, by a statement addressed to the Authority, a representative established in the Greek territory, who will substitute the Controller to all the Controller’s rights and duties, without prejudice to any liability the latter may be subject to. The same shall also apply when the Controller is subject to extraterritoriality, immunity or any other reason inhibiting criminal prosecution.”

According to ADAE the current regime leaves a lot of open issues in relation to transnational cases; for instance situations where the provider is established outside Greece, although they are incurring a breach of confidentiality of communications to a Greek citizen. Similarly the HDPA understands the territorial scope of Law 3471/2006 as covering only providers that have an establishment in Greece. There have been interesting cases of providers established in Cyprus, who although they have received a licence by the Hellenic Telecommunications and Post Commission (EETT), do not fall under the Greek Law 3471/2006, and therefore HDPA had to refer the relevant cases to the Cypriot DPA.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

<table>
<thead>
<tr>
<th>Section</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. national enforcement authorities mentioned under section A</td>
<td>(either through general guidance documents or through decisions in concrete cases)</td>
</tr>
<tr>
<td>b. national courts through rendering of case law</td>
<td></td>
</tr>
</tbody>
</table>

a. We are not aware of any guidance on the interpretation and/or scoping of the definitions mentioned in this section
b. We are not aware of any case law on the interpretation and/or scoping of the definitions mentioned in this section
<table>
<thead>
<tr>
<th>7. What is your individual view of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?</td>
</tr>
<tr>
<td>b. possible improvements of the effectiveness of this legal framework.</td>
</tr>
</tbody>
</table>

| a. The distinction between providers of electronic communications services and providers of information society services is, in the context of the application of provisions with regard to privacy and personal data protection, irrelevant. It seems that the exclusion of information society service providers from the scope of Law 3471/2006 can create practical difficulties with regard to services that do not clearly fall either in one or the other category (i.e. electronic communications service or information society service). This point is further strengthened by the choice of the Greek legislator that an electronic communications service consists wholly or partially of the transmission of signals to electronic communications networks, broadening the scope of electronic communications services, compared to the European definition. |
| b. Given that the distinction between providers of electronic communications services and providers of information society services is entirely irrelevant in the context of the application of provisions with regard to privacy and personal data protection, this aspect of the ePrivacy Directive should better be revised. Several provisions of Law 3471/2006 as already applicable to information society service providers, e.g. the ones of cookies and unsolicited communications. |
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Article 19 of the Greek Constitution safeguards the secrecy of communications, stating that “Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable”.

Art. 4(1) of Law 3471/2006 provides that “any use of electronic communications services offered through a public communications network and publicly available electronic communications services, as well as the related traffic and location data, as described in art. 2 of [Law 3471/2006], shall be protected under the confidentiality of communications. The withdrawal of confidentiality shall be allowed only under the conditions and procedures provided for in Art. 19 of the Constitution”. Paragraph 2 of Article 4 Law 3471/2006 prohibits the “listening, tapping, storage or other kind of interception or surveillance of electronic communications and the related traffic and location data, except when otherwise legally authorised”. Finally Art 4(4) allows technical storage “with the reservation of complying with the obligations arising from the protection of confidentiality, according to [Law 3471/2006], when necessary for the conveyance of the communication”.

The term communication is defined in Art 2(5) of Law 3471/2006 as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network, except those cases in which the information can relate to the identifiable subscriber or user receiving it”. The definition is in line with the definition of communication in the ePrivacy Directive.

ADAE published in 2011 a Regulation for the Assurance of Confidentiality in Electronic Communications\(^4\) on the Security Policy for the Assurance of Communications Confidentiality that concerns all persons involved in providing electronic communications networks and/or services. ADAE also published two recommendations for the protection of the confidentiality of communications relating to lawful interception.\(^5\)

---


The content of communications is protected directly by the Greek Constitution and legal interception (relating to the content of the communications) is regulated under Law 2225/1994 and Presidential Decree 47/2005, remaining however outside the scope of the provisions transposing the ePrivacy Directive.


2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

This provision has been transposed in Article 4(3) of Law 3471/2006.

Art. 4(3) of Law 3471/2006 stipulates that “The recording of communications and the related traffic data is allowed, when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication, under the condition that both parties have provided their consent, after previous information as to the aim of the recording. An act by the Data Protection Authority defines the manner in which parties are informed and provide consent, as well as the manner and duration of storage for the recorded conversations and related traffic data”.

However, such an act from the HDPA is most likely not going to be issued, as the issue of providing information to users has been already discussed since 2006, and the DPA has confirmed this position in a number of relevant cases. The HDPA has found that the recording of conversations for the ordering of goods or services, as well as for subscribers data and issues relating to the bills of subscribers of mobile telephony is legitimate. To the contrary the request for recording of threatening customer calls was not granted, neither was the request for sample recording of calls for the purpose of training of call-centre staff.

In the document with protocol number G/EX/596-1/07-03-2013 (ΓΕΞ/596-1/07-03-2013), the HDPA found that the services offered via line 14541, which provides a telephone information service for ferry routes, have a purely informative character and therefore they are not covered by the exception of Art. 4(3) of Law 3471/2006, as it cannot be deduced that the purpose of the recording of the telephone conversations is the provision of evidence of a commercial transaction or of any other business communication (as it would be required under Art. 4(3) of Law 3471/2006).

---


10 HDPA Annual Report 2013, pp.94, available online only in Greek at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2013/ARXH%20PROSTASIAS_APOLOGISMOS%202013%20WEBUSE.PDF.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

| Law 3471/2006 does not provide for any other exceptions to the confidentiality principle. The regulation of legal interception falls outside the scope of this question. |
4.
a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?
b. Is there any other important legislation with regard to the protection of private electronic communications?
   a. The Greek legislation doesn’t explicitly address “automated breaches of confidentiality without human intervention”. In principle such breaches of confidentiality will be considered as an infringement of Article 4 Law 3471/2006.

   With regard to the distinction between the protection of content of the communications and the external elements of a communication (e.g. traffic data), according to Arts. 3 and 4 of Presidential Decree 47/200511 not only the internal elements of a communication (i.e. content), but also the external elements (e.g. identification data of the parties, method and time of the communication, location of the parties etc) are protected under the confidentiality of communications.

   b. We are not aware of any other important legislation with regard to the protection of private electronic communications.

---

11 Presidential Decree 47/2005, Procedures as well as technical and organisational sasfeguards for legal interception and its protection, GG Α’ 64/10.03.2005 (Προεδρικό Διάταγμα 47/2005, Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του, ΦΕΚ Α’ 64/10.03.2005 available online at http://www.dsanet.gr/Epikairothta/Nomothesia/pd47_05.htm).
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

<table>
<thead>
<tr>
<th>a. the scope and substance of your national implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?</td>
</tr>
</tbody>
</table>

a. As regards the use of “cookies” and other techniques whereby, especially through the internet, it is possible to get remote access to the user’s end equipment and/or to store data on this equipment, Article 4(5) of Law 3471/2006 provides the following:

“The storage of data or the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed if the specific subscriber or user has given his/her consent following clear and detailed information, according to art. 11, par. 1 of law 2472/1997, as effective. The consent of the subscriber or user can be given by means of appropriate settings in the web browser or by means of another application. The above shall not impede any technical storage or access, the sole purpose of which is the conveyance of a communication through an electronic communications network, or which is necessary for the provision of information society services explicitly requested by the user or subscriber. An act by the Data Protection Authority defines analytically the manner in which information is provided and consent is declared”.

However, such an act from the HDPA is most likely not going to be issued, as the issue of providing information to users has been already discussed since 2006, and the DPA has confirmed this position in a number of relevant cases.  

Article 4(4) of Law 3471/2006 is not specifically addressed to “providers of electronic communications services or networks” but aims at protecting all subscribers or users. The HDPA gives as examples of entities that will need to acquire user/subscriber consent for the installation and use of cookies the provider of an internet service (e.g. an on-line store) or a third party (e.g. advertising network that promotes products via the website of an on-line store)13, who clearly do not qualify as “providers of electronic communications services or networks”

b. The provision quoted above doesn’t distinguish between types of cookies or between categories of end equipment.

---


13 HDPA: [http://www.dpa.gr/portal/page?_pageid=33,146950&_dad=portal&_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,146950&_dad=portal&_schema=PORTAL)
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

<table>
<thead>
<tr>
<th>Article 4(5) of Law 3471/2006 specifically states that the consent “can be given by means of appropriate settings in the web browser or by means of another application”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Hellenic DPA has a dedicated webpage on the use of cookies on the internet, where detailed information is provided on how to obtain informed consent for the installation and use of cookies, what is the best way to inform the users, cookies for advertising and web analytics etc.</td>
</tr>
<tr>
<td>According to the HDPA, the consent of the user or the subscriber can be provided via the website of the website provider via adequate measures, e.g. pop-up windows. The acceptance of cookies can be realised at once for all cookies installed by the same information society service provider. Alternatively, consent can also be provided via special settings of the web browser or other application. Art. 4(5) of Law 3471/2006 explicitly states that “The consent of the subscriber or user can be given by means of appropriate settings in the web browser or by means of another application”. However, default settings of the web browser that accept all cookies do not qualify for the provision of valid consent. For example web browsers or other applications that by default reject third party cookies and require active choice off the user in order to accept the installation of and further transmission of the cookies from specific websites can offer valid and effective consent. To the contrary, in cases when the default settings of the web browser allow the acceptance of all cookies and the user has to act in order to deactivate them, then the consent requirements are not met. The requirements for valid consent are also not met when the web browser settings allow the prior rejection of cookies from specific information society service providers (e.g. via “black lists”) or similar mechanisms, which, although they offer the user or the subscriber more choices, they do not require the user to provide consent to the installation of cookies from providers that are not included in the back list. The HDPA highlighted that it is crucial to provide the subscriber or the user the possibility to withdraw their consent in the same way as they offered it.</td>
</tr>
<tr>
<td>According to the HDPA the information of the user or the subscriber should be provided in the most adequate way, in order to ensure sufficient information before the storage or the gaining of access to information in their terminal equipment. For example a general information in the general terms of service or terms of use of the service, as well as information included in the privacy policy, which is usually lengthy and cover a number of issues relating to the protection of personal data, is not considered as adequate in the context of installation of cookies. To the contrary, the information has to be uploaded on a clearly visible part of the website and be specific for each case.</td>
</tr>
</tbody>
</table>

14 http://www.dpa.gr/portal/page?_pageid=33,146950&_dad=portal&_schema=PORTAL
15 HDPA: http://www.dpa.gr/portal/page?_pageid=33,147142&_dad=portal&_schema=PORTAL
16 HDPA: http://www.dpa.gr/portal/page?_pageid=33,147142&_dad=portal&_schema=PORTAL
17 HDPA: http://www.dpa.gr/portal/page?_pageid=33,147164&_dad=portal&_schema=PORTAL
The HDPA has clearly taken the position that cookies installed for online advertising do not fall under the exception from the obligation to obtain consent.\textsuperscript{18}

\textsuperscript{18} HDPA: \url{http://www.dpa.gr/portal/page?_pageid=33,147230&_dad=portal&_schema=PORTAL}.\!
The exceptions from the information obligation and the consent requirement are in line with the provisions of the ePrivacy Directive.¹⁹

The exceptions from the information obligation and the consent requirement are specified in Art 4(5) of Law 3471/2006 and cover technical storage or access, the sole purpose of which is the conveyance of information through an electronic communications network, or which is necessary for the provision of information society services explicitly requested by the user or subscriber. These exceptions are in line with the provisions of the ePrivacy Directive. The HDPA follows the opinion of the Article 29 Data Protection Working Party in its opinion 4/2012 and recognises the following types of cookies as falling under the exception from the consent requirement:

- Cookies that are necessary for the recognition and/or conservation of context entered by the subscriber or the user during a website session throughout the given session (information filling-in a webform, adding products to shopping basket etc), including persistent cookies installed for such purposes that have a lifetime of a few hours.
- Cookies necessary for the authentication of the subscriber or the user to services that require authentication (e.g. for an online bank transaction).
- Cookies installed aiming at the security of the subscriber or the user, for instance cookies that identify repeated failed attempts to enter a user account on a specific website.
- Cookies with multimedia content, such as flash player cookies during a website session (e.g. cookies installed when watching a video).
- Cookies necessary for load balancing during a website session.
- Cookies remembering user or subscriber choices relating to the presentation of a website (e.g. on language preference).
- Cookies installed via plug-ins to social networking websites and relate to the distribution of content between registered members that are already logged in.²⁰

The HDPA has clearly taken the position that cookies installed for online advertising do not fall under the exception from the obligation to obtain consent.²¹

It should be noted that the old provision of law 3471/2006 on cookies was stricter than the original (initial – before the amendments) wording of Art 5(3) of the ePrivacy Directive and in practice in many cases the consent of the user or the subscriber was required. In particular the HDPA found in 2010 (before the implementation of the amendments to Art. 5(3) ePrivacy Directive in the Greek legal system) that the use of cookies for Google analytics used in the website www.apografi.gov.gr

---

¹⁹ See also [http://www.dpa.gr/portal/page?_pageid=33,147186&_dad=portal&_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,147186&_dad=portal&_schema=PORTAL).
that aimed at the inventorisation of public sector staff was only allowed after the consent of the users. The HDPA found that a public sector website offers information, useful for any interested party, that should not be deprived of it or gain access to it only under the condition that they accept a cookie (for Google analytics), let alone in the specific case where the public sector staff had to access the website for the inventorisation. Therefore, the website should offer access to it without the installation of cookies or should find other methods for the collection of statistical data. Following its position on the use of cookies for Google analytics, the HDPA published in 2011 (before the implementation of the amendments to Art. 5(3) ePrivacy Directive in the Greek legal system) an opinion where it found that the installation of cookies for web analytics is allowed after the consent of the user.

---

22 Letter on the use of the service Google Analytics from the website of electronic inventorisation of staff obtaining salary from the Greek State www.apografi.gov.gr, 02.08.2010 (Χρήση της υπηρεσίας Google Analytics από την ιστοσελίδα της ηλεκτρονικής απογραφής των μισθοδοτουμένων από το Ελληνικό Δημόσιο www.apografi.gov.gr), unpublished.

8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The practical implementation of the new rules is still very diverse. Therefore, in relation to potential infringements of the provisions relating to cookies, the HDPA at a first phase aims at providing guidance on how the users or the subscribers can receive clear and detailed information, and how they can provide valid consent, and at the issuing of recommendations to the providers, without imposing fines. The HDPA is also in close collaboration with the IAB Greece, which is currently developing a code of conduct for the use of cookies.²⁴

---

9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

| a. | The information on the HDPA towards the regulation of cookies is mentioned in the relevant questions of this section. In short it can be said that The Hellenic DPA has a dedicated webpage on the use of cookies on the internet, where detailed information is provided on how to obtain informed consent for the installation and use of cookies, what is the best way to inform the users, cookies for advertising and web analytics etc. |
| b. | Not available |

25 http://www.dpa.gr/portal/page?_pageid=33,146950&_dad=portal&_schema=PORTAL.
10. What is your individual view of:

| a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country? |
| b. possible improvements of the effectiveness of this legal framework. |

| a. Without additional guidance of the HDPA the provisions of the Greek legislation transposing Art. 5.3 of the ePrivacy Directive are too vague to allow a consistent application in practice by service providers. The DPA aims at issuing recommendations to the entities that wish to install cookies. |
| b. In practice, website owners (information society service providers) start to implement the rules and inform users about the possibility to accept or refuse cookies in the form of a one-time banner that can easily be “clicked away”. IAB Greece is working, in collaboration with the HDPA on the development of a code of conduct for the use of cookies, which will hopefully introduce more clarity in the practical application of Art. 4(S) of Law 34714/2006. |
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Art. 2(3) of Law 3471/2006 defines traffic data as “data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data may, inter alia, consist of the number, the address or the identity of the connection or the terminal equipment of the subscriber and/or user, the passwords, location data, the date and time of beginning and end and duration of a communication, the volume of transferred data, information about the protocol the formatting, the routing of the communication, as well as they network from which the communication originates or terminates in.”

It is striking that the Greek definition of traffic data consider “passwords” as traffic data.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Art. 5 of Law 3471/2006 stipulates the rules for processing of personal data, including traffic and location data. More concretely it states that:

“1. The processing of personal data, including traffic and location data, must be limited to those absolutely necessary to serve the purposes thereof.
2. The processing of personal data is only allowed if:
   a. The subscriber or user has given consent after information as to the type of data, the purpose and extent of the processing, the recipients or categories of recipients, or
   b. The processing is necessary for the implementation of a contract to which the user or subscriber is party, or the taking of measures during the pre-contractual stage, following a request of the subscriber.
3. When the present law requires the consent of the subscriber or the user, the relevant statement is given in writing or by electronic means. In the latter case, the controller ensures that the subscriber or user acts in full awareness of the consequences of his/her statement, which is recorded in a secure manner, can be accessed by the user or subscriber at any time and can be withdrawn at any time.
4. The design and selection of technical means and information systems as well as the equipment for the provision of publicly available electronic communications services must be performed with the processing of the minimum personal data as the main criterion.
5. The provider of publicly available electronic communications services must enable the use and the payment of services anonymously or pseudonymously, to the extent that this is technically feasible and subject to law 3783/2009 (Official Gazette A´ 136/07.08.2009), as effective. In case of a dispute, the Hellenic Telecommunications and Post Commission (EETT) shall deliver an opinion on the technical feasibility of paying these services anonymously or pseudonymously.”

Article 6 of Law 3471/2006 is dedicated to traffic and location data. The first three paragraphs refer to the processing of traffic data:

“1. Traffic data relating to subscribers and users that are processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous at the end of the transmission of the communication, subject to law 3917/2011 (A´ 22) and paragraphs 2-6 of the present article.
2. For the subscriber’s billing and interconnection payment, if it is necessary, the provider of a public network or publicly available electronic communications services is allowed to process traffic data. The electronic communications service provider shall inform the subscriber as to the type of traffic data to be processed, as well as the duration of processing. This processing for the purposes of billing and payment is permitted for a period that cannot exceed twelve (12) months from the date of the communication, unless the bill has been challenged or the payment has not been settled. In that case the processing is permitted until the irrevocable resolution of the dispute. The transfer of traffic data to another provider of a public network or publicly available electronic communications service is permitted for the purpose of billing the services provided, under the condition that the subscriber or user is informed in an clear and appropriate manner in writing or by electronic means during the conclusion of the contract or before the transfer. Similarly, the transfer of the necessary traffic data and the personal data that are related to the contract is permitted for the only purpose of the collection of the bill payment under the condition that the subscriber or user is informed in an clear and appropriate manner in writing or by electronic means during the conclusion of the contract or before the transfer.
3. For the commercial promotion of the electronic communications services or for the provision of value added services the provider of a publicly available electronic communications service can process the traffic data to the extent and the duration needed, correspondingly, only if the subscriber or user has previously given his/her consent after he/she had been informed about the type of traffic data that are subject to processing, as well as the duration of processing. The consent can be withdrawn at any time. If it is withdrawn and if in the meantime the data have been disclosed to third parties, the withdrawal is announced to them by the provider. It is forbidden to the provider of a public network or of publicly available electronic communications services to depend the provision of these services to the subscriber or user on his/her consent to the processing of these data, for other purposes than those serving directly the provision of the services that are related to the articles of the present law”.

The Hellenic DPA has not dealt with many cases relating to traffic and location data and has not issued any relevant guidance or guidelines.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</th>
</tr>
</thead>
</table>
| Art. 6(1) of Law 3471/2006 states that “Traffic data relating to subscribers and users that are processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous at the end of the transmission of the communication, subject to law 3917/2011 (A’ 22) and paragraphs 2-6 of the present article”.
| (Law 3917/2011 implemented the Data Retention Directive into the Greek legal system). |
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

We are not aware of such cases.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions of Article 6 of the Law 3471/2006 are not sufficient for the protection of subscribers and users because their scope is limited to providers of publicly available electronic communications service or network. The processing of traffic data by network and service providers, other than “providers” falling under the scope of Article 6 is only protected via the general data protection legislation (in particular the proportionality principle).
D. Location data

| 1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects. |

The term “location data” is defined in Article 2(4) of Law 3471/2006, as follows: “data processed in an electronic communications network or by an electronic communications service that indicate the geographic location of the terminal equipment of a user of a publicly available electronic communications service”.

What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

<table>
<thead>
<tr>
<th>Art. 5 of Law 3471/2006 stipulates the rules for processing of personal data, including traffic and location data. More concretely it states that:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“1. The processing of personal data, including traffic and location data, must be limited to those absolutely necessary to serve the purposes thereof.</td>
</tr>
<tr>
<td>2. The processing of personal data is only allowed if:</td>
</tr>
<tr>
<td>a. The subscriber or user has given consent after information as to the type of data, the purpose and extent of the processing, the recipients or categories of recipients, or</td>
</tr>
<tr>
<td>b. The processing is necessary for the implementation of a contract to which the user or subscriber is party, or the taking of measures during the pre-contractual stage, following a request of the subscriber.</td>
</tr>
<tr>
<td>3. When the present law requires the consent of the subscriber or the user, the relevant statement is given in writing or by electronic means. In the latter case, the controller ensures that the subscriber or user acts in full awareness of the consequences of his/her statement, which is recorded in a secure manner, can be accessed by the user or subscriber at any time and can be withdrawn at any time.</td>
</tr>
<tr>
<td>4. The design and selection of technical means and information systems as well as the equipment for the provision of publicly available electronic communications services must be performed with the processing of the minimum personal data as the main criterion.</td>
</tr>
<tr>
<td>5. The provider of publicly available electronic communications services must enable the use and the payment of services anonymously or pseudonymously, to the extent that this is technically feasible and subject to law 3783/2009 (Official Gazette A’ 136/07.08.2009), as effective. In case of a dispute, the Hellenic Telecommunications and Post Commission (EETT) shall deliver an opinion on the technical feasibility of paying these services anonymously or pseudonymously.”</td>
</tr>
</tbody>
</table>

Article 6 of Law 3471/2006 is dedicated to traffic and location data. Art. 6(4) is dedicated to location data an reads as follows:

“4. The processing of data that indicate the geographic location of the terminal equipment of a subscriber or user of a public network or publicly available electronic communications services for the provision of value added services is permitted only if these are rendered anonymous or with the explicit consent of the subscriber or user to the extent and for the duration necessary for the provision of an value added service. The service provider shall inform the user or subscriber, prior to obtaining his/her consent, about the type of data which will be processed, the purposes and duration of the processing and whether the data may be transmitted to third parties for the purpose of providing the value added service. The consent can be withdrawn at any time. Users or subscribers shall be given the possibility during each connection to the network or communication transmission, to temporarily refuse the processing of the given data using simple means and free of charge.”

Article 6(5) of Law 3471/2006 regulates the use of traffic data for emergency services:

“5. Exceptionally, the processing of location data by the providers of a public communications network or publicly available electronic communications service is permitted without the prior
consent of the subscriber or the user, in order to provide to the competent authorities dealing with emergency situations, such as law enforcement agencies, ambulance services and fire brigades, the information necessary for the localisation of the caller and only for this specific purpose. The procedures, manner and all other technical details pertaining to the implementation of the present provision shall be described in an act by the Hellenic Authority for Ensuring the Secrecy of Communications (ADAE).”

In short, according to the provisions of article 171(5) of L. 4070/2012, which amended Art. 6(5) of Law 3471/2006, the processing of location data by providers of public communications networks or publicly available communications services is permitted without the prior consent of the subscriber or user, in order to provide the authorized organizations dealing with emergency calls, such as law enforcement agencies, ambulance services and fire brigades, the necessary information required for the tracking of the caller location and only for that particular purpose. The procedures and any technical details regarding the implementation of this provision are determined by ADAE by means of a regulatory Act. The Act of ADAE was adopted in 2008 (Decision Nr. 216/2008).26

The HDPA issued in 2012 a decision on the terms and conditions for the provision of geolocalisation services to vulnerable groups and minors in compliance with the protection of persona data.27 With regard to the processing of location data, the HDPA found that in the given case the processing was carried out for the purposes of the personal safety of the data subjects and for the provision of emergency services.28

The Hellenic DPA has not dealt with many cases relating to traffic and location data and has not issued any relevant guidance or guidelines.

---

27 Decision 112/2012 (27.06.2012) Terms and conditions for the provision of geolocalisation services of vulnerable groups and minors in compliance with the protection of persona data, available online in Greek at http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=182,50,191,223,158,152,237,19.
28 Decision 112/2012 (27.06.2012) Terms and conditions for the provision of geolocalisation services of vulnerable groups and minors in compliance with the protection of persona data, available online in Greek at http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=182,50,191,223,158,152,237,19.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

| Article 6(4) of Law 3471/2006 is worded as follows: “The processing of data that indicate the geographic location of the terminal equipment of a subscriber or user of a public network or publicly available electronic communications services for the provision of value added services is only permitted if these are rendered anonymous or with the explicit consent of the subscriber or user to the extent and for the duration necessary for the provision of an value added service”.
|
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>We are not aware of any such guidance</td>
</tr>
<tr>
<td>b.</td>
<td>We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)</td>
</tr>
</tbody>
</table>
### 5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

<table>
<thead>
<tr>
<th>Article 5(4) of Law 3471/2006 doesn’t sufficiently protect individuals against illegitimate processing of location data because the scope of the Article is limited to providers of publicly available electronic communications services or networks.</th>
</tr>
</thead>
</table>

E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. Article 11 of Law 3471/2006 regulates unsolicited communications in its paragraph 1 as follows:
      “1. The use of automated calling systems, especially via the use of facsimile machines (fax) or electronic mail, and in general the realisation of unsolicited communications via any electronic communications means, without human intervention, for the purposes of direct marketing of goods or services, or any advertising purposes is allowed only if the subscriber have given his/her prior consent.”

      The HDPA, via a document with protocol number 1713/07-03-2013, found that political communication falls under the provisions of Art. 11 Law 3471/2006, given that commercial communication is not only carried out by commercial establishments, but also by political parties.  
      The DPA published in 2010 a Guidance on political communication differentiating between different means of sending unsolicited communications to prospective voters.

   b. Although Art. 13(1) of the ePrivacy Directive refers to both subscribers and users, the Greek law refers only to subscribers.

      Another important difference is that although the Directive, when it comes to subscribers, applies only to natural persons (see Art. 13(5) ePrivacy Directive), the Greek provisions on unsolicited communications apply also to subscribers that are legal persons, as explicitly mentioned in Art. 11(7) of Law 3471/2006, as amended: “The above regulations apply also to subscribers who are legal persons”.

      Finally, the 13(1) ePrivacy Directive regulates the use of specific means “for the purposes of direct marketing”. However, the Greek implementation of the provision is more concrete covering “the purposes of direct marketing of goods or services, or any advertising purposes”.

---

29 HDPA Annual Report 2013, pp.98, available online only in Greek at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2013/ARXH%20PROSTASIAS_APOLOGI SMOS%202013%20WEBUSE.PDF.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Paragraph 2 of Article 11 of Law 3471/2006 regulated the use of unsolicited communications with human intervention (calls) and was amended via Art. 16(2) of Law 3917/2011 introducing an opt-out rule:

“2. Unsolicited communications with human intervention (calls) for the above purposes must not be performed, if the subscriber has stated to the provider of the publicly available electronic communications service that he/she does not wish to accept such communications in general. The provider must enter these statements in a special subscriber directory, which shall be at the subscriber's disposal, free of charge”.

Art. 11(1) of Law 3471/2006 was covering “the use of automated calling systems with or without human intervention”. However Art. 16(1) of Law 3917/2011 deleted the words “with or” leaving only “the use of automated calling systems without human intervention” under the protective ambit of Art 11(1) of Law 3471/2006 and in line with the wording of the Directive.

The introduction of an opt-out regime for the realisation of unsolicited communications with human intervention (calls)31, was dictated due to the excessive number of claims that were addressed to the DPA on such calls. The new regime (as of 2011) foresees that the subscriber states to the provider of the publicly available electronic communications service that they do not wish to accept such communications in general; the provider must enter these statements in a special subscriber directory, which shall be at the subscriber’s disposal, free of charge (Art 11(2) Law 34714/2006, as amended). A problem that has arisen in practice is that there is no unified directory, which makes consultation of the directories and consequently the application of the provision in practice very difficult. This is an issue that the DPA is currently looking into.

---

31 Art. 16 par. 1 of law 3917/2011, which implemented the Data Retention Directive. Law 3917/2011 Retention of data that are generated or processed in connection with the provision of publicly available electronic communications services or public communications networks, use of surveillance systems via obtaining or recording sound or image at public areas and relative provisions, GG Α’ 22/21.02.2011 [Νόμος 3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις, ΦΕΚ Α’ 22/21.02.2011, available online in Greek at http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QrtC22wFYAFdDx4L2G3dtvSoClrL8fWfWt9l9LdkF53Ulxsz942Cdysx5SQYNuqAGCF0lfB9HI6hq62kZV96Fis4Vx0wZ4DJEF7ZC9POpV8pFNoxXD0P2tuuZovvHjKz].
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Article 11(3) of Law 3471/2006, as amended by Art. 172(1) of Law 4070/2012, and in line with Art 11 of the ePrivacy Directive, introduces the exception for existing customers. The exception exempts consent by one's customers to send advertisements by electronic mail when the conditions have been met, cumulatively:

- The exception covers only the contact details for electronic mail of the recipient of the communication.
- The contact details for electronic mail must have been legitimately obtained in the context of the sale of a product or service or other transaction.
- The contact details for electronic mail may be used for direct marketing of similar products or services by the supplier or the fulfilment of similar purposes.
- The recipient of the message must be clearly and distinctly given the opportunity to object, in an easy manner and free of charge, to such collection and use of their electronic contact details, when collecting the contact data, as well as on the occasion of each message in case the user has not initially refused such use.

While the HDPA has suggested best practices for the provision of consent via SMS in its Guidance 2/2011, in practice the major problem is that it is difficult to include the information necessary for the efficient application of an opt-out procedure.

A second exception to the opt-in mechanism concerns unsolicited communications with human intervention (calls), as discussed under Section E, question 2, above.

---

Electronic mail is defined in Art. 2(7) of Law 3471/2006 as “any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient”. This definition covers not only electronic mail through the internet, but also MMS/SMS/text messages, voice mail, etc., in line with the definition of “electronic mail” in the ePrivacy Directive.

The HDPA has found that the sending of advertising SMSs to mobile phones without the prior consent of the recipients and without safeguarding the rights of information and access violates Art. 11 of Law 3471/2006. The HDPA published Guidance 2/2011 on the provision of electronic consent in the context of Art. 11 of Law 3471/2006. The focus of the guidance was on the identification of the user, who wishes to receive email, SMS or telephone calls for the promotion of products or services without becoming at the same time the recipient of spam messages. The guidance analyses the legitimate requirements for electronic consent and the obligations for the information of the subscribers. It also presents best practices that should be followed by data controllers, when realising promotional activities via email, written messages (SMS-MMS) and telephone calls, as well as when invitations are sent to friends for electronic consent. In such cases, the data controller has to follow special procedures in order to confirm the consent declaration of the subscriber or the user, such as the “procedure for the provision of consent with additional information” or the “double opt-in procedure”. Finally the Guidance proposed technical measures in order to avoid the mass sending of advertising messages. The Guidance has an Annex with examples for the application of the best practices it introduces.

---

35 A summary of the content of the Guidance can also be found in the HDPA Annual Report 2011, section 3.7.2, available online in Greek at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2011/ARXH_PROSTASIAS_2011.PDF.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. The HDPA deals with a large number of cases relating to unsolicited communications every year, issuing about 150-200 recommendations to providers and about 5-10 decisions imposing fines per year.  

As also mentioned under the previous question, the HDPA published Guidance 2/2011 on the provision of electronic consent in the context of Art. 11 of Law 3471/2006. The focus of the guidance was on the identification of the user, who wishes to receive email, SMS or telephone calls for the promotion of products or services without becoming at the same time the recipient of spam messages. The guidance analyses the legitimate requirements for electronic consent and the obligations for the information of the subscribers. It also presents best practices that should be followed by data controllers, when realising promotional activities via email, written messages (SMS-MMS) and telephone calls, as well as when invitations are sent to friends for electronic consent. Finally the Guidance proposed technical measures in order to avoid the sending of advertising messages. The Guidance has an Annex with examples for the application of the best practices it introduces.

The HDPA has been very active on issue relating to unsolicited communications. Under the dedicated webpage “Promotion of products and services” the DPA offers extensive information to citizens and data controllers on the sending of unsolicited communications, under which circumstances this is allowed and how can the users be protected against them.

Moreover (as already discussed under Section E, Question 1), the HDPA published Guidance 1/2010 on political communication differentiating between different means of sending unsolicited communications to prospective voters.

b. There is very little jurisprudence on the application of the rules with regard to unsolicited direct marketing communications.

---

36 See for example HDPA Annual Report 2013, sections 3.7.4 and 3.7.5, available online only in Greek at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2013/ARXH%20PROSTASIAS_APOLOGI%20SMOS%20WEBUSE.PDF. The HDPA has issued a number of decisions on spam, such as 109/2013, 100/2013, 86/2013 etc.


38 http://www.dpa.gr/portal/page?_pageid=33,124936&_dad=portal&_schema=PORTAL

6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The introduction of an opt-out regime for the realisation of unsolicited communications with human intervention (calls), was dedicated by the excessive number of claims that were addressed to the DPA. The new regime (as of 2011) foresees that the subscriber states to the provider of the publicly available electronic communications service that they do not wish to accept such communications in general; the provider must enter these statements in a special subscriber directory, which shall be at the subscriber’s disposal, free of charge (Art 11(2) Law 3471/2006, as amended). A problem that has arisen in practice is that these no unified directory, which makes consultation of the directories and consequently the application of the provision in practice very difficult. This is an issue that the DPA is currently looking into.

Art 11(5) of Law 3471/2006 introduced an obligation for providers of electronic communications services to take suitable measures for the prevention of unsolicited communications. Although this provision is in accordance with Article 13(3) of the ePrivacy Directive, the Greek legislator introduced the additional requirement that the suitable measures will be “defined by a common act of the DPA and ADAE”. This provision created problems in practice as the common act has not been issued yet and the providers –via a literal translation of the provision- are not required to take the necessary and adequate measures for the prevention of unsolicited communications, before the issuing of the act. The introduction of an obligation for providers of electronic communications services to take suitable measures for the prevention of unsolicited communications was seen as a positive addition to the ePrivacy Directive, although the Greek implementation that the suitable measures will be “defined by a common act of the DPA and ADAE”, creating problems in the practical application of the provision.

It seems that the number of e-mails addressed to Greek internet users that are unsolicited messages is higher than the European average, reaching 80% (so-called “spam”, http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/). This has lead to an excessive burden of the HDPA in resolving cases relating to spam: The HDPA deals with a large number of cases relating to unsolicited communications every year, issuing about 150-200 recommendations to providers and about 5-10 decisions imposing fines per year.43

---

40 Art. 16 par. 1 of law 3917/2011, which implemented the Data Retention Directive. Law 3917/2011 Retention of data that are generated or processed in connection with the provision of publicly available electronic communications services or public communications networks, use of surveillance systems via obtaining or recording sound or image at public areas and relative provisions, GG Α’ 22/21.02.2011 [Νόμος 3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις, ΦΕΚ Α’ 22/21.02.2011, available online in Greek at http://www.et.gr/idocs-nph/search/pdfViewerForm.html?args=5C7QtC22wFYAfDx4L2G3dtySoClrl8fyWInrOQqHtI9ILGd35F3Uljsx5Q2CdQxvSQYNuqAGCpFtH9H6h6gZkZV96Fls4vX0wZ4DlE7ZC9POpV8pFNovXDi8GPZtuuZocvHjkZM].

41 Art 11(5) of Law 3471/2006, as amended.


43 See for example HDPA Annual Report 2013, sections 3.7.4 and 3.7.5, available online only in Greek at http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2013/ARXH%20PROSTASIAS_APOLOGI
The HDPA has issued a number of decisions on spam, such as 109/2013, 100/2013, 86/2013 etc.
COUNTRY REPORT

SPAIN

For the Study

*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Miquel Peguera. Universitat Oberta de Catalunya

Date: 18 August, 2014
Contents

Part 1: Management summary ............................................................................................................. 3
Part 2: Answers to the questionnaire .................................................................................................. 4
**Part 1: Management summary**

The transposition of the e-Privacy Directive into Spanish law can be summarized as follows:

- Directive 2002/58/EC was initially transposed through the General Law on Telecommunications of 2003 (Law 32/2003 of 3 November) which regards to electronic communications networks and services, and through the Law on Information Society Services and Electronic Commerce (Law 34/2002, of 11 July) with regards to unsolicited communications and the use of cookies. The 2009 amendments to the Directive were subsequently transposed into Spanish Law. This was done first through the “Royal Decree-Law 13/2012, of 30 March, transposing Directives with regards to internal markets of electricity and gas and to electronic communications, and adopting measures to correct deviations due to costs and revenue gaps in the sectors of electricity and gas.” This Royal Decree-Law amended both the General Law on Telecommunications of 2003 and the Law on Information Society Services. More recently, the legal framework has been amended again through the new General Law on Telecommunications of 2014, which has repealed the former Law of 2003 and has modified again the Law on Information Society Services.

- The scope of the implementing provisions varies. The rules implemented in the General Law on Telecommunications do not apply to information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. On the other hand, the provisions implemented in the Law on Information Society Services, namely the rules on cookies and unsolicited commercial communications, do apply to any information society service.

- Art. 5(3) of the Directive regarding cookies has been implemented almost verbatim, including the exceptions provided for in the Directive. The Spanish Data Protection Authority, which is the competent body for enforcing this provision, released a “Guide on the use of cookies”, elaborated in close cooperation with the industry. To a large extent the Guide follows the criteria put forward by the Article 29 Data Protection Working Group and provides useful guidance on how to comply with the provision. A number of infringement decisions have already been rendered by the Data Protection Authority.

- Rules on traffic and location data have been implemented in the General Law of Telecommunications, though the business exception of Art. 5(2) has not been expressly transposed.

- Rules on unsolicited commercial communications are implemented in the Law on Information Society Services, more or less literally. Nonetheless, the material scope of the transposition may be wider as the law refers not only to *electronic mail* but also to “*other equivalent means of electronic communication*”. In addition, the implementing provisions are not limited to the cases where the recipient is a natural person, unlike in Art. 13(5) of the Directive. The competence for enforcing these rules lies with the Spanish Data Protection Authority which has made a number of infringement decisions.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject

| The transposition of Directive 2002/58/EC in its current form is to be found in following Laws: |

Directive 2002/58/EC had initially been partially transposed into Spanish Law, with regards to electronic communications networks and services, through the General Law on Telecommunications of 2003 (Law 32/2003 of 3 November), and through Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce (with regards to unsolicited communications and the use of cookies).

The 2009 amendments to the Directive 2002/58 were subsequently transposed into Spanish Law. This was done first through the “Royal Decree Law 13/2012, of 30 March, transposing Directives with regards to internal markets of electricity and gas and to electronic communications, and adopting measures to correct deviations due to costs and revenue gaps in the sectors of electricity and gas.” This Royal Decree Law amended both the General Law on Telecommunications of 2003 and the Law on Information Society Services. More recently, the legal framework has been amended again through the new General Law on Telecommunications of 2014, which has replaced the former Act of 2003 and has newly modified the Law on Information Society Services.

| Concordance table |
| Transposed into national law by: |
| ePrivacy Directive | URL |
|--------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------|
| Art. 5.2 (Business exception) | Not specifically transposed.                                         |                                                                     |
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agencia Española de Protección de Datos</td>
<td>Spanish Data Protection Authority</td>
<td>Provisions affecting user’s rights to privacy or data protection. It enforces as well the provisions regarding cookies and unsolicited commercial communications.</td>
<td><a href="http://www.agpd.es/">http://www.agpd.es/</a></td>
</tr>
<tr>
<td>Ministerio de Industria, Energía y Turismo</td>
<td>Ministry of Industry, Energy and Tourism</td>
<td>Provisions affecting electronic communications other than those enforced by the Data Protection Authority and by the National Commission for the Markets and the Competence</td>
<td><a href="http://www.minetur.gob.es/">http://www.minetur.gob.es/</a></td>
</tr>
<tr>
<td>Comisión Nacional de los Mercados y de la Competencia</td>
<td>National Commission for the Markets and the Competence</td>
<td>Provisions which are not directly related to the aspects examined in this report</td>
<td><a href="http://www.cnmc.es/">http://www.cnmc.es/</a></td>
</tr>
</tbody>
</table>

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The General Law on Telecommunications of 2014 includes the following definitions:

**“Electronic communications network**: transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including
satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.”

(General Law on Telecommunications of 2014, Annex II, No. 31). This definition is a verbatim transcription of the definition provided by the Framework Directive.

“Public communications network: an electronic communications network used wholly or mainly for the provision of publicly available electronic communications service which support the transfer of signals between network termination points.”

(General Law on Telecommunications of 2014, Annex II, No. 32). This definition is an almost verbatim transcription of the definition provided by the Framework Directive.

“Associated services: those services associated with an electronic communications network and/or an electronic communications service which enable and/or support the provision of services via that network and/or service or have the potential to do so and include, inter alia, number translation or systems offering equivalent functionality, conditional access systems and electronic programme guides, as well as other services such as identity, location and presence service.”

(General Law on Telecommunications of 2014, Annex II, No. 34). This definition is a verbatim transcription of the definition provided by the Framework Directive.

“Electronic communications service: that normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing content transmitted using electronic communications networks and services or activities consisting of exercising editorial control over the said contents; it does not include, either, information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.”

(General Law on Telecommunications of 2014, Annex II, No. 34). This definition is an almost verbatim transcription of the definition provided by the Framework Directive.

Regarding providers, the General Law on Telecommunications of 2014 defines an “operator” as the “natural or legal person who exploits public electronic communication networks or provides publicly available electronic communication services, and has notified to the Ministry of Industry, Energy and Tourism the start of its operations or is registered with the Register of Operators.”

It must be noted that provisions regarding the use of cookies (art. 5(3) of the ePrivacy Directive) and those dealing with unsolicited commercial communications (art. 13 of the ePrivacy Directive) are located in the Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce.

In both cases (cookies and unsolicited communications) the provisions apply to information society service providers, which are defined as a “natural or legal person which provides an information society service” (Law on Information Society Services, Annex of Definitions, c)). An information society service is defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” (Annex of Definitions, a)). The Annex provides an indicative list of information society services which includes the sending of commercial communications.
### 4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

As noted, the e-Privacy Directive has been implemented through two different legal instruments – the General Law on Telecommunications of 2014 and the Law on Information Society Services – each one with a different scope of application.

The scope of the General Law on Telecommunications of 2014 is that of telecommunications, which encompasses the exploitation of networks and the provision of electronic communication services and the associated facilities (see Art. 1). The scope of the Act expressly excludes audiovisual communication services, audiovisual contents transmitted through the networks and the basic regulation of audiovisual media. Moreover, the Act excludes from its scope services providing content transmitted using electronic communications networks and services, the activities consisting of exercising editorial control over the said contents, and the information society services (regulated in the Law on Information Society Services) which do not consist wholly or mainly in the conveyance of signals on electronic communications networks (see Art. 1).

Services more focused on contents will generally be understood as information society services covered by the Law on Information Society Services. It is a matter of interpretation to determine whether or not these services (VoIP, webmail, location-based services) consist wholly or mainly in the conveyance of signals on electronic communications networks. It must be noted that some provisions of the e-Privacy Directive, namely those referring to unsolicited communications and to the use of cookies, have been implemented through the Law on Information Society Services. Therefore, information society service providers, even those who are not electronic communication service providers, fall within the scope of those provisions.

### 5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The General Law on Telecommunications of 2014 applies to “operators”, which are defined as a natural or legal person who exploits public electronic communication networks or provides publicly available electronic communication services, and has notified to the Ministry of Industry, Energy and Tourism the start of its activity or is registered with the Register of Operators.

The Law on Information Society Services applies to the providers established in Spain and to the services they provide. The mere fact of using technological means located in Spain will not be a strong enough criterion in itself to determine that the provider is established in Spain. The Law
applies as well to the information society services from foreign providers which are provided through a permanent establishment located in Spain. For providers located in other Member States of the EU of the EEA, the Law follows the origin principle established in the Directive on Electronic Commerce, and sets forth a number of derogations from the coordinated field in accordance with Art. 3 of the Directive.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. Not available
   b. Not available

7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The distinction between electronic communication services and information society services may prove not clear enough in practice.

   b. A clearer definition of the scope of the rules, in particular with regards the so-called over-the-top applications and services.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The principle of confidentiality of communications and related traffic data (article 5.1 of the ePrivacy Directive) was implemented in Art. 33 of the General Law on Telecommunications of 2003, which was developed through the Royal Decree 424/2005 of 15 April, which approves the Regulation on the conditions for the provision of electronic communication services, the universal service and the protection of users. As noted above, the Law of 2003 has been recently repealed and substituted with the new General Law on Telecommunications of 2014.

Art. 39(1) of the current General Law on Telecommunications of 2014 establishes (in the same vein it was established in Art. 33 of the former Law of 2003) that operators exploiting public communication networks or providing publicly available electronic communications service must guarantee the secrecy of the communications in accordance to Articles 18(3) and 55(2) of the Constitution, and must adopt the needed technical measures to that effect.

The 2005 Regulation contains a definition of “communication”, in the following terms: “Any information which is interchanged or conducted between a finite number of interested persons by means of a publicly available electronic communications service. The present definition does not include information which, as part of a service of broadcasting to the public, is conducted through an electronic communications network, except to the extent that the information may be linked to the identifiable subscriber or user who receives the information.” Although the 2005 Regulation develops the now repealed Law of 2003, it is still in force – as long as it does not go against the Law of 2014 – until a new set of developing rules is approved. (See Transitory Disposition No 1 of the General Law on Telecommunications of 2014).

As a general matter, confidentiality of communications is enshrined in Article 18(3) of the Spanish Constitution, which also provides for the possibility of court orders for intercepting communications. Art. 18(3) states: “Secrecy of communications is guaranteed, particularly of postal, telegraphic and telephonic communications, except in the event of a court order to the contrary.” (source of the translation: http://www.tribunalconstitucional.es/es/constitucion/Paginas/ConstitucionIngles.aspx)

- Violations of the secrecy of communications are typified as criminal offences in the Spanish Penal Code. In particular, Art. 179 of the Penal Code reads as follows:

  “1. Whoever, in order to discover the secrets or to breach the privacy of another, without his consent, seizes his papers, letters, electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal, shall be punished with imprisonment of one to four years and a fine of twelve to twenty-four months.

  2. The same penalties shall be imposed upon whoever, without being authorised, seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telematic files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without being authorised,
accesses these by any means, and whoever alters or uses them to the detriment of the data subject or a third party.

3. Whoever, by any means or procedure and in breach of the security measures established to prevent it, obtains unauthorised access to computer data or programs within a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years.

When, pursuant to the terms established in Article 31 bis, a legal person is responsible for the offences included in this Article, the punishment of a fine from six months to two years shall be imposed thereon. Pursuant to the rules established in Article 66 bis, the Judges and Courts of Law may also impose the penalties established in Sub-Sections b) to g) of Section 7 of Article 33.

4. A sentence of imprisonment shall be imposed from two to five years if the data or facts discovered, or the images captured to which the preceding numbers refer, are broadcast, disclosed or ceded to third parties. Whoever, being aware of their unlawful origin and without having taken part in their discovery, perpetrates the conduct described in the preceding Section shall be punished with imprisonment from one to three years and a fine of twelve to twenty-four months.

5. Should the acts described in Sections 1 and 2 of this Article be perpetrated by persons in charge of or responsible for the files, computer, electronic or telematic media, archives or records, a sentence of imprisonment of three to five years shall be imposed on them, and if they disclose, communicate or reveal reserved data, the upper half shall be imposed.

6. Likewise, when the acts described in the preceding Sections concern personal data that reveal the ideology, religion, belief, health, racial origin or sexual preference, or when the victim is a minor or incapacitated, the penalties imposed shall be those foreseen in the upper half.

7. If the acts are perpetrated for profit-making purposes, the penalties shall be imposed as foreseen in Sections 1 to 4 respectively of this Article in the upper half. If they also affect the data mentioned in the preceding Section, the punishment to be imposed shall be that of imprisonment from four to seven years.

8. Should the acts described in the preceding Sections be committed within a criminal organisation or group, more severe penalties shall be applied respectively.”

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

This particular provision does not appear to have been specifically transposed into Spanish Law.

In practice, at the beginning of the communication businesses inform the user that the telephone conversation will be recorded for legal or security reasons. There have been no relevant problems with this practice, as it is assumed that the user is granting their consent. No complaints have been filed with the Data Protection Authority. The Data Protection Authority has sometimes acted in response to a petition of a user to make sure that the business gives that user access to the content of the communication.

3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.
Art. 55(2) of the Constitution provides for the possibility to limiting this right by means of an Organic Law in some particular cases related to the fight against terrorism.

In addition, the Criminal Procedural Law deals, in Arts. 579 and followings, with the situations where a court may authorize the interception of a communication (we are not dealing further with this matter in this report).

Art. 39(2) of the General Law on Telecommunications of 2014 establishes that operators are obliged to carry out the interceptions authorized in accordance to Art. 579 of the Criminal Procedural Law, to the Organic Law 2/2002 of 6 May regulating the National Centre of Intelligence, and to other organic laws. Subsequent paragraphs of Art. 39 deal with the way in which operators must fulfil this obligation.

More detailed provisions on how operators must proceed in the case of legal interception of communications can be found in Arts. 83 and followings of the Royal Decree 424/2005 of 15 April, which approves the Regulation on the conditions for the provision of electronic communication services, the universal service and the protection of users.

4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

   a. Traffic data is distinguished from the content of communications in the Law 25/2007 of 18 October, on the retention of data relative to electronic communication and public communication networks.

   b. See above the provisions of the Constitution and the Criminal Code, those in the General Law on Telecommunications of 2014, and the Royal Decree 424/2005 of 15 April, approving the Regulation on the conditions for the provision of electronic communication services, the universal service and the protection of users. In addition, with regards to personal data the legal framework regarding data protection will apply (Organic Law 15/1999 of 13 December, on protection of personal data, and Royal Decree 1720/2007 of 21 December, approving the regulation developing the Organic Law 15/1999 of 13 December, on the protection of personal data).

5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third
party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Article 5(3) of the e-Privacy Directive is implemented into Spanish Law by means of Art 22(2) of the Law on Information Society Services. After the 2009 amendment of the Directive, this article was modified accordingly through the Royal Decree Law 13/2012, of 30 March, transposing Directives with regards to internal markets of electricity and gas and to electronic communications, and adopting measures to correct deviations due to costs and revenue gaps in the sectors of electricity and gas. Finally, the General Law on Telecommunications of 2014 slightly changed the language of this provision with regards to the use of adequate settings of the browser or of other applications to express consent.

The current version of Art. 22(2) of the Law on Information Society Services sets forth:

“Service providers may utilize devices to store, and to gain access to, data in the terminal equipment of the recipients, provided that those recipients have granted their consent after having been given clear and comprehensive information about such utilization, in particular about the purposes of the processing of the data, in accordance to what is established in the Organic Law 15/1999 of 13 December, on protection of personal data.

Where it is technically feasible and effective, the recipient’s consent to accept the data processing may be granted by the use of the adequate settings of the browser or of other applications.

This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the recipient.”

It must be noted that the word “recipient” refers to the recipient of the information society service provided. According to the Law on Information Society Services, “recipient” means “a natural or legal person who uses, whether or not for professional purposes, an information society service”

On the other hand, the second paragraph of this provision (browser settings), which is not included in Art. 5(3) of the e-Privacy Directive, was taken from Recital 66 in the Preamble to the Directive 2009/136/EC.

This provision is directed to information society service providers. Several parties may be involved in the use of cookies – publisher, advertiser, advertising networks. The Guide issued by the Spanish Data Protection Authority in 2013 noted that the law does not precise who is the one responsible for complying with the duty to inform and gain the consent, and that all parties participating in the use of cookies should cooperate to fulfil the legal requirements. The new General Law on Telecommunications of 2014 has introduced a new paragraph Art. 37 of the Law on Information Society Services that deals specifically with the case of third party cookies. This paragraph establishes that in case of an infringement of the rules on cookies which is due to the fact that the information society service provider has reserved to a third party some spaces to show advertisements, not only the information society service provider but also the ad network or the ad agent will be liable if they had not adopted the measures to require the to the publisher the fulfilment of the legal duties of informing and obtaining the user’s consent.
b. The implementation does not refer to particular types of cookies, nor does it distinguish between different types of terminal equipment. Nonetheless, the Guide issued by the Spanish Data Protection Authority does refer to different types of cookies and notes that – but for cookies exempted from consent – any kind of cookie, whether session or persistent, first party or third party, falls within the scope of the provision. Regarding the equipment, the Guide assumes that any terminal equipment – such as a PC, cell phone or tablet – is included in the provision’s scope.

<table>
<thead>
<tr>
<th>6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?</th>
</tr>
</thead>
</table>
| Art 22(2) of the Law on Information Society Services, which implements Art. 5(3) of the e-Privacy Directive states that the consent must be granted in accordance to the Organic Law 15/1999 of 13 December, on protection of personal data. In addition, it also establishes that “[w]here it is technically feasible and effective, the recipient’s consent to accept the data processing may be granted by the use of the adequate settings of the browser or of other applications.”

Beyond this, the Law does not provide further clarification as to how the consent must be granted. Nonetheless, in 2013 the Spanish Data Protection Authority issued a public guide on how to comply with this provision. This document, titled “Guide on the use of cookies”, is available at [https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf)

The Guide suggests different ways of granting the consent, essentially following the criteria offered by the Article 29 Data Protection Working Party Opinions (Opinion 2/2010 on online behavioural advertising, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, and Opinion 04/2012 on Cookie Consent Exemption). The different options offered by Spanish Data Protection Authority Guide include that of presenting a notice informing that the site is using cookies, providing a link to more detailed information, and noting that certain action of the user, such as keeping on surfing the website, will be understood as consent. In this case, for instance, it may be understood that the consent has been granted once the user moves the scroll or clicks on any link on the page.

The Guide considers that cookies requiring consent may only be installed once the consent has been granted, thus not immediately when loading the page.

<table>
<thead>
<tr>
<th>7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Both exceptions have been implemented in Art 22(2), third paragraph of the Law on Information Society Services, almost verbatim. This paragraph states:

“This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provision of an information society service explicitly requested by the recipient.”

In addition, the Guide issued by the Spanish Data Protection Authority follows the criteria expressed by the Article 29 Data Protection Working Party in its Opinion 04/2012 on Cookie Consent Exemption. Hence, the Guide leaves aside the cookies which are, or in some cases may be, exempted from consent, namely “user-input” cookies, user authentication or identification cookies (only session cookies), user-centric security cookies, load balancing session cookies, user interface customization cookies, multimedia player session cookies and social plug-in content sharing cookies.

8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

It appears that the more common way of asking and obtaining the consent consist of a notice stating that the website is using cookies (sometimes expressing in general terms the ends of that usage, such as “to improve your surfing experience” and “to provide advertising which relevant to your interests”), along with a link to the cookie policy. The notice may actually offer the option of accepting or refusing cookies, or state that consent will be assumed if the user keeps on surfing the page. We are not aware of official statistics on compliance.

The Data Protection Authority has taken enforcement actions against a number of websites, and imposed fines according to the rules of the Law on Information Society Services.

9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law
a. On 1st April, 2013, the Spanish Data Protection Authority, issued a document titled “Guide on the use of cookies”, which is available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

The Guide was elaborated in close cooperation with the industry. It is not meant to offer a general and uniform solution on how to comply with the law. It rather seeks to provide some guidance so that entities may reflect the issue and make decisions according to their interests and their business model. The Guide covers (i) the scope of the provisions; (ii) terminology and definitions of the relevant elements (cookies, data, terminal equipment, information society service, web page, advertising space, advertising inventory) and the concerned parties (user, publisher, advertiser, advertising networks, etc); (iii) obligations of the parties (duty to inform, duty to obtain the consent); and (iv) parties’ responsibility on the use of cookies.

To a large extent, the guide follows the criteria put forward by the Article 29 Data Protection Working Group in its opinions.

It must be noted that the Spanish Data Protection Authority is the competent body for enforce the provisions regarding cookies, and thus this document provides very useful guidance on how to comply with the provision.

In addition, the Data Protection Authority has issued several legal reports in response of questions posed by interested parties. These legal reports provide guidance on the interpretation of the cookies provision. They are available at the following links:
- Report 2014-0196: Information in the second layer regarding cookies
- Report 2014-0011: The consent for the use of cookies. An opt-out system is not possible

b. As noted earlier, a number of infringement decisions have already been rendered by the Spanish Data Protection Authority. The decisions are available at the Authority’s website https://www.agpd.es.

10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

a. It is not obvious that users are actually making informed choices about the acceptance of cookies even if they happen to read the cookie policy. The fact of asking for users’ consent in the way is generally done probably does not add much to their privacy. It may be seen more as a formal obligation for webmasters than a strong protection for users.

b. A more general system of preventing websites and third parties from tracking users might better enhance their privacy protection.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic data is not expressly defined in the legislation implementing the e-Privacy Directive, namely, the Law 9/2014 on Telecommunications and the Law 34/2002 on Information Society Services and Electronic Commerce. Implicitly, traffic data may be understood as those other than the contents of the communication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects</th>
</tr>
</thead>
<tbody>
<tr>
<td>According to Art. 48(2)(a) and (b) of the General Law on Telecommunications of 2014, final users of electronic communication services will have the right:</td>
</tr>
<tr>
<td>“(a) That their traffic data is made anonymous or erased when it is no longer needed for the purpose of the transmission of a communication. Traffic data necessary for the purposes of subscribers billing and interconnection payments may be processed only up to the end of the period for the bill to be challenged, for the amount charged by the operator to be returned, for bill to be paid or for the payment to be pursued by the operator.</td>
</tr>
<tr>
<td>(b) That their data traffic are used for commercial promotion of electronic communication services or for the provision of value added services, inasmuch and for the time which is necessary for those services or commercial promotion, only where they have granted their informed consent to that end. Final users will have the right to withdraw their consent for the processing of traffic data at anytime and with immediate effects.”</td>
</tr>
<tr>
<td>According to Art. 48(4), this must be understood without prejudice to the obligations laid down in the Law 25/2007 of 18 October, on the retention of data relative to electronic communication and public communication networks</td>
</tr>
<tr>
<td>According to Art. 81(4) of the Royal Decree 1720/2007 of 21 December, approving the regulation developing the Organic Law 15/1999 of 13 December, on the protection of personal data, operators providing publicly available electronic communication services or exploiting public electronic communication networks, with regards to the file systems of traffic and location data they control, in addition to the security measures of basic and medium level must also fulfill the high level security measure consisting of a log of accesses. This particular measure is described in Art 103 of the Royal Decree.</td>
</tr>
</tbody>
</table>
### 3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Art. 48(2)(a) of the General Law on Telecommunications of 2014, establishes that final users of electronic communication services will have the right:

“(a) That their traffic data is made anonymous or erased when it is no longer needed for the purpose of the transmission of a communication. Traffic data necessary for the purposes of subscribers billing and interconnection payments may be processed only up to the end of the period for the bill to be challenged, for the amount charged by the operator to be returned, for bill to be paid or for the payment to be pursued by the operator.”

### 4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

We not aware of specific cases.

### 5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The rules seem to be reasonable to protect users’ privacy. In any event, the legal framework should be clarified with regards to the Law 25/2007 of 18 October, on the retention of data relative to electronic communication and public communication networks, which allows the retention of traffic data by operators. This Law implements the Data Retention Directive, which the Court of Justice of the European Unión has declared to be invalid. The Regulator considers the law to be valid in Spain and applicable to operators.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>The term “location data” is defined in the Annex II (9) of the General Law on Telecommunications of 2014 as:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service”</td>
</tr>
<tr>
<td>Hence, the definition provided by Art. 2(c) of the e-Privacy Directive has been implemented verbatim.</td>
</tr>
</tbody>
</table>

2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

<table>
<thead>
<tr>
<th>According to Art. 48(2)(c) of the General Law on Telecommunications of 2014, final users of electronic communication services will have the right:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“c) That their location data other than traffic data are processed only when they have been made anonymous or where final users have previously granted their informed consent and exclusively to the extent and for the duration necessary for the provision, where the case may be, of value added services, with unequivocal knowledge of the data that will be processed, the purposes and duration of the processing and of the value added service that will be provided. Final users will have the right to withdraw their consent for the processing of location data other than traffic data at anytime and with immediate effects.</td>
</tr>
<tr>
<td>Final users may not exercise this right when it comes to emergency calls through number 112 or communications made to entities providing urgency call services which are determined by the Ministry of Industry, Energy and Tourism.”</td>
</tr>
<tr>
<td>According to Art. 48(4), this must be understood without prejudice to the obligations laid down in the Law 25/2007 of 18 October, on the retention of data relative to electronic communication and public communication networks.</td>
</tr>
<tr>
<td>Art. 81(4) of the Royal Decree 1720/2007 of 21 December, approving the regulation developing the Organic Law 15/1999 of 13 December, on the protection of personal data, operators providing publicly available electronic communication services or exploiting public electronic communication networks, with regards to the file systems of traffic and location data they control, in addition to the security measures of basic and medium level, must also fulfill the security measure of high level consisting of a log of accesses. This particular measure is described in Art 103 of the Royal Decree.</td>
</tr>
</tbody>
</table>
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

According to Art. 48(2)(c) of the General Law on Telecommunications of 2014, final users of electronic communication services will have the right:

“c) That their location data other than traffic data are processed only when they have been made anonymous or where final users have previously granted their informed consent and exclusively to the extent and for the duration necessary for the provision, where the case may be, of value added services, with unequivocal knowledge of the data that will be processed, the purposes and duration of the processing and of the value added service that will be provided. Final users will have the right to withdraw their consent for the processing of location data other than traffic data at anytime and with immediate effects.

Final users may not exercise this right when it comes to emergency calls through number 112 or communications made to entities providing urgency call services which are determined by the Ministry of Industry, Energy and Tourism.”

4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. The Spanish Data Protection Authority issued a Guide on Data Security, which is available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guías/GUIASEGURIDAD_2010.pdf

   The Observatory of Information Security, at the National Institute of Telecommunication Technologies (INTECO), an entity ascribed to the Ministry of Industry, Energy and Tourism, issued a “Guide to security and privacy of geolocation tools”. It is available in English at http://www.inteco.es/CERT_en/publications/guides/Guia_Geolocalizacion_EN

   b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)

5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The rules seem to be reasonable to protect users’ privacy. In any event, the legal framework should be clarified with regards to the Law 25/2007 of 18 October, on the retention of data relative to
electronic communication and public communication networks. This Law implements the Data Retention Directive, which the Court of Justice of the European Unión has been declared to be invalid.
### E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. 
   - Article 48(1) of the General Law on Telecommunications of 2014 provides that final users of electronic communication services have the right to: “(a) not to receive automatic callings without human intervention or fax messages for the purposes of commercial communication without having granted their prior and informed consent to that end; (b) to oppose receiving unwanted callings for purposes of commercial communication made by systems other than those indicated above, and to be informed about this right.”

   - The Law on Information Society Services deals generally with electronic commercial communications. These are the relevant provisions:

     “Art. 20. Information required about commercial communications, promotional offers and contests.

     1. Commercial communications made by electronic means must be clearly identifiable as such. The natural or legal person on whose behalf they are made must also be clearly identifiable.

     (...)

     4. In any event, it is prohibited the sending of commercial communications which disguise or conceal the identity of the sender on whose behalf the communication is made, or that contravene this Article, as well as those inducing the recipients to visit Internet pages which contravene this Article.”

   “Art. 21. Prohibition of commercial communications carried out by electronic mail or by equivalent means of electronic communication.

   1. It is prohibited the sending of advertising or promotional communications by electronic mail or other equivalent means of electronic communication which have not been previously solicited or expressly authorized by their recipients.

   2. The previous paragraph will not apply where a prior contractual relationship exists, provided that the provider has lawfully obtained the recipient’s contact details and uses them to send commercial communications related to products or services of its own company which are similar to those which initially were the subject of contract with the customer.

   In any event, the provider must give the recipient the opportunity to object to the processing of his or her details for promotional purposes by means of an easy and free of charge procedure, both at the time of their collection and on the occasion of each commercial communication it sends to the recipient.

   Where the communications are sent by electronic mail that procedure must necessarily consist of
including an electronic mail address or another valid electronic address where that right may be exercised. Communications not including such an address are prohibited.”

“Art. 22. Rights of the recipients of the services.

1. The recipient may withdraw at anytime the consent granted to receive commercial communication simply by notifying such will to the sender.

To that effect, service providers must provide for easy and free of charge procedures so that recipients may revoke the consent they had granted. Where the communications are sent by electronic mail that procedure must necessarily consist of including an electronic mail address or another valid electronic address where that right may be exercised. Communications not including such an address are prohibited.

Service providers must provide electronically accessible information about those procedures.”

In addition to these rules, Art. 19 of the Law on Information Society Services states that the specific legislation in the field of commercial activity and advertising will also apply, as well as the legislation on data protection, particularly the Organic Law 15/1999 of 13 December on Protection of Personal Data and the secondary rules developing it.

The Annex of the Law on Information Society Services defines “commercial communication” as follows:

(f) “Commercial communication“: Any form of communication directed to the promotion, direct or indirect, of the image or the goods or services of a company, organization or person developing a commercial, industrial, artisanal or professional activity. For the effects of this Law, it will not be considered a commercial communication the data that allow accessing directly the activity of a person, company or organization, such as the domain name or the electronic mail address, nor the communications regarding the goods or services or to the image offered when they are elaborated by a third party and without economic remuneration”

b. The implementation is made through to different instruments, with a different scope, namely the General Telecommunications Act, and the Law on Information Society Services. Communications by electronic mail and other equivalent means are regulated under the Law on Information Society Services, the scope of which is wider, as it encompasses all information society services providers and thus is not limited to those who provide services consisting wholly or mainly in the conveyance of signals on electronic communications networks.

In addition, the material scope of the transposition may be wider as the law refers not only to electronic mail but also to “other equivalent means of electronic communication”

Moreover, the rules on unsolicited commercial communications are not limited to the cases where the recipient is a natural person, unlike in Art. 13(5) of the Directive. This has been expressly confirmed both by the Data Protection Authority (the body responsible for enforcing these provisions and issuing infringement decisions) and by the Audiencia Nacional (the court to which the Data Protection Authority decisions may be appealed). See for instance, the judgment rendered by the Audiencia Nacional on 17 September 2008.
The implementation presents some are other minor differences in the language. For instance, when it comes to the exception set forth in Art. 13(2), the last part of the last sentence (“in case the customer has not initially refused such use.”) is omitted. Arguably, however, the outcome is not different, as the provider must have given the recipient the opportunity to object to the processing at the time of their collection. On a side point, the omission of those final words was probably caused because they did not appear either in the Spanish version of the Directive.

2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

As a general rule, the sending of unsolicited messages via electronic mail or other equivalent means of electronic communication is only allowed if it has been previously solicited or expressly authorized by their recipients. The recipient may withdraw at anytime the consent granted to receive commercial communication simply by notifying such will to the sender.

As an exception to the general rule, the requirement prior consent does not apply in the case that a prior contractual relationship exist, provided that the provider has lawfully obtained the recipient’s contact details and uses them to send commercial communications related to products or services of its own company which are similar to those which initially were the subject of contract with the customer.

The provider must give the recipient the opportunity to object to the processing of his or her details for promotional purposes by means of an easy and free of charge procedure, both at the time of their collection and on the occasion of each commercial communication it sends to the recipient. Where the communications are sent by electronic mail that procedure must necessarily consist of including an electronic mail address or another valid electronic address where that right may be exercised. Communications not including such an address are prohibited. It is required that service providers provide electronically accessible information about those procedures.

Commercial communications must be clearly identifiable as such. The natural or legal person on whose behalf they are made must also be clearly identifiable. The sending of commercial communications which disguise or conceal the identity of the sender on whose behalf the communication is made is prohibited.

Obviously, the legal framework regarding personal data protection applies. In this regard, for instance, the Royal Decree 1720/2007 of 21 December, approving the regulation developing the Organic Law 15/1999 of 13 December, on the protection of personal data, deals with the file systems containing the data of those who have expressed their opposition to receive advertising (exclusion lists) (see Art. 48 and followings). The Spanish Association of the Digital Economy maintains an exclusion list for telephone calls, mail, e-mail, sms, mms and other equivalent electronic communications. See https://www.listarobinson.es/

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

a. The implementation does provide the exception set forth in Art. 13(2) of the e-Privacy Directive.
According to Art. 21(2) of the Law on Information Society Services, the previous consent or express authorization from the recipient is not required where
(a) a prior contractual relationship exists, and
(b) the provider has lawfully obtained the recipient’s contact details, and
(c) uses them to send commercial communications related to products or services of its own company which are similar to those which initially were the subject of contract with the customer.

The law requires, that “in any event, the provider must give the recipient the opportunity to object to the processing of his or her details for promotional purposes by means of an easy and free of charge procedure, both at the time of their collection and on the occasion of each commercial communication it sends to the recipient.”

b. The Spanish implementation does distinguish whether the recipient is a natural or a legal person. Therefore, it does not implement the exception for legal persons set forth in Art. 13(5) of the e-Privacy Directive.

4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Law on Information Society Services implements the rules on commercial communications without distinguishing between different channels. In fact, it refers generally to communications made “by electronic mail or other equivalent means of electronic communication”, and subjects all of them to the same requirements.

Regarding particularly the premium-rate services via SMS and MMS, a specific binding code of conduct exists (Resolution of 8 July 2009, of the Secretary of State for Telecommunications and Information Society publishing the code of conduct for the provision of premium-rate services based on the sending of messages, available at http://www.boe.es/buscar/doc.php?id=BOE-A-2009-12439). The Code explicitly forbids the sending of unsolicited commercial communications – See Art. 5(1)(3).

5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. A number of infringement decisions have already been rendered by the Spanish Data Protection
Authority. The decisions are available at the Authority’s website https://www.agpd.es.

As noted above, according to Art. 19 of the Law on Information Society Services, commercial communications must fulfil the conditions set forth in the Organic Law on Personal Data Protection (LOPD) and the secondary legislation developing it. Thus, the Data Protection Authority concludes that where personal data are involved, the consent required to send commercial communications must be an informed consent (See Art. 3(h) LOPD). In particular, Art. 45(1)(b) of the Royal Decree 1720/2007, of 21 December, which develops the LOPD, establishes that the data subject must have been informed about the specific sectors and activities in respect of which he or she will receive commercial communications.


b. The Audiencia Nacional (the court before which the infringement decisions issued by the Data Protection Authority may be appealed) has confirmed that the rules on commercial communications apply as well where the recipient is a legal person. See for instance the judgment rendered by the Audiencia Nacional on 17 September 2008.

6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

While the threat of fines is an obvious deterrence from sending unsolicited messages, the volume of spam appears to be very high and thus the norm fails to provide an adequate protection.
COUNTRY REPORT

Finland

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

Date: 15.8.2014
Contents

Part 1: Management summary................................................................. 3
Part 2: Answers to the questionnaire....................................................... 4
Part 1: Management summary

- Generally speaking, the Finnish “Act on the Protection of Privacy in Electronic Communications” offers adequate tools for protecting user rights. However, there’s a significant problem regarding the resources of the administrate organizations, which makes the enforcement side rather weak. Both the Finnish Communication Regulatory Authority (FICORA) and the Data Protection Ombudsman are very hesitant to do anything other than give advice to violating parties.

- The Finnish current transposition is much more detailed than the directive, especially the rules regarding traffic data and commercial communication, which use the leeway left by the directive to the full extent. On the other hand, The Finnish approach to cookies is relatively lax i.e. it’s not seen as a priority in protecting user privacy.

- There’s a bigger legislative process to create one single law (the “Information Society Act”), which would bring the current separate laws under one title. However, its exact content is still very much open so the effects remain to be seen only later after the Finnish parliament has finalized the process.

- The international scope of the directive and its national implementation is a very hard problem to solve. A partial solution could be changing the ePrivacy directive to a Regulation similarly as has been tried with the data protection directive.

- The Finnish approach to use strict opt-In for spam is has been successful in limiting Finnish spamming. However, it does not help against foreign actors.
Part 2: Answers to the questionnaire
Implementing legislation: identification of the laws and their scope

Directive 2002/58/EC has been transposed into Finnish legislation by the Act on the Protection of Privacy in Electronic Communications (516/2004). The law was amended in 2011 (365/2011) to add the new rules regarding cookies etc. There are also general rules regarding marketing in Consumer Protection Act (29/2005) and specific rules regarding email communication in Act on the Protection of Privacy in Working Life (759/2004). The Constitution of Finland also protects confidential communications.

<table>
<thead>
<tr>
<th>Concordance table</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePrivacy Directive</td>
</tr>
<tr>
<td>Art. 2 (Definitions)</td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
</tr>
<tr>
<td>Art. 6 (Traffic data)</td>
</tr>
</tbody>
</table>

URLs:

### Art. 9 (Other location data)

Act on the Protection of Privacy in Electronic Communications, sections 9-12


### Art. 13 (Unsolicited communications)

Act on the Protection of Privacy in Electronic Communications, sections 16-18


### Full name of the authority

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tietosuojavaltuutetun toimisto- Data Protection Ombudsman</td>
<td>Data Protection Ombudsman</td>
<td>1) corporate or association subscribers’ processing of identification data referred to in sections 13a–13k; 2) the processing of location data referred to in Chapter 4; 3) compliance with the provisions on telephone directories and other subscriber directories, and on directory inquiries, as referred to in section 25; 4) compliance with the provisions on direct marketing in Chapter 7; 5) compliance with the provisions in Chapter 9 on right of</td>
<td><a href="http://www.tietosuojatietoavustaja.fi/en/index.html">http://www.tietosuojatietoavustaja.fi/en/index.html</a></td>
</tr>
<tr>
<td>Supervision Authority</td>
<td>Function/Supervision</td>
<td>Website</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>

**Explanation:**

- In Finland the Ministry of Communication is in charge of transposing the ePrivacy Directive which has been inserted into the Finnish Act on the Protection of Privacy in Electronic Communications.
- The supervision authority has been divided between the Finnish Data Protection Ombudsman’s office and the Finnish Communication Regulatory Authority.
- Also the Finnish Competition and Consumer Authority supervises where there’s connection to marketing.
- In practice the supervision of the legislation is quite flexible and there’s very close co-operation between the Ombudsman and FICORA. There’s also close coordination with Finnish Competition and Consumer Authority and Ombudsman. There’s currently no “turf battles”.


3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The Act on the Protection of Privacy in Electronic Communications, section 2 has the following definitions for networks:

2) communications network means a system comprising cables and equipment joined to each other for the purpose of transmitting or distributing messages by wire, radio waves, optically or by other electromagnetic means;

3) public communications network means a communications network available to a set of users that is not subject to any prior restriction

However, it excludes private networks:

(2) This Act does not apply to internal communications networks and other communications networks accessible to a restricted set of users, unless such networks are connected to a public communications network referred to in subsection 1.

(3) Notwithstanding the above, sections 4 and 5 of this Act apply to internal communications networks and other communications networks accessible to a restricted set of users, even if such networks are not connected to a public communications network referred to in subsection 1.

There’s also a limitation regarding public broadcast, which is in line with the Art 2.(d):

(6) This Act does not apply to messages transmitted over a mass communications network if the message cannot be associated with an individual case of a subscriber or user receiving it.

In addition, the networks used specifically by the public authorities (police, defence forces etc.) are excluded, which is in line with the Article 1.3 of the Directive:

(7) This Act does not apply to the actions of public authorities in public authority networks as defined in the Communications Market Act or in any other communications network built for the needs of public order and security, national defence, rescue operations, civil defence or the safety of land, sea, rail or air transport.

The definitions for services are the following:

5) network service means the provision of a communications network by a telecommunications operator for the purposes of transmitting, distributing or
providing messages to a set of users that is not subject to any prior restriction;

6) communications service means the transmission, distribution or provision of messages by a telecommunications operator in a communications network to a set of users that is not subject to any prior restriction;

7) value added service means a service based on the processing of identification data or location data for a purpose other than the provision of a network service or communications service;
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

If VoIP and webmail are offered to the general public, the Finnish law covers them (as “network services” and “communications networks”). However, regarding location the matter is more complicated. There has to be some kind of communication element attached to the service i.e. it has to fall into one of these categories: “network services, communications services, value added services and services where data describing the use of the service is processed, which are provided in public communications networks.”
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The territorial scope is not defined in the Finnish law and this is seen as one of its biggest problems. There’s currently a new law proposal in the Finnish parliament, which may add this definition but its exact content is still totally open. The original proposal from the Government would extend the scope to any services offered in Finnish or to Finnish citizens i.e. also foreign services would fall in the scope of the law. However, there’s been significant lobbying against the text and it’s very likely to change in the process.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. Currently there’s only the guidance from FICORA, which has short definitions for e-mail, push e-mail, VoIP exchange, instant messaging services and Internet access services: https://www.viestintavirasto.fi/en/steeringandsupervision/regulatoryobjectives/interpretationguidelinesontelecommunicationsandtelecomsoperators/examplesofservices.html

b. There’s no such cases that we are aware of.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The system works relatively well in Finland and the situation should get even better after the current law reform is accepted in the Finnish parliament that combines E-Privacy and E-Commerce Directive into one law. The biggest problem is that both agencies in charge of monitoring the compliance of the law are rather under-resourced so they are mostly reacting to the complaints and not acting ex officio to start cases.

b. It would make sense also at EU level to combine the E-Privacy and E-Commerce Directives into one coherent directive.
A. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The Finnish Constitution (Art. 10.2) protects confidential communication:

“The secrecy of correspondence, telephony and other confidential communications is inviolable”

However, Art 10.3. makes it possible to limit this right in the context of crime:

Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.

The strongest protection to confidentiality of communications comes from the criminal law, which criminalizes the breach of confidentiality. In Act on the Protection of Privacy in Electronic Communications Section 4 defines the confidentiality:

Section 4 - Confidentiality of messages, identification data and location data

(1) All messages, identification data and location data are confidential unless this Act or another Act provides otherwise.

(2) When a message has been transmitted to be universally received, it is not confidential. The identification data associated with such a message is, however, confidential. Provisions on disclosing identification data of a network message are laid down in section 17 of the Act on the Exercise of Freedom of Expression in Mass Media (460/2003).

(3) Subsection 1 above also applies to identification data generated through the browsing of websites.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

In Finland the Art 5.2. is transposed in Act on the Protection of Privacy in Electronic Communications Section 10 - Processing for billing purposes.

It gives rather wide ranging right to use identification data as long as the subscribers are informed:

“(6) Telecommunications operators and value added service providers must inform subscribers or users about what identification data is being processed and how long the processing will last.”

There’s a minimum (3 months) and maximum time (the time until the debt becomes statute-barred under the Act on statute-barred debt).
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

There’s a wide ranging list of exceptions in law in the Chapter 3 of the Act on the Protection of Privacy in Electronic Communications. The exceptions are limited by the Section 8.3:

“Processing as referred to in the sections below is only allowed to the extent necessary for the purpose of such processing, and it may not limit the confidentiality of messages or the protection of privacy any more than is necessary. Identification data may only be disclosed to those parties entitled to process it in the given situation. After processing, messages and identification data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law.”

The exceptions are:

- Section 9 (125/2009) - Processing identification data for the purpose of providing and using services
- Section 10 - Processing for billing purposes
- Section 11 - Processing for marketing purposes (requires consent)
- Section 12 (125/2009) - Processing for the purposes of technical development
- Section 12 a (125/2009) - Processing for the purposes of statistical analysis
- Section 13 (125/2009) - A telecommunications operator’s and value added service provider’s right to process data in cases of misuse
- Section 13a (125/2009) - A corporate or association subscriber’s right to process data in cases of misuse (“Lex Nokia”)
- Section 13d (125/2009) - A corporate or association subscriber’s right to process data for investigating unauthorised use of information society service. (“Lex Nokia”)
- Section 13e (125/2009) - A corporate or association subscriber’s right to process data for investigating disclosures of business secrets communications network or communications service. (“Lex Nokia”)

- Section 14 (125/2009) - Processing for the purpose of detecting a technical fault or error

- Section 14a (343/2008) - Obligation to store data for the purposes of the authorities
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Finnish legislation doesn’t explicitly address “automated breaches of confidentiality without human intervention” but the general rules apply to both interception of MAC addresses and capturing Wi-Fi traffic.

b. The criminal law forbids any unlawful breach of confidentiality of communication.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. The scope and substance of your national implementation

b. Whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. The Section 7 transposes the art 5.3.:

“Section 7 (365/2011) - Saving data on the use of a service in the user’s terminal device and the use of such data

(1) The service provider may save cookies or other data concerning the use of the service in the user’s terminal device, and use such data, if the user has given his or her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data.

(2) Provisions of subsection 1 above do not apply to any saving or use of data which is intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider for the purpose of providing a service that the subscriber or user has specifically requested.

(3) The saving and use of data referred to above in this section is allowed only to the extent required for the service, and it may not limit the protection or privacy any more than is necessary.”

There’s also little additional guidance from FICORAI, whose key message is: “In Finland, the Directive on privacy in electronic communications has been interpreted so that users can give their consent to storing cookies for example through the settings of a browser or some other application.”


b.

No, the general rule applies to all kinds of cookies.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

As described in FICORA’s guidance above, in Finland the user can give consent in the settings of the browser. That’s also technology neutral. As a consequence it’s very rare that a Finnish website asks permission for setting cookies.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The exceptions are implemented in aforementioned Sec 7.2., which does not treat cookies differently based on their type.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

This matter has not been very controversial in Finland i.e. as long as the sites do not try to circumvent the browser settings, there’s consent from the user. There’s no official statistics on this issue but none of the major websites currently ask for permission from Finnish users.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. FICORA has given this aforementioned guidance:

b. There’s no court cases we are aware of.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The Finnish approach is quite practical. However, the progress in super cookies etc. may challenge the situation. However, here the easiest solutions are technical, not legal.

b. The best solution is to offer consumer a clear choice in the browser for different kind of cookies. The web sites should be required to follow these requirements. It does not make sense to individually ask on every web site for the consent, because that’s huge waste of time.
B. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Act on the Protection of Privacy in Electronic Communications defines traffic data as the following (section 2):

8) identification data means data which can be associated with a subscriber or user and which is processed in communications networks for the purposes of transmitting, distributing or providing messages;
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

The Act on the Protection of Privacy in Electronic Communications has a wide ranging list of exceptions, which allow the use of traffic data in law in the Chapter 3. The exceptions are:

- Section 9 (125/2009) - Processing identification data for the purpose of providing and using services

- Section 10 - Processing for billing purposes

- Section 11 - Processing for marketing purposes (requires consent)

- Section 12 (125/2009) - Processing for the purposes of technical development

- Section 12 a (125/2009) - Processing for the purposes of statistical analysis

- Section 13 (125/2009) - A telecommunications operator’s and value added service provider’s right to process data in cases of misuse

- Section 13a (125/2009) - A corporate or association subscriber’s right to process data in cases of misuse (“Lex Nokia”)

- Section 13d (125/2009) - A corporate or association subscriber’s right to process data for investigating unauthorised use of information society service. (“Lex Nokia”)

- Section 13e (125/2009) - A corporate or association subscriber’s right to process data for investigating disclosures of business secrets communications network or communications service. (“Lex Nokia”)

- Section 14 (125/2009) - Processing for the purpose of detecting a technical fault or error

- Section 14a (343/2008) - Obligation to store data for the purposes of the authorities
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Yes – in Sec 8.3 of the Act on the Protection of Privacy in Electronic Communications:

“Processing as referred to in sections below is only allowed to the extent necessary for the purpose of such processing, and it may not limit the confidentiality of messages or the protection of privacy any more than is necessary. Identification data may only be disclosed to those parties entitled to process it in the given situation. After processing, messages and identification data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

No.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Finnish approach with wide range of exceptions offers quite weak protection to the users. Especially the “Lex Nokia”-additions are theoretically quite worrisome. However, at the practical level the use of traffic data has been quite conservative. A stronger legal protection for traffic data should be still required because in reality it’s actually a bigger threat to user’s privacy than the actual content of the communication (it’s much cheaper and faster to use in automated processes to data mine information regard the users).
C. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Act on the Protection of Privacy in Electronic Communications has the definition in Section 2.:

“9) location data means data which shows the geographic location of a subscriber connection or terminal device and which is used for a purpose other than the provision of a network service or communications service;”

As can been seen, there’s additional second part in the definition, which is not in the directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

The Chapter 4 of Act on the Protection of Privacy in Electronic Communications defines the use of location data:

Chapter 4 - Location data

Section 16 - Processing and disclosure of location data

. (1) Telecommunications operators, value added service providers and corporate or association subscribers and any persons acting on their behalf may process location data subject to the provisions of this Chapter for the purpose of providing and using value added services. However, the provisions of this Chapter do not, unless otherwise provided by law, apply to location data rendered such that it cannot, in itself or in combination with other data, be associated with a specific subscriber or user.

. (2) Processing of location data shall be restricted to persons employed by or acting on behalf of the telecommunications operator, value added service provider or corporate or association subscriber whose job involves the processing of location data for the purpose of carrying out measures referred to in this Chapter.

. (3) Such processing is allowed only to the extent required for the purpose of the processing, and it shall not limit the protection of privacy any more than is necessary. After processing, the location data shall, unless otherwise provided by law, be destroyed or rendered such that it cannot be associated with a specific subscriber or user.

. (4) The prohibiting of the processing of location data and the service-specific consent referred to in this Chapter are decided in the case of minors under the age of 15 by their guardian under section 4 of the Child Custody and Right of Access Act (361/1983), and in the case of legally incompetent persons other than minors by their guardian under the Guardianship Services Act (442/1999), unless this is impossible by virtue of the technical nature of the service.

Section 17 - Subscriber’s right to prohibit processing of location data

. (1) A telecommunications operator may process location data if the subscriber has not forbidden it.
(2) The telecommunications operator shall ensure that the subscriber can easily and at no separate charge prohibit processing of location data, unless otherwise provided by law.

(3) The telecommunications operator shall ensure that the subscriber has easy and continuous access to information on the precision of the location data processed, the purpose of the processing and whether location data can be disclosed to a third party for the purpose of providing value added services.

(4) Before disclosing location data to a value added service provider or corporate or association subscriber, the telecommunications operator shall take appropriate steps to ensure that the provision of such a value added service is based on the consent referred to in section 18(1).

Section 18 - Service-specific consent of the party to be located

(1) The value added service provider or the corporate or association subscriber shall request service-specific consent from the party to be located before beginning the processing of location data, unless such consent is unambiguously implied from the context or unless otherwise provided by law.

(2) The party to be located shall have the opportunity easily and at no separate charge to cancel the consent referred to in subsection 1, unless otherwise provided by law.

(3) The value added service provider or corporate or association subscriber shall ensure that the party to be located has easy and continuous access to information on the precision of the location data processed, on the exact purpose and duration of the processing and on whether the location data may be disclosed to a third party for the purpose of providing a value added service. The value added service provider or corporate or association subscriber shall particularly ensure that this information is available to the party to be located before giving the consent referred to in subsection 1.

As can be seen from the sec 17. Above, a clear and continuous consent is required for the third parties to get the data.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

The aforementioned Sec. 16.3 of the Act on the Protection of Privacy in Electronic Communications:

“(3) Such processing is allowed only to the extent required for the purpose of the processing, and it shall not limit the protection of privacy any more than is necessary. After processing, the location data shall, unless otherwise provided by law, be destroyed or rendered such that it cannot be associated with a specific subscriber or user.”
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. There’s currently no general guidance.

b. There’s currently no case law we are aware of.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The Finnish law is quite well defined. Again, here the best solution is technical i.e. the users should be given an easy way to see and prevent the release of the location information from their device.
D. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

a. Chapter 7 of in Act on the Protection of Privacy in Electronic Communications deals with direct marketing:

Chapter 7 - Direct marketing

Section 26 - Direct marketing to natural persons

1. (1) Direct marketing by means of automated calling systems, facsimile machines, or e-mail, text, voice, sound or image messages may only be directed at natural persons who have given their prior consent.

2. (2) Direct marketing other than that referred to in subsection 1 to a natural person is allowed if the person has not specifically prohibited it. A natural person must be able easily and at no charge to prohibit direct marketing as referred to in this subsection.

3. (3) Notwithstanding subsection 1, where a service provider or a product seller obtains from any customer who is a natural person his contact information for e-mail, text, voice, sound or image messages in the context of the sale of a product or service, that service provider or product seller may use this contact information for direct marketing of his or her own products of the same product group and of other similar products or services. The service provider or product seller shall allow any customer who is a natural person the opportunity to prohibit, easily and at no charge, the use of contact information at the time when it is collected and in connection with any e-mail, text, voice, sound or image message. The service provider or product seller shall notify the customer clearly of the possibility of such a prohibition.
Section 27 - Direct marketing to legal persons

. (1) Direct marketing to legal persons is allowed if the recipient has not specifically prohibited it.

. (2) Any legal person shall be allowed the opportunity to prohibit, easily and at no separate charge, the use of its contact information in connection with any e-mail, SMS, voice, sound or image message sent in direct marketing. The party undertaking direct marketing shall give clear notification of the possibility of such a prohibition.

Section 28 - Identification of direct marketing

. (1) The recipient of an e-mail, text, voice, sound or image message sent for the purpose of direct marketing as referred to in sections 26 and 27 above shall be able to recognize such a message as marketing clearly and unambiguously.

. (2) It is prohibited to send such an e-mail, text, voice, sound or image message intended for direct marketing that 1) disguises or conceals the identity of the sender on whose behalf the communication is made; 2) is without a valid address to which the recipient may send a request that such communications be ended; 3) solicits recipients to visit websites that contravene Chapter 2 of the Consumer Protection Act (38/1978). (365/2011)

Section 29 - Preventing the reception of direct marketing

Telecommunications operators and corporate or association subscribers are entitled, at a user’s request, to prevent the reception of direct marketing as referred to in sections 26–28. Such measures must be undertaken with care, and they must not restrict freedom of speech or limit the confidentiality of messages or the protection of privacy any more than is necessary.

b. As can be seen from the above, the Finnish implementation is more detailed than the Directive. The content of the law is still totally in the line of the Directive. Sec. 29 is something that the Directive does not directly address i.e. what kind of technical measures ISPs can take to filter out spam.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Consent from the user is required for natural persons, or the subscriber must not have prohibited it for legal persons. In the case of existing business relationships, there must be a way to prohibit, easily and at no charge, the use of contact information for marketing communications. The sender and the nature of the communication has to be clear and unambiguous. The definition is somewhat more detailed but still in line with the directive.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

The Sec. 26.3. regulates the matter for natural persons:

   (3) Notwithstanding subsection 1, where a service provider or a product seller obtains from any customer who is a natural person his contact information for e-mail, text, voice, sound or image messages in the context of the sale of a product or service, that service provider or product seller may use this contact information for direct marketing of his or her own products of the same product group and of other similar products or services. The service provider or product seller shall allow any customer who is a natural person the opportunity to prohibit, easily and at no charge, the use of contact information at the time when it is collected and in connection with any e-mail, text, voice, sound or image message. The service provider or product seller shall notify the customer clearly of the possibility of such a prohibition.

For the legal entities, opt-out is the main rule (Sec 27) but there has to be an easy way to do it.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

As seen above in sec 26.1., the language of the law does not differentiate between the formats used to communicate.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It explains why sometimes the user has to opt-out for marketing and how opt-in is supposed to work. The document has also a concise definition for spam (“all unwanted email sent to a certain recipient”)</td>
</tr>
<tr>
<td></td>
<td>b. There is no jurisprudence on the application of the rules with regard to unsolicited direct marketing communications.</td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The law is very effective in curbing Finnish spam. Unfortunately it does not help at all against foreign actors, which send most of the spam coming to Finnish persons. The problem has been lately aggravated by the affiliate companies claiming to offer valid marketing tools without really having mailing lists of consenting users.
COUNTRY REPORT

FRANCE

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Fanny Coudert, Time.lex

Date: 18 September 2014
Contents

Part 1: Management summary

Part 2: Answers to the questionnaire
Management Summary for France

The transposition of the ePrivacy Directive into French law can be summarized as follows:

- France transposed most of the provisions in the Postal and Electronic Communications Code, of which the scope is largely determined by the term “operator”. The provision relating to unsolicited communications has been reproduced into the Consumer Law Code, extending its scope of application. In addition, the French privacy Commission has clarified the application of the provisions of the Data Protection Act to unsolicited communications. Finally, provisions relating to cookies have been transposed into the Data Protection Act, but it also applies to cookies that do not contain personal data.

- Art. 5.3 of the Directive (about cookies, etc.) has been more or less literally transposed into French law. France has taken the option of an opt-in approach. The CNIL has recently published guidelines to guide its interpretation, clarifying the multiple questions linked to the implementation of the provision.

- France has developed more precise rules on traffic and location data than those contained in the ePrivacy Directive, making use of the margin left to the Member States in this respect. There is no information available about whether or not the rules are applied in practice, and this aspect seems left to the sole responsibility of the “operators”. As far as the processing of location data is concerned, the French Privacy Commission issued opinions on automated vehicle location via GPS, carried out in the context of an employment relationship and in the car insurance sector, and on the collection of location data through Wi-Fi hotspots.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into French law into the Postal and Electronic Communications Code. The French Privacy Commission has however been granted competence for supervision of infringement of these provisions whenever they also breach the provisions of the Data Protection Act. Competent public authorities (Privacy Commission, DG for the protection of consumers, law enforcement authorities) and operators have created a platform – Signal Spam - to ease the fight against spam and the reporting of unsolicited communications by users.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC has been transposed into French legislation by the Act n° 2004-575 of 21 June 2004 for trust in the digital economy. This law modifies the Postal and Electronic Communications Code, the Data Protection Act and the Consumer Code introducing various provisions regarding electronic communications.
- Following the 2009 amendments of the European Regulatory Framework for Electronic Communications, the French legislator amended its legal framework by an Ordinance of 24 August 2011 which modifies the relevant provisions of the Postal and Electronic Communications Code, the French data Protection Act and the Consumer Code.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
**Communications Code**

**Art. 5.1 (Confidentiality)**
Art. L.32-1-II.5 Postal and Electronic Communications Code

http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=3FC912619C986AA4495B88AB4D8981FF8.tpdjo03v_2?idArticle=LEGIARTI000028345210&cidTexte=LEGITEXT000006070987&dateTexte=20140911&categorieLien=id&oldAction=rechCodeArticle&nbResultRech=1

**Art. 5.2 (Business exception)**
Art. L34-1-IV Postal and Electronic Communications Code

http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=23CB346C51E08FC36C767C323143138E.tpdjo03v_2?idArticle=LEGIARTI000006465728&cidTexte=LEGITEXT000006070987&dateTexte=20140905&categorieLien=id#LEGIARTI000024506066

**Art. 5.3 (Cookies)**
Art. 32-II Data Protection Act (Act n°78-17 of 6 January 1978 on Information technology data files and civil liberties)

http://legifrance.gouv.fr/affichTexteArticle.do;jsessionid=23CB346C51E08FC36C767C323143138E.tpdjo03v_2?idTexte=JORFTEXT000000886460&idArticle=LEGIARTI000024506226&dateTexte=20140905&categorieLien=id#LEGIARTI000006465728

**Art. 6 (Traffic data)**
Art. L34-1 Postal and Electronic Communications Code

http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=23CB346C51E08FC36C767C323143138E.tpdjo03v_2?idTexte=JORFTEXT000000886460&idArticle=LEGIARTI000024506226&dateTexte=20140905&categorieLien=id#LEGIARTI000006465728
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

<table>
<thead>
<tr>
<th>Art. 9 (Other location data)</th>
<th>Art. L34-1 Postal and Electronic Communications Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. L121-20-5 Consumer Law Code</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Art. 13 (Unsolicited communications)</th>
<th>Art. L34-5 Postal and Electronic Communications Code</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://legifrance.gouv.f...">http://legifrance.gouv.f...</a></td>
</tr>
</tbody>
</table>

http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=23CB346C51E08FC36C767C323143138E.tp...| http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=23CB346C51E08FC36C767C323143138E.tp...|
<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commission Nationale de l’Informatique et des Libertés (CNIL)</td>
<td>CNIL (French Data Protection Authority)</td>
<td>All provisions having an impact on privacy or data protection</td>
<td><a href="http://www.cnil.fr">www.cnil.fr</a></td>
</tr>
<tr>
<td>Direction Générale de la Concurrence, de la Consommation et de la répression des fraudes</td>
<td>DGCCRF (General Directorate of Competition, Consumers and repression of frauds)</td>
<td>Provisions applying to the protection of consumers (such as unsolicited communications)</td>
<td><a href="http://www.economie.gouv.fr/dgccrf">http://www.economie.gouv.fr/dgccrf</a></td>
</tr>
</tbody>
</table>

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?
The definition of networks, services and providers and the provisions transposing the ePrivacy Directive (except for the provision on cookies) are contained in the Postal and Electronic Communications Code (Art. L.32). The scope of application of the Code is limited to operators of electronic communications. However, the scope of some of the provisions is broadened wherever required. This is for instance the case for the provisions that regulate the processing of traffic data which is extended to “persons who, for the needs of their main or a secondary professional activity, provide the public with a connection enabling online communication through access to a network, including free of charge” (hotels, Internet cafés, etc.). Finally one should also keep in mind that the data or activities addressed by the provisions of the ePrivacy Directive involve the processing of personal data. As such the scope of these provisions is also determined by the (scope of the) French data protection law and in particular by the provision transposing Art. 4 of Directive 95/46/EC.

Art. L.32 defines networks, services and providers (operators) as follows:

**Electronic communication networks** are defined as “*any transportation or transmission equipment or systems, including, where relevant, other resources used to convey electronic communications, particularly switching and routing equipment. Electronic communications are defined as emission, transmissions and reception of signs, signals, texts, images or sounds conveyed by electromagnetic means*”. Are listed as electronic communication networks: satellite networks, terrestrial networks, electricity cable networks to the extent they are used for the purpose of transmitting signals, networks used or ensuring the broadcasting of audiovisual communications.

The main difference with the Framework Directive is that French law distinguishes between private and public networks.

Public networks are electronic communication networks that are established or used for the provision of publicly available electronic communication services or public communication services by electronic means. These definitions were transposed by the Act on the Trust in Digital Economy which also transposed the E-Commerce Directive.

**Electronic communication services** are services that entirely or mainly consist in the provision of electronic communications. Are not included services that consist in editing or distributing public communication services provided by electronic means.

Art. L.32 refers to the concept of associated services, which encompasses **value added services**

Associated services are “*any services linked to an electronic communication network or services that contribute or can contribute to the provision of services through such networks or services such as: services of conversion of phone numbers, system of conditional access, electronic guides of programs and services relative to the identification, location and availability of the user*”.

**Operators** are “*any natural or legal persons exploiting a public electronic communication network or providing access to publicly available electronic communication services*.”
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

VoIP, webmail and location based services will fall under the scope of application of Art. L34-1 as far as they can be acknowledged as publicly available electronic communication services, i.e. services that entirely or mainly consist in the emission, transmissions or reception of signs, signals, texts or sounds by electromagnetic way. If the emphasis is on content, the service does not fall under the definition, and therefore also not under the scope of the law. In practice services such as Skype, Gmail, etc. will today be considered as information society services.

In that sense, ARCEP’s Guide of legal obligations of Operators and Service providers clarifies that activities of web hosting, website domain name administrators, creator of website, editor of content and activities exclusively based on software are not subject to the obligation of notification. VoIP, webmail and location based services, as long as they fall under these criteria will thus be exempted from the application of the law.


- A network should include from the start an active element of transmission, switching or routing.
- An electronic communication service consist mainly in a service of transportation information.
- An addressing service, without transport, is not an electronic communications service.
- The concept of remuneration (service not free of charge) is, contrary to the definition contained in the Directive, implicit in the French definition of electronic communication service.
- The provider in charge of signal transmission is the operator.
- It is possible for an entity to qualify both as an information society provider and as an electronic communications operator.

This study examines the status of providers of VoIP. It considers that providers of VoIP services that connect a computer with a phone could qualify as publicly available electronic communication networks providers. In that case, the study recommends to perform a proportionality test before concluding on its qualification as operator. This test should take into account the following elements:

- Whether such qualification would allow to reach the objectives of article 8 of the Framework Directive and article L.32-1 II of the Postal and Electronic Communications Code (processing of traffic data).
- Considering the obligations and constraints that this entity would have to bear, are there
other means, less restrictive (such as the application of competition law) that would allow to achieve the same goals?

- Whether the qualification is coherent with the situation in other EU member States
- Whether the supervision of this entity by ARCEP (resulting from the qualification as operator) would be efficient considering its activity and geographical situation?

5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

Because the ePrivacy Directive has been transposed into French law by legal provisions which have been integrated into the Postal and Electronic Communications Code, the Data Protection Act and the Consumer Law Code, the answer to the question about the territorial scope of the provisions is not obvious.

The provisions of the Postal and Electronic Communication Code are applicable to operators of publicly available electronic communication networks or services that have been notified to the ARCEP (art. L-33-1). The provisions on (L34-1) applies to providers of publicly available electronic communication services whose equipment is located in France or whenever services may have a significant impact on French Internet users. This criteria was confirmed by the State Council in the AT&T and Verizon case (ruling of 10 July 2013). In that ruling, the Court confirmed that ARCEP is entitled to require both Internet service providers and providers of online electronic communications to the public, to provide information about technical conditions and prices applied to interconnection and to the conveyance of data. This obligation reaches any operators whose activity may have an impact on French Internet users, irrespective of the operator’s location.

The ruling is available in French at:

http://www.arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1616&tx_gsactualite_pi1%5BbackID%5D=26&cHash=1253f7c6762d834a2974580817253299

The provisions of the Data Protection Act are applicable to cookies, spam, personal data breaches. As noted in this act:

“This Act shall apply to the processing of personal data only if:

1° the data controller is established on French territory. The data controller who carries out his
activity on French territory within an establishment, whatever its legal form, is considered established on French territory;

2° the data controller, although not established on French territory or in any other Member State of the European Union, uses means of processing located on French territory, with the exception of processing used only for the purposes of transit through this territory or that of any other member State of the European Union."

The provision of the Consumer Code are applicable to the provision of services directed to consumers established in French territory.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law


b. None identified.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The distinction between providers of electronic communications services and providers of information society services is, in the context of the application of provisions with regard to privacy and personal data protection, entirely irrelevant and illogical.

b. Given that the distinction between providers of electronic communications services and providers of information society services is entirely irrelevant in the context of the application of provisions with regard to privacy and personal data protection, this aspect of the ePrivacy Directive should be revised. Streamlining and harmonisation of these rules through convergence is necessary to ensure the credibility and effectiveness of the legal framework.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Art. L.32-3 stipulates that operators and their staff are bound by the secrecy of correspondence. The Ministry in charge of Electronic communications and ARCEP should supervise in order to ensure that operators comply with this obligation (Art. L.32-5-II-5°).

The secrecy of correspondence conveyed by electronic communications is guaranteed by Art. L.241-1 of the Internal Security Code. This provision states that only public authorities are entitled to interfere into this right where justified by needs of public interest as defined by the Law. Art. L.241-2 of the Internal Security Code only allows such interferences on an exceptional basis and for purposes of obtaining information relative to national security, the safeguarding of essential elements of the scientific and economic potential of France, prevention of terrorism, criminality or organised crime and the formation or maintenance of dissolved groups. Infringements of the secrecy of correspondence can qualify as crime or be subject to penalties as defined under article L.226-15 of the Penal Code.

Articles L34-1 to L34-6 of the NCPE defines specific obligations for operators to protect the secrecy of correspondence in transposition of the ePrivacy Directive. Electronic communications are defined by Art. L.32 NCPE as any emission, transmission or reception of sign, signals, text, images or sounds by electromagnetic means.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

Art. L34-1 CPCE mandates the deletion or anonymisation of traffic data for operators of electronic communications and persons whose activity is to provide access to publicly available electronic communication services. This article contains a limited list of derogations:

- Operators can, for purposes of invoicing and payment of electronic communications services, use, store or share with third parties involved with such invoicing or payment, traffic data.
- Operators can also process traffic data to market their own electronic communication...
services, provide added-value services with the express consent of subscribers for a definite period of time which cannot supersede the period of provision of such service.

- Operators can process traffic data to ensure the security of their networks.

The data stored and processed under these exemptions can exclusively relate to the identification of users, technical characteristics of communications (as defined for each exemption by article R10-14 Postal and Electronic Communications Code) and location of terminal equipment. They can never relate to the content of correspondences or information consulted, irrespective of its form, during these communications.

The processing and storage of such data should comply with the provisions of the Data Protection Act.

Operators should take all measures to prevent the use of such data for any other purpose.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Art. L.34-1-III. provides for an additional derogation to the deletion or anonymisation of traffic data, for a period of one year, for the needs of investigation, identification and pursuit of penal offenses or in case of breach of obligations defined under art. L 336-3 of the Intellectual property code (HADOPI related provisions). Traffic data can only be processed for the purpose of disclosing, as far as needed, information to judicial authority or the administrative body mentioned at art. L331-12 of the Intellectual Property Code (HADOPI).

Article L.34-1-1 defines the modalities for access to traffic data by competent law enforcement authorities for purposes of prevention of acts of terrorism. Traffic data that can be accessed are limited to: identification of subscription or connection numbers, listing of all of those numbers for an identified person, location data, technical data of a subscriber relating to called and calling numbers, duration and date of communication. This provision was initially valid until 31 December 2008 but has been prolonged until 31 December 2015.

Article 6 of Act n°2004-575 of 21 June 2004 for Trust in the Digital Economy imposes on ISPs and hosting providers the obligation to retain and store identification data of anyone who has contributed to the creation of content for the services they provide.

A Law proposal on the use of location data in real time for judicial investigations (for penal and customs crimes punished by at least 3 years of prison and for investigations related to deaths, worrying disappearances and search for fugitives) is currently being examined by the Parliament. In its opinion of 19 December 2013 (http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/D2013-404-geolocalisation.pdf), the CNIL stressed that, in that specific case, the use of location data should be acknowledged as interception of the content of communications.
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. French Legislation does not address specifically automated breaches of confidentiality without human involvement. However, the CNIL provided a first interpretation of how the Data Protection Act should apply to the interception of MAC addresses and the capturing of payload data from unencrypted Wi-Fi networks in its Decision 2011-035 of 17 March 2011 (Google case). In this decision, the CNIL considers that the collection of data carried out by Google interferes into the right to privacy, the secrecy of correspondences and to freedom of speech. The CNIL based its interpretation on the massive amount of data that have been collected without previous knowledge by data subjects, some of them being sensitive data (sexual orientation, health data).

In this decision, the CNIL considered that:

- MAC addresses, insofar they only identify a Wi-Fi router, cannot by themselves qualify as personal data. However, when additional information allows to link a MAC address to individuals, they should qualify as personal data. This will be the case when the MAC address is captured by a website after the user has identified himself to this website.
- In the Google case, the CNIL considered that because the collection of MAC addresses was combined with the collection of GPS data of Google cars and the SSID identifiers, for the provision of the service Latitude and other localisation services of Google, the main purpose of the collection was to be able to localise users. MAC addresses thus qualified as personal data. Their collection, without sufficient legal basis, entail a breach of privacy.
- The CNIL first specifies that the recording of data in a format non readable for human has an impact on the qualification of personal data. In the case of Google, the following data were collected: emails, email addresses, location data, websites consulted by Internet users, identifiers and passwords. These data qualify as personal even if they do not relate the names of the individuals they refer to.

With respect to the distinction between protection of content and traffic data: as outlined in the question below, while the NCPE contemplates some derogation to the obligation to delete and anonymise data related to communications, this exception does not apply to data related to the content of communications. The monitoring of the content of electronic communications is
regulated by the Internal security Code.

b. No

5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

- Art. 5.3 of the ePrivacy Directive has been transposed in Art. 32-II DPA. It is drafted as follows:

“Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by the data controller or its representative, except if already previously informed, regarding:

- the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device;

- the means available to them to object to such action.

Such access or recording may only be carried out provided that the subscriber or user has explicitly expressed, after receiving said information, their agreement that may result from appropriate parameter settings in their connection device or any other system under their control.

These provisions shall not apply if the access to data stored in the terminal device of the user or the recording of information in the terminal device of the user is:

- either exclusively intended to enable or facilitate communication by electronic means; or

- strictly necessary for the provision of an online communication service at the user’s express request.”

This provision has been inserted into the Data Protection Act. However, the CNIL clarified that the provision was also applicable to cookies that do not contain personal data. It is thus addressed to any entity accessing the information stored in cookies or storing information on the device of the user/subscriber.

b. The provision quoted above only applies to cookies “either exclusively intended to enable or facilitate communication by electronic means; or strictly necessary for the provision of an online communication service at the user’s express request.” The CNIL clarified that the provision was thus
not applicable to:

- Cookies used to enable “shopping carts” on a commercial website
- Session cookies whenever required for the provision of the service requested by the user
- Cookies used for purpose of security of the service requested by the user
- Cookies used to record users’ preferences, such as language, required for the provision of the service requested by the user
- Flash cookies containing elements strictly necessary for the functioning of media players and relative to a content asked by the user

In those case, while prior information does not have to be provided to the user, the CNIL recommends to inform of their use in the website’s privacy policy.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Article 32-II of the Data protection Act has been interpreted by the CNIL as follows:

- In order to order to gather a valid consent, the user/subscriber should be informed of the purpose of the cookie and then be asked to consent to the installation of a cookie on his device. The user/subscriber should be informed about his right to withdraw his consent at any time. Consent is defined as in the French Data Protection Act: i.e. it should be free, specific and informed. Specific emphasis is put on the content of the information provided as it will determine the validity of the consent gathered. The CNIL stresses the need to provide clear and comprehensible information to the user.
- The CNIL lists as examples several means to gather such consent: banners, an area of application for consent superimposed on the page, ticking boxes in subscription pages to an online service. The CNIL however does not recommend to use classical pop-up pages as they are often blocked by browsers.
- With regard to the possibility to use browser’ settings to gather users’ consent on the use of cookies, while the CNIL does not oppose the solution in principle, it however stresses the multiple problems raised in the current state of the art. Browser settings should allow users to express their choices on a case by case basis. Setting the browser on ‘accept all cookies” does not allow for the user to express a valid consent (it is not specific). In addition, this solution does not allow data controllers to provide clear and complete information to users as required by law, website providers do not have any means to know if the browser has been correctly set, this setting is complex for users and varies from browser to browser. In order to conform to legal requirements, the CNIL suggest the development of specific modules to be installed into the browser or the platform that would allow users to manage their consent.
- The CNIL also clarifies that it is not required to gather a new consent each time the user visit the website. This position also applies to third parties’ cookies, provided that the user consents to it.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Art. 32-II of the Data Protection Act excludes the application of the informed consent rule “if the access to data stored in the terminal device of the user or the recording of information in the terminal device of the user is:

- either exclusively intended to enable or facilitate communication by electronic means; or
- strictly necessary for the provision of an online communication service at the user’s express request.”

As mentioned above, The CNIL clarified that the provision on consent was not applicable to:

- Cookies used to enable “shopping carts” on a commercial website
- Session cookies whenever required for the provision of the service requested by the user
- Cookies used for purpose of security of the service requested by the user
- Cookies used to record users’ preferences, such as language, required for the provision of the service requested by the user
- Flash cookies containing elements strictly necessary for the functioning of media players and relative to a content asked by the user

In those case, while prior information does not have to be provided to the user, the CNIL recommends to inform of their use in the website’s privacy policy.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The clarification by the CNIL of the rules applying to cookies provided more legal certainty and gave concrete guidance for the implementation of the new rules. This encouraged many websites to obtain prior consent of their user for the use of cookies, mainly through an area of application for consent superimposed on the entry page.

Statistics on compliance or on user views are to our knowledge not available.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

   a. CNIL, recommendation on cookies (Délibération n° 2013-378 of 5 December 2013):
      http://www.cnil.fr/documentation/deliberations/deliberation/delib/300/

   b. No case law is, to our knowledge, available. However, the CNIL recently sanctioned Google Inc. for not complying with its obligation to obtain user consent prior to the storage of cookies on their terminals (Deliberation n°2013-420 of the Sanctions Committee of CNIL imposing a financial penalty against Google Inc. An English translation is available at: http://www.cnil.fr/fileadmin/documents/en/D2013-420_Google_Inc_EN.pdf).

   The CNIL first finds that, for users of the company’s services who are not pre-authenticated, cookies are stored immediately on the terminal upon connection to the service. The company thus does not provide the information required by the law before any action of registering or reading information stored on users’ terminal.

   Second, the CNIL finds that the information banner appears only on two of its services and the information provided through this banner does not allow users’ company’s services to be informed in a sufficiently precise way as to the purposes pursued by the company to use cookies. Indeed, the latter mentions only that cookies are placed in order to insure the “proper operation of the services”. The information provided through the layered approach is considered as not sufficiently detailed. This information delivered is thus too general to satisfy the objective of clear and complete information of the users. In addition, the CNIL notes that the presence of an “OK” button in the banner gives the user the impression that they can decide about the storage of cookies on their terminal, while it is not the case.

   The CNIL reminds that “Compliance with article 32-II, then, implies that the storage of this cookie must be done after delivery of information about this second purpose and after the user has expressed his/her consent. The same conditions are required prior to storage of any other cookie which, not being covered by the aforementioned exception, is intended for a different purpose, without the necessity of determining the existence or presence of such cookies”.

   About the validity of consent provided through browser setting, the CNIL points out that browser settings may be validly claimed to constitute a means of expressing consent in the sense of article 32-II of the law only to the extent that the user has been given the means to
understand the scope of this consent. In that case, “both the generic nature of the information provided in the banner and the simultaneous placement of cookies on the user’s terminal deprive the latter of the option of expressing a choice as to the writing of cookies on his/her terminal”.

Finally, about cookies placed on the terminals of “passive users”, whose data are sent to the company during their browsing on third-party sites (such as analytics cookies). In this specific case, the company still collates the data from users of its Analytics services to generate statistics per sector and use these data in making improvement to its own services. It thus plays a role of data controller and as such it is incumbent to the company to comply with the obligation set in article 32-II for that part of the processing of which it determines the purposes and means and for which the site publisher are not responsible. The CNIL concludes that “in the absence of an informative statement on the site visited displayed prior to the storage of a cookie, the company may not validly maintain that the user has been informed of the purpose for the processing, and even less so, claim his/her consent”. The storage of cookies in that case thus cannot benefit from the exceptions provided for in article 32-II.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The transposition of the cookies provision directly into the Data Protection Act, even if its scope of application is broader as it applies to cookies that do not contain personal data, together with the competence given to the CNIL for the supervision of its application, gave a better chance for its implementation in practice. Furthermore, because it was not transposed into the Postal and Electronic Communication Code, it avoids the problem relating to the interpretation of its scope of application.

The recommendation on cookies issued by the CNIL at the end of 2013 contributed to clarify how the rules on cookies should be implemented in practice. It should help to achieve a larger and more systematic application of the rules.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Art. L32-18° CPCE reproduces the definition of traffic data contained in the Directive. It defines traffic data as “any data processed for the conveyance of a communication through an electronic communication network or for the billing thereof”.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Art. L34-1. NPCE is formulated as follows:

“II- Operators of electronic communications, most particularly persons whose activity consists in providing access to an online publicly available communication service, must delete or anonymize any traffic data without prejudice to provisions of III, V and VI.

Persons who provide publicly available electronic communication services must establish, in accordance with the provision of the previous paragraph, internal procedure to answer requests from competent authorities.

Persons who, for the needs of their main or a secondary professional activity, provide the public with a connection enabling online communication through access to a network, including free of charge, must comply with provisions applicable to operators of electronic communications contained in this article.

(…)

IV. – For the needs of invoicing and the payment of electronic communication services, and for the period during which the invoice can be legally challenged or pursuit engaged to obtain the payment, operators can use, store and wherever relevant share with third parties involved in invoicing and payment the categories of technical data within limits defined under IV according to activities of operators and the nature of the communication, as defined by a decree of the State Council adopted after priori opinion of the CNIL.

[Art. R10-14 I and II list the categories of traffic data whose retention is allowed:

- Technical data allowing the identification of the user
- Data relative to terminal equipment used for communication
- Technical data, date, hours and duration of each communication
- Data relative to complementary services requested or used and their providers]

Operators can also process traffic data to market their own electronic communication services or to provide added-value services, provided that subscribers expressly consent to it and for a defined period of time. This period cannot be, in any case, superior to the one necessary for the provision or the marketing of such services.

They can also store certain data to ensure the security of their networks.

[Art. R10-14 IV lists the categories of data that can be retained for security purposes:

- Technical data allowing the identification of the user
- Data relative to terminal equipment used for communication
- Technical data, date, hours and duration of each communication]
Data relative to complementary services requested or used and their providers

VI. – Data stored and processed under III, IV and V only relate to the identification of users of services provided by operators, on technical characteristics of communications ensured by operators and on location of terminal equipment. They cannot relate, in any case, to the content of the correspondence exchanged of information consulted, whatever its form, within these communications.

Storage and processing of data should comply with the provisions of the Act n° 78-17 of 6 January about informatics, files and freedoms.

Operators should take all necessary measures to prevent the use of these data for other purposes.”

The main differences with the ePrivacy Directive are:

- The obligations relating to the processing of traffic data extends to persons who, for the needs of their main or a secondary professional activity, provide the public with a connection enabling online communication through access to a network, including free of charge.
- French legislation specifies which traffic data can be processed for the purposes of subscriber billing and interconnection payment,
- Consent provided by the user for the processing of its traffic data for purposes of electronic communications services or the provision of value added services should be express, and is only valid for a definite period of time which cannot be longer than the one necessary for the provision or the marketing of such services.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

As noted above, Art. L34-1 is formulated as follows:

“II. Operators of electronic communications, most notably persons whose activity consists in providing access to online publicly available communication services, must delete or anonymize any traffic data, without prejudice of provisions contained in III, V and VI.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

No.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions of Article L.34-1 of the Postal and Electronic Communications Code are not sufficient for the protection of subscribers and users because their scope is limited to “operators” and persons who, for the needs of their main or a secondary professional activity, provide the public with a connection enabling online communication through access to a network. The processing of traffic data by network and service providers, other than those entities is only protected via the general data protection legislation (in particular the proportionality principle).
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Location data are not defined; rather, they are treated as a specific category of traffic data. They are referred to as “data allowing the location of user’ terminal equipment” (art. L.34-1-V)
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Art. L.34-1-V NPCE is formulated in similar terms as the Directive.

This article states that:

“V.- Without prejudice to III and IV and the needs of judicial investigations, data allowing the location of user’ terminal equipment can neither be used during communication for other purposes than their conveyance, or be stored and processed after the end of the communication, except if user has consented to it after being informed of categories of data involved, of the duration of the processing activity and whether that such data will be shared with third party service providers. Subscriber can withdraw their consent at any time, free of charge, besides costs linked to the transmission of the withdrawal. User can suspend the consent given, through simple means and free of charge, except for the costs of this suspension. Any call directed to an emergency service is acknowledged as user consent until the end of the rescue operation it triggers and only to allow it to be carried out.”

The main difference is that it adds a provision to allow the processing of location data in cases of emergency calls during the rescue operation (transposing the eCall directive).
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Location data being acknowledged as a specific categories of traffic data, they fall under the general requirement of deleting or anonymising traffic data (art. L.34.1-II CPCE)
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. The CNIL has issued guidelines to process location data in specific cases. This guidance however refers to the application of the data protection act:
   - Geolocalisation and collection of information from Wi-Fi hotspots, 5 May 2011
   - Recommendation on the implementation by Insurance companies and Car constructors, of devices of geolocalisation on vehicles (Decision 2010-096 of 8 April 2010) [http://www.cnil.fr/documentation/deliberations/deliberation/delib/224/](http://www.cnil.fr/documentation/deliberations/deliberation/delib/224/)

b. None available to our knowledge.

The CNIL has recently fined with 5000€ a car rent company who had installed location devices on the luxury cars rented by the company to fight against car retention and theft (Deliberation n°2014-294 of 22 July 2014). The devices were set to be always active without any possibility to deactivate them. This allowed the company to know the location of their clients at all times and to reconstitute their itineraries. The CNIL found that the amount of location data collected is excessive with regard to the purpose of collection. The device should only be activated whenever required (retention of the car by the client or theft).

The CNIL has also fined an employer with 3000€ for not individually informing employees about the characteristics of the location devices installed on their cars (Deliberation n°2013-366 of 23 November 2013).
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

Article L.34-1 of the Postal and Electronic Communications Code doesn’t sufficiently protect individuals against illegitimate processing of location data because the scope of the Article is limited to “operators”. The CNIL had to issue a broad interpretation of the general rules of the data protection framework in order to compensate for this lack of protection.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. Art. L34-5 CPCE regulates unsolicited direct marketing communications.

   It bans direct marketing making use of automated systems of electronic communications, fax or email based on subscribers’ contact details who did not consent to it. The definition of consent is identical to the one provided by the 95/46/EC Directive.

   This article defines direct marketing as the sending of any message intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services. Calls and messages directed to incite users or subscribers to call an added-value phone number to send an added value text message are acknowledged as direct marketing.

   It also transposes the derogation contained in the Directive and allows direct marketing of providers’ own similar products and services, provided that the user is given the possibility, expressly and without ambiguity, to object, free of charge, except for those linked to the transmission of the objection, in a simple means, to the use of his contact details, at the moment of collection and each time a direct marketing email is been sent to him.

   Direct marketers should include valid contact information to which users and subscribers can object to receiving additional communication. It also forbids to conceal the identity of the person for which the communication is issued or to mention a subject line with no relation to the service proposed.

   The CNIL is charged with enforcement of these provisions. It can receive complaints from users and subscribers. Together with other public authorities with competence to fight spam (such as the DGCCRF and law enforcement) and operators, it has created a dedicated platform to ease the report of spam by users and their effective blocking by private operators. See: https://www.signal-spam.fr/
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The legal requirements for the lawful sending of unsolicited messages via electronic mail or fax and SMS-MMS are regulated under art. L34-5 of the Postal and Electronic Communications Code. As described above, the content of French legislation is similar to the Directive.

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Art. L34-1 contains two exceptions:

- If the user/subscriber is a client of the service provider and the communication relates to similar products offered by the provider
- If the message lacks any commercial nature (notably targeting charity messages)

In both cases, the user/subscriber should, at the moment of the collection, be informed that his email will be used for direct marketing purposes and be able to object to such use by simple means and free of charge.

The prohibition does not apply to legal persons, provided that the following conditions are complied with:

- the user/subscriber should, at the moment of the collection, be informed that his email will be used for direct marketing purposes and be able to object to such use by simple means and free of charge
- The content of the message should relate to the professional activity of the recipient

Direct marketing can at any rate be sent to generic professional address such as info@society.fr, as they do not qualify as personal data.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Electronic mail is defined as: "a text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient" (Act for Trust in the Digital Economy). This definition covers not only electronic mail through the internet, but also MMS/SMS/text messages, voice mail, etc.. This broad scope is thus in line with the definition of “electronic mail” in the ePrivacy Directive.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. Factsheets of the CNIL on:

b. None available to our knowledge.

The CNIL has however fined a company with 20.000 € for sending direct marketing SMS to individuals without their prior consent (Deliberation n°2011-384 of 12 January 2012). The company bought databases with contact details of house owners captured from websites specialised on real estate listings and used this information to market their own services. The CNIL stressed that article L.34-5 of the Code of Postal and Electronic Communications does not punish the collection of data but the collection of contact details for direct marketing of individuals who did not consent to it. The company had the duty to ensure that the data used complied with the prior consent requirement. It cannot be presumed that the company from which the data were obtained gathered users’ consent, as it is not an obligation put upon them.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The French legal framework on unsolicited communications is in practice interpreted and amended by codes of conduct adopted by the advertising sector. The fight against spam is organised and the initiative of creating a specific entity that incorporates representatives of the public and the private sector is a positive step. However, its real impact on the amount of unsolicited communications remains unclear, as this information is not communicated.
COUNTRY REPORT

CROATIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Nina Gumzej, University of Zagreb Faculty of Law

Date: August 19, 2014
Contents

Part 1: Management summary ................................................................. 3
Part 2: Answers to the questionnaire ......................................................... 5
Part 1: Management summary

Management summary Croatia:

- Relevant rules transposing the ePrivacy Directive are implemented in the Electronic Communications Act. The Croatian Regulatory Authority for Network Industries (HAKOM) carries out inspections over the implementation of this Act and regulations adopted pursuant to it. It is also competent to carry out supervision over compliance of business operations of operators of electronic communications networks and/or services with the provisions of this Act (also) concerning personal data protection. Prescribed sanctions in the Act are strict and dissuasive, and HAKOM has direct sanctioning authority. According to the Electronic Communications Act in addition to HAKOM also the Personal Data Protection Agency (AZOP) is authorized to order termination of breaches of relevant rules transposing the ePrivacy Directive (which are in focus of this study), ex officio or upon request of an interested party. AZOP has general authority on the basis of the Personal Data Protection Act to supervise implementation of personal data protection in Croatia, upon request of the data subject, upon proposal of a third party or by official duty. Unlike HAKOM, it has no direct sanctioning authority.

- On the whole, relevant rules in the Electronic Communications Act are implemented in line with the ePrivacy Directive. These apply on Croatian territory and only natural and legal persons registered in Croatia are subject to them. They apply in the first place to operators of public communications networks / publicly available electronic communications services. Furthermore, according to their text, Article 100 which transposes Article 5 of the ePrivacy Directive and Article 107 (1) - (4) transposing Article 13 of ePrivacy Directive, apply to all domestic persons/bodies. According to their text, Articles 102 and 104 transposing Articles 6 and 9 of the ePrivacy Directive apply, in addition to operators of public communications networks / publicly available electronic communications services, also to providers of special tariff services. In 2011 the concept of value added services was replaced by the different concept of special tariff services. In my opinion the definition of value added services and references to it should be reintroduced into the Act in line with the ePrivacy Directive.

- Of all the rules implementing the ePrivacy Directive it is the rule on unsolicited communications, i.e. Article 107 (1) – (4) of the Act that mostly gives rise to customer complaints and supervision measures and there is some regulatory and court case law on this in Croatia. This rule is also referred to in other acts, one of which is the Electronic Commerce Act, which applies to information society providers and prescribes significantly lower monetary fines for breaches of the relevant rule (in relation to the Electronic Communications Act). Implementation of that Act is supervised by Inspectorate of the Ministry of Finance - Customs Administration. According to the Inspectorate there has yet been no supervision (upon requests/complaints or by official duty) regarding the implementation of the relevant rules. The Second act referring to the rule on unsolicited communications is the new Consumer Protection Act (2014). This Act does not stipulate a fine for violation of the rule. Supervision over its implementation (inspection) is carried out by Ministry of Economy market inspectors. Relevant rule was recently adopted and no complaints have yet been filed (from consumers - natural persons). Also, in reference to both
mentioned Acts, there is already envisaged venue to address unsolicited communications complaints on the basis of the *Electronic Communications Act* (to HAKOM), *i.e.* Article 107 of that Act, which applies to all natural and legal persons. Taking all these rules into account and different competent authorities for supervising their implementation it is reasonable to expect ongoing efforts towards consistency of practice as regards interpretation of legal requirements of Article 107 (1)–(4) of the *Electronic Communications Act* and implementation thereof. A need may well arise to align, across different sectors, sanctions prescribed in different acts, *i.e.* monetary fines, for breaches of one and the same rule on unsolicited communications.

- Additionally to implementation of Article 13 of ePrivacy Directive in Article 107 (1) – (4), further stipulated in that Article are also duties and rights of operators providing e-mail services with respect to filtering of incoming emails and resolving users’ complaints on e-mail abuse, subscriber contracts prohibiting unsolicited communications and sanctions for subscribers, etc.

- The *Personal Data Protection Act* has its own direct marketing provision, which is exclusively supervised by AZOP. In cases where AZOP estimates upon user’s complaint that a breach of Article 107 of the *Electronic Communications Act* occurred, it cooperates with HAKOM, to which it sends those complaints. This is in cases of unsolicited e-mails in particular where AZOP finds that the user could benefit special protection on the basis of above mentioned additional rules in the *Electronic Communications Act* (e-mail filters, e-mail abuse procedure).

- *Electronic Communications Act* rules transposing Articles 5, 6 and 9 of the ePrivacy Directive have so far not been the focus of regulatory attention (HAKOM, AZOP), mostly due to lack of complaints/requests and to the best of our knowledge there is no case law on this. According to its 2008 Annual report AZOP conducted supervision in the telecommunications sector, where it made inquiries from operators as to their practices in protecting subscribers’ personal data under the Telecommunications Act (then in force) and the *Data Protection Act*. End-result was a general recommendation for all operators to work on special procedures for protecting subscribers’ personal to prevent abuse and to organize education for their employees.

- There is currently no regulatory guidance in Croatia on implementation of relevant rules implementing the ePrivacy Directive. That seems in particular necessary in the case of Article 100 (4) of the *Electronic Communications Act* (“cookie rule”) due to users’ requests filed to both HAKOM and AZOP. Interpretations of relevant ePrivacy Directive rules do exist at EU level, *e.g.* documents of the Article 29 Working Party that can help in creating guidance materials in Croatia - even though they are not binding. It is therefore suggested, especially taking into account that AZOP takes part in activities of that party, that relevant practice and documents are shared and consulted between relevant authorities, especially in coordination with HAKOM. As for binding interpretations of the ePrivacy Directive (CJEU case law) it would be helpful for transparency purposes to regularly publish them at the regulatory authorities’ webpages.

- There are examples of rules implemented in the *Electronic Communications Act* and related secondary legislation, which should be reconsidered in light of their significant impact on e-privacy rights (encroachment).
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

The ePrivacy Directive has first been transposed into Croatian legislation by the 2003 Telecommunications Act (Official Gazette of the Republic of Croatia no. 122/03). In 2008 a new law, Electronic Communications Act, entered into force. The Electronic Communications Act (hereinafter “the Electronic Communications Act”) has been amended four times (Official Gazette of the Republic of Croatia no. 73/08, 90/11, 133/12, 80/13 and 71/14). The unofficial consolidated text in Croatian is available at: http://www.mppi.hr/UserDocsImages/ZEK2008-2014%20RED-T%2018-6_14.pdf.

The Electronic Commerce Act and Consumer Protection Act refer to the rule on unsolicited communications in the Electronic Communications Act. The Electronic Commerce Act, Official Gazette of the Republic of Croatia no. 173/03, 67/08, 36/09, 130/11 and 30/14 (in which the E-Commerce Directive 2000/31/EC was implemented) applies to information society service providers.

Recently a new Consumer Protection Act (Official Gazette of Republic of Croatia no. 41/14) entered into force in Croatia (most provisions entered into force, replacing the old Consumer Protection Act, Official Gazette of Republic of Croatia no. 79/07, 125/07, 75/09, 79/09, 89/09, 133/09, 78/12 and 56/13), however, some provisions of the old act shall remain in force until January 1, 2015, when the corresponding provisions of the new Act will enter into force.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 3 (Scope)</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>Articles 100 (1) - (2) of the Electronic Communications Act.</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Article 100 (3) of the Electronic Communications Act,</td>
<td></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Article 100 (4) of the Electronic Communications Act,</td>
<td></td>
</tr>
<tr>
<td>Art. 6 (Traffic data)</td>
<td>Article 102 of the Electronic Communications Act</td>
<td></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Article 104 of the Electronic Communications Act</td>
<td></td>
</tr>
<tr>
<td>Art. 13 (Unsolicited communications)</td>
<td>Article 107 (1) – (4) of the Electronic Communications Act,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 8 of the Electronic Commerce Act (reference to relevant rules in the Electronic Communications Act)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 94 of the Consumer Protection Act (reference to relevant rules in the Electronic Communications Act)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://narodne-novine.nn.hr/clanci/sluzbeni/2014_03_41_723.html">http://narodne-novine.nn.hr/clanci/sluzbeni/2014_03_41_723.html</a></td>
<td></td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hrvatska regulatorna agencija za mrežne djelatnosti</td>
<td>Croatian Regulatory Authority for Network Industries (HAKOM)</td>
<td>All provisions transposed into the Electronic Communications Act</td>
<td><a href="http://www.hakom.hr">www.hakom.hr</a></td>
</tr>
<tr>
<td>Agencija za zaštitu osobnih podataka</td>
<td>Personal Data Protection Agency (AZOP)</td>
<td>All provisions having an impact on personal data protection - in line with the Agency’s authority to supervise the collection, processing and use of personal data relating to natural persons in the Republic of Croatia (Personal Data Protection Act). Furthermore, pursuant to Article 107a of the Electronic Communications Act, which was first adopted in this Act in 2011, AZOP is competent, in accordance with its authority, ex officio or upon request of an interested party, to adopt a decision ordering the termination of breaches of provisions of Articles 99 to 107</td>
<td><a href="http://www.azop.hr">www.azop.hr</a></td>
</tr>
</tbody>
</table>
of this Act. These Articles include *inter alia* transposed provisions of the ePrivacy Directive that are in focus of this study, *i.e.* Articles 5, 6, 9 and 13.

<p>| Market inspectors at the Ministry of Economy | Reference to the provision on unsolicited communications as regulated by Article 107 of the <em>Electronic Communications Act</em>, which transposes Article 13 of the ePrivacy Directive, is contained in the <em>Consumer Protection Act</em> (Article 94). Implementation of this Act is supervised by market inspectors at the Ministry of Economy. | <a href="http://www.mingo.hr">www.mingo.hr</a> |
| Inspectorate of the Ministry of Finance - Customs Administration | Reference to the provision on unsolicited communications as regulated by Article 107 of the <em>Electronic Communications Act</em>, which transposes Article 13 of the ePrivacy Directive, is contained in the <em>Electronic Commerce Act</em> (Article 8). Supervision over implementation of this Act (inspection) has recently been passed from the State Inspectorate to the | <a href="http://www.carina.hr">www.carina.hr</a> |</p>
<table>
<thead>
<tr>
<th>Inspectorate of the Ministry of Finance - Customs Administration.</th>
</tr>
</thead>
</table>

**Explanation:**

- The relevant telecoms regulator - the Croatian Regulatory Authority for Network Industries (HAKOM) carries out inspections over the implementation of the Electronic Communications Act and regulations adopted pursuant to it (secondary legislation). It is also competent for carrying out supervision over compliance of business operations of operators of electronic communications networks and/or services with the provisions of the *Electronic Communications Act* (also) concerning personal data protection.

- Specifically with respect to breaches of relevant rules transposing the ePrivacy Directive (which are in focus of this study) HAKOM is authorized to adopt decisions ordering their termination, *ex officio* or upon request of an interested party. For the purpose of implementing such decisions it is entitled to request all data deemed necessary for the establishment of possible breaches of relevant provisions or for monitoring and implementing them. These competencies are according to the Electronic Communications Act also granted to the Croatian Personal Data Protection Agency (AZOP). AZOP supervises the processing of personal data of natural persons in Croatia in line with its main act, under which it was founded – the Personal Data Protection Act. The Personal Data Protecton Act (Official Gazette of Republic of Croatia no. 103/03, 118/06, 41/08 and 130/11, no. 106/12 – the consolidated text in Croatian is available at: [http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html](http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html)) regulates protection of personal data regarding natural persons and the supervision of collecting, processing and use of personal data in Croatia. AZOP supervises the implementation of personal data protection upon request of the data subject or a third party, or by official duty.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Relevant rules of the Electronic Communications Act transposing the ePrivacy Directive will in the first place apply to operators of public communications networks / publicly available electronic communications services. Electronic communications service is defined as “a service that is normally provided for remuneration and which consists wholly or mainly of conveyance of signals in electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but which excludes services providing, or exercising editorial control over content transmitted using electronic communications networks and services. These services do not include information society services that do not consist wholly or mainly of conveyance of signals in electronic communications networks”. Public communications services are “electronic communications services that are publicly available on a market basis” (Article 2 (1) points 10 and 20 of the Electronic Communications Act). Electronic communications network is defined as “transmission systems and, where applicable, switching or routing equipment and other resources, including inactive network elements, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, broadcasting networks, and cable television networks, irrespective of the type of information conveyed”. Public communications network is “an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services and which supports the transfer of information between network termination points””. (Article 2 (1) points 7 and 19 of the Electronic Communications Act). Operator (of public communications networks / publicly available electronic communications services) is defined as “a legal or a natural person providing or authorised to provide a public communications service, or to make available a public communications network or associated facilities” (Article 2 (1) point 36 of the Electronic Communications Act).

The most relevant definitions in the Act are aligned with the ePrivacy Directive. An exception is the definition of value added services. Namely, with the amendment of the Act in 2011, the definition of a value added service, which was until this amendment correctly transposed into Croatian legislation in accordance with the ePrivacy Directive (in the 2003 Telecommunications Act), as any service requiring processing of traffic data or location data other than traffic data beyond what is necessary to transmit or bill a communication, was replaced by the concept of special tariff services. Accordingly, all references to the value added services in the Act were substituted with this new term. It is in my opinion it is not unlikely that where relevant provisions of the Electronic Communications Act transposing the ePrivacy Directive are concerned, substitutions of references to special tariff services were made “automatically”. ‘Special tariff services’ are defined as “services provided via public communications networks and services by means of special numbers or special codes from the ‘Numbering Plan’ or the ‘Addressing Plan’, for the purpose of realisation of predetermined additional contents and/or services within these contents outside the scope of public communications” (Article 2 (1) point 73). Addressing Plan refers to “all possible combinations of addressing elements which are used for the unique identification of persons, computer processes, machines, devices or electronic communications equipment which is included in the procedure of establishing a connection”. Numbering Plan refers to “all possible combinations of addressing elements by means of digits for the purpose of unique identification of persons, computer processes, machines, devices or electronic communications equipment which is included in the procedure of
establishing a connection”. Operator of special tariff services is “the operator who is authorised to provide special tariff services pursuant to an access or interconnection agreement “ (Article 2 (1) point 38). According to HAKOM special tariff services are electronic communication services and operators must register with HAKOM prior to providing these services in Croatia.

According to its general provisions the Electronic Communications Act does not apply to content produced, conveyed or published by means of providing electronic communications networks and services. Accordingly, electronic communications services exclude services providing, or exercising editorial control over content transmitted using electronic communications networks and services. As such, electronic communications services do not include information society services that do not consist wholly or mainly of conveyance of signals in electronic communications networks (information society services are defined in the Electronic Commerce Act, which transposed the E-Commerce Directive 2000/31/EC). On the other hand, according to the text of relevant rules, Article 100 of the Electronic Communications Act which transposes Article 5 of the ePrivacy Directive and Article 107 (1) - (4) which transpose Article 13 of ePrivacy Directive, will apply to all domestic persons/bodies and thus also to webmail services and location based services, information society service providers (regardless of the fact if they are authorized to provide an electronic communications service or not). This is with respect to the unsolicited communications rule in the Electronic Communications Act also in line with the scope of protection afforded by the Consumer Protection Act and the Electronic Commerce Act, since these acts refer to it. In line with the text of Articles 102 and 104 which transpose Articles 6 and 9 of the ePrivacy Directive, these provisions will, in addition to operators of public communications networks / publicly available electronic communications services, also apply to providers of special tariff services (concept of special tariff services in the Act that substituted the earlier concept of value added services, as explained above).
<table>
<thead>
<tr>
<th>4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAKOM considers VoIP a public electronic communications service, which therefore falls within the scope of implementing legislation (<em>Electronic Communications Act</em>). For other answers please see information in the previous point (3).</td>
</tr>
</tbody>
</table>
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

Operators are entitled to install, use and make available an electronic communications network and provide electronic communications services on the territory of the Republic of Croatia on the basis of general authorisation, i.e. without obtaining a special authorisation, under the conditions laid down in the Electronic Communications Act and regulations adopted pursuant to this Act. Operators of public electronic communications networks and publicly available electronic communications services, which are provided on a commercial basis, must notify HAKOM in writing, at least fifteen days in advance, about the start, changes and termination of the provision of electronic communications networks and services. This also applies to operators of public communications services from EU Member States providing cross-border publicly available electronic communications services in several EU Member States, including to legal persons in the Republic of Croatia (Articles 31 and 32).

According to HAKOM the Electronic Communications Act applies only on the territory of the Republic of Croatia, and only natural and legal persons registered in Croatia are subject to it. It is not possible to apply the Act to providers who provide services or whose services are available in Croatia if they are not registered to provide their services and if they are not established in Croatia. Supervision over those providers is carried out by competent authorities of their establishment and HAKOM is in case of irregularities on their part only in the position to ask for help of the competent foreign authority, although there is also a case where HAKOM successfully cooperated directly with the foreign company in resolving the breach (spam) directed toward Croatian users. With the exception of the above, according to HAKOM there were with respect to provisions of the Electronic Communications Act implementing Articles 5, 6, 9 and 13 of the ePrivacy Directive no complaints and actions taken by HAKOM with respect to foreign operators/entities/persons in the sense that they would affect service users in Croatia and if there were HAKOM would turn to the competent foreign authority.

The Electronic Communications Act as of its amendment in 2011 (transposing inter alia Directive 2009/136/EC) provides for the possibility for HAKOM to prescribe measures to ensure efficient cross-border cooperation in the implementation of relevant rules implementing the ePrivacy Directive, and harmonised conditions for the provision of services involving cross-border data flows (Article 107a (3)). According to HAKOM, such ordinance and measures were not adopted.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. There is regulatory case law where Article 107 (1) - (4) which transposes Article 13 of ePrivacy Directive was applied also to legal and natural persons who are not operators, which proves the general scope of that provision (for details please see below the corresponding section on unsolicited communications – E 5).

   b. There are court cases showing that Article 107 (1) - (4) which transposes Article 13 of ePrivacy Directive will be applied to legal and natural persons who are not operators, which proves the general scope of that provision (for details please see below the corresponding section on unsolicited communications – E 5).
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. There is a general lack of regulatory guidance and case law in Croatia on most of the relevant rules transposing the ePrivacy Directive that are the focus of this study (with the exception of rules on unsolicited communications). Distribution of regulatory competencies in the area of e-privacy is not entirely clear and the competences of authorities supervising the application of relevant rules significantly diverge (HAKOM, AZOP, different inspectorates supervising the application of relevant rules in the Electronic Commerce Act and the Consumer Protection Act). This may impair the goal of applying clear, consistent and effective e-privacy legislation in Croatia.

   b. In order to ensure harmonized interpretation and the application of Articles 6 and 9 of the ePrivacy Directive, the definition and concept of ‘value added services’ should be reintroduced into the Electronic Communications Act. What could also be considered is the introduction of a rule on the scope of the relevant provisions implementing the ePrivacy Directive (e.g. in line with Article 3 of the ePrivacy Directive) into the general provisions of this Act and, especially to avoid legal uncertainty where addressees are not (only) providers of electronic communications services, include references to the broad scope of application of certain rules, i.e. those applying to all natural and legal persons, including information society providers.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Article 100 (1) – (2) of the Electronic Communications Act stipulates that in order to secure the confidentiality of electronic communications and related traffic data in the public communications network and publicly available communications services, listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data shall be prohibited.

According to its text, this rule applies to all domestic persons/bodies and not only to relevant operators. The rule contains a general prohibition, which is different from the ePrivacy Directive, where stated interception or surveillance by persons other than users, is to be prohibited (without the consent of users concerned).

Exceptions to the rule (prohibition) include the technical storage of data necessary for the conveyance of communications, without prejudice to the principle of confidentiality - Article 100 (2) of the Electronic Communications Act, and the legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication - Article 100 (3) of the Electronic Communications Act (see also below, under B 2). Other exceptions are specified further below (answer under B 3).

The monetary fines prescribed for violation of Article 100 (1) of the Electronic Communications Act (misdemeanour) range from app. 13100 - 131000 Euros for legal persons, and from 1300 – 6500 Euros for natural persons.

A communication is defined in Article 2 (1) point 24 of the Electronic Communications Act in line with the ePrivacy Directive, as any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include information broadcasted to the public as part of radio and television activities to the public over an electronic communications network, except for information that can be related to an identifiable subscriber or user receiving such information.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Article 100 (3) of the Electronic Communications Act stipulates that the prohibition of listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data does not apply to legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Article 100 (1) of the *Electronic Communications Act* prescribes that ‘cases’ referred to in Article 108 of that Act and ‘cases prescribed by special laws’ constitute exceptions to the prohibition:

- ‘Cases’ referred to in Article 108 of the *Electronic Communications Act* are duties of operators to ensure and maintain at their own expense the function of *lawful interception of electronic communications networks and services*, as well as electronic communications lines to the operational and technical authority competent for activation and management of lawful interception measures in electronic communications, in accordance with legislation on national security (Act on the Security Intelligence System of the Republic of Croatia, Official Gazette of the Republic of Croatia no. 79/06 and 105/06; Decree on obligations in the area of national security of the Republic of Croatia for legal and natural persons in telecommunications, Official Gazette of the Republic of Croatia no. 64/08 and 76/13). Article 108 of the *Electronic Communications Act* also prescribes that in such cases all provisions of the Act implementing the ePrivacy Directive as well as special rules on personal data protection do not apply. Furthermore, if the operators are compressing or encrypting electronic communications traffic, they are obliged to deliver such traffic data in their original form and they must upon request of the ‘competent authorities’ prevent their users from using programmes for encrypting content of communications or enable competent authorities to implement measures for removal of encryption (‘competent authorities’: operational and technical authority competent for the activation and management of the lawful interception measure in electronic communications, authorities authorised for implementation of lawful interception measures in electronic communications networks and services)

- ‘cases prescribed by special laws’ are e.g.: above mentioned national security legislation as to measures of secret surveillance of telecommunication services, activities and traffic; criminal procedure law concerning the special collection of evidence by measures temporarily restricting citizens' constitutional rights (Criminal Procedure Act, Official Gazette of the Republic of Croatia no. 152/08, 76/09, 80/11, 91/12, 143/12, 56/13 and 145/13).

Furthermore, according to special obligations concerning data retention for the purposes of investigation, discovery and criminal prosecution of criminal offences and for defence and national security purposes, it is strictly forbidden for operators to record and store data revealing content of communications (Article 110 (3) of the *Electronic Communications Act*).

On the other hand, HAKOM’s *Ordinance on the manner and conditions for the provision of electronic communications networks and services*, secondary legislation based on the *Electronic Communications Act*, prescribes a particular duty of operators to ‘retain and provide destination IP addresses’. Namely, the operator is in case of a complaint from an end-user regarding the bill for Internet access services obliged to deliver also a detailed list of IP addresses accessed from the end-user’s account (destination IP addresses), together with names of IP addresses (if possible). According to HAKOM, the legal basis for the above stated duty to keep and deliver destination IP addresses is the provision of the *Electronic Communications Act* pursuant to which operators must automatically record data on provided services to their end-users for billing purposes and allow
them verification and control of the data on charges for provided services, as well as allow their subscribers an itemized bill for provided services, free of charge and upon their request (Article 44 (1)-(2) of the Electronic Communications Act).

In case of users’ complaint to Internet traffic charges, the only document for cost control would be the bill, i.e. originating IP addresses. HAKOM considers that this does not constitute enough proof to verify that the bill is correct. In such cases it finds it necessary to compare the time and duration of the session by way of detailed printed (destination) IP addresses with the bill in order to determine their compatibility. HAKOM also points to the fact that the Ordinance prescribes such obligations only as an exception - in cases of bill complaints, which would sufficiently meet the purpose to be achieved. While recognising that this does amount to the monitoring of visited web sites, pointing to specific type of content, HAKOM notes that users can give their consent in the subscription agreement (agree to operators’ general terms and conditions) and that users may at any time withhold their consent. HAKOM further points to the duty to retain traffic data in Article 102 (2) - processing of traffic data needed for billing purposes, and to the paragraph 5 of the same Article, which allows processing of such data for the purpose of resolving customer complaints. This according to HAKOM undoubtedly includes also destination addresses. Finally, it notes the exception to strict rules in paragraph 6 of the said Article in cases of reports that the operators send to HAKOM towards the settlement of relevant disputes between operators and users. This would, according to HAKOM, point to its authority to seek any information from operators that is necessary to establish accuracy of the bill and thus also destination IP addresses.

It is possible that confidentiality of communications and related traffic data could to some extent be overridden in the course of fulfilment of certain operators’ duties, which are prescribed in detail in secondary legislation. These include their duties to implement measures for protecting safety and integrity of networks and services (Article 99 of the Electronic Communications Act and HAKOM’s Ordinance on the manner and deadlines for the implementation of measures for protecting safety and integrity of networks and services, Official Gazette of the Republic of Croatia no. 109/12, 33/13 and 126/13) as well as duties relating to implementation of measures and procedures to suppress abuse and fraud in the provision of electronic mail services (Article 107 (5) – (11) of the Electronic Communications Act and HAKOM’s Ordinance on manner and conditions for prevention and suppression of abuse and fraud in provision of electronic mail services, Official Gazette of the Republic of Croatia no. 42/09).

According to the Croatian Labour Act (Official Gazette of the Republic of Croatia no. 93/14) the employer must consult with the works council before deciding on introducing new technologies and changes in organization and ways of work (Article 150) and this was confirmed in case law with respect to introduction of video surveillance intended to monitor employees (County Court of Zagreb, Gžr 389/2007-2, April 22, 2008). As for surveillance of work communications, according to the publication “Privacy protection in the workplace. Guide for employees” which was developed by the Polish, Czech, Bulgarian and AZOP (http://www.giodo.gov.pl/462/id_art/784/j/en), employers have to notify their employees about surveillance and monitoring of work emails. AZOP provided an opinion as regards surveillance of electronic communications of employees in the workplace (http://www.azop.hr/news.aspx?newsID=281&pageID=25), taking into account Article 29 Working Party’s Working document on the surveillance of electronic communications in the workplace. It must be noted that in this opinion AZOP did not refer to any specific legislation and thus it also did not refer to relevant provisions of the Electronic Communications Act transposing Article 5 (2) of the ePrivacy Directive (the Article 29 Working document to which AZOP refers primarily interprets Directive 95/46/ECC, and it briefly notes also relevance of Directive 97/66/EC
that was later replaced by Directive 2002/58/EC, specifically its Articles 5 and 6). According to AZOP monitoring of electronic communications of employees (content) can only be justified by exceptional circumstances (e.g. security incidents, breach of work duty, disclosure of business information to a competitor, suspected workplace mobbing) and if the value of interest that needs to be preserved with such monitoring and degree of threat to it prevails over the need to protect privacy. AZOP considers that it is not enough to merely prescribe a possibility of monitoring content of electronic communications, e.g. in the employer’s work ordinance, and in respect of which the employees are to provide their consent. Taking into account the particular nature of employment relationship, seeking consent of the employee / potential employee would according to AZOP only constitute a formality, and lack of employees’ real consent could lead to their disadvantage.
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. Automated breaches of confidentiality without human intervention are not expressly addressed by legislation.

b. According to Article 36 of the Constitution of the Republic of Croatia, freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable. Restrictions necessitated by the protection of national security and conduct of criminal prosecution may only be prescribed by law (Constitution of the Republic of Croatia, Official Gazette of the Republic of Croatia no. 85/10 – consolidated text). Furthermore, Croatia ratified the Convention for the Protection of Human Rights and Fundamental Freedoms (relevant fundamental rights guarantees under Article 8 of that Convention, guaranteeing the respect for private life and secrecy of correspondence, as interpreted in practice by the European Court of Human Rights).

The Penal Code (Official Gazette of the Republic of Croatia no. 125/11 and 144/12) prescribes violation of privacy of correspondence and other pieces of mail as a criminal offense in cases “where a person, without authorization, opens a package, letter, telegram, e-mail or any other means of correspondence of another person, or in some other way violates their secrecy, or without authorization keeps, conceals, destroys, delivers to another a person’s closed package or letter, telegram or e-mail or any other means of correspondence (punishment by imprisonment for up to one year). Punishment by imprisonment for up to two years is envisaged for offenses where a person with the aim of acquiring pecuniary gain for him-/herself or for another person, or to inflict damage to another person, communicates to a third person information learned by violation of secrecy of another person’s package, letter, telegram or e-mail or any other means of correspondence, or uses that secret”. Criminal proceedings for these offenses are instituted following a motion (Article 142). Also instituted following a motion are proceedings for a criminal offense of unauthorized audio recording and eavesdropping (Article 143), for which imprisonment of up to three years is envisaged. The offense entails one’s audio recording without authorization the nonpublicly spoken words of another person, or one’s eavesdropping without authorization with specific devices nonpublicly spoken words of another person not intended to him/her, as well as one’s use of those recorded words or making them available to a third person or one’s public pronunciation of those eavesdropped words. It must be noted, especially, that there is no criminal offense if mentioned activities were made in public interest or other interest outweighing the interest of protecting recorded or eavesdropped person’s privacy.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

| a. Article 100 (4) of the Electronic Communications Act stipulates that “the use of electronic communications networks to store information or to gain access to information already stored in the terminal equipment of a subscriber or user shall only be allowed on the condition that the subscriber or user concerned has given his/her consent after having been provided with clear and comprehensive information in accordance with the specific regulations on personal data protection, in particular about the purposes of the processing. This shall not prevent any technical storage of, or access to data for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or, as strictly necessary, in order to provide information society services explicitly requested by the subscriber or user”.

The scope of protection with respect to Article 5 (3) has not been widened in accordance with Directive 2009/136/EC, i.e. Article 100 (4) of the Electronic Communications Act still applies only in cases where access and/or storage is made over the electronic communications network (“the use of electronic communications networks to store information or to gain access to information already stored ...”).

According to its text, this rule applies to all domestic persons/bodies and not only to relevant operators.

The monetary fine prescribed for violation of this rule (misdemeanour) amounts from a minimum of app. 13100-131000 Euros for legal persons, and from 1300 – 6500 Euros for natural persons.

b. Croatian legislation makes no reference to this and does not distinguish between types of cookies and types of devices. |
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

| The subscriber or user concerned needs to give his/her consent after having been provided with clear and comprehensive information in accordance with the specific regulations on personal data protection, in particular about the purposes of the processing - Article 100 (4) of the Electronic Communications Act. The definition of consent in the Electronic Communications Act is autonomous, i.e. it does not refer to the definition of consent in the Personal Data Protection Act, although in substance both definitions contain the requirement of a freely given, express and specific (informed) consent. So far no opinion or regulatory guidance was issued in Croatia on how to meet the informed consent requirement with respect to cookies, including details such as what information needs to be provided (other than information specified in the Personal Data Protection Act). |
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Article 100 (4) of the Electronic Communications Act stipulates that the use of electronic communications networks to store information or to gain access to information already stored in the terminal equipment of a subscriber or user shall only be allowed on the condition that the subscriber or user concerned has given his/her consent after having been provided with clear and comprehensive information in accordance with the specific regulations on personal data protection, in particular about the purposes of the processing. This shall not prevent any technical storage of, or access to data for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or, as strictly necessary, in order to provide information society services explicitly requested by the subscriber or user.

It can be concluded, therefore, that exceptions to the informed consent rule are implemented into the Electronic Communications Act in accordance with the ePrivacy Directive. However, there is no guidance or other interpretation on implementation thereof in practice in Croatia.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

As regards relevant practices of Croatian websites, the general impression of the author of this report (concerning some of the most popular Croatian websites) is that the available notifications on cookies, in website terms and conditions or privacy policies and/or pop-out notices on webpages (which can in most cases easily be clicked away), have improved in relation to previous years. To the best of my knowledge, no study on methods used by website operators to implement the relevant rule has yet been conducted in Croatia; there are no statistics on compliance and no data, statistics or surveys on users’ views, percentage of users refusing or accepting cookies once information and choice has been provided. There have been no enforcement actions against violations of the rules.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

| a. HAKOM and AZOP reported no customer complaints and no supervision (e.g. inspections) upon complaints or by official duty) over compliance of operators with regard to Article 100 (1) – (3) of the Electronic Communications Act. According to its 2008 Annual report, AZOP conducted a supervision in the Croatian telecommunications sector during 2008 and made inquiries from operators as to their practices in protecting personal data of subscribers according to the Telecommunications Act (which was then in force) and the Personal Data Protection Act (http://www.sabor.hr/fgs.axd?id=13950, p. 22). The end-result of this inspection was a general recommendation for all operators to create special procedures for protecting personal data of their subscribers to prevent abuse and to organize educational activities for their employees. As for Article 100 (4) of the Electronic Communications Act (cookie rule), although there were requests for interpretation and guidance on how to meet the legislative requirements, including that of informed consent, so far none have been issued in Croatia. HAKOM received two requests from interested parties on interpretation of the rule and how to implement these in practice, however, no detailed guidance was provided. In its reply HAKOM stated that website owners are obliged to inform users on the existence of cookies in some way. According to HAKOM, the method of implementation is not determined in detail in Croatia, since this is also not prescribed at EU level. Furthermore, it points to AZOP as another authorized body to supervise implementation of Article 100 (4) of the Electronic Communications Act. AZOP received also requests for interpretation of the stated rule. In its reply to one such request it pointed to HAKOM’s authority under the Electronic Communications Act to provide expert opinions and explanations concerning application of this Act and, accordingly, advised the party to seek guidance/opinion from HAKOM. AZOP also noted its right to supervise personal data processing in Croatia pursuant to its authority under the Data Protection Act, as well as under the relevant rules of the Electronic Communications Act. It then reiterated prescribed conditions for providing consent under the Data Protection Act, which are also to be observed when cookies are used. Apart from reiterating the legal requirements and those on the controller’s duty to inform data subjects prior to personal data processing (under the Data Protection Act), it provided no guidance on how to inform and obtain informed consent in practice. |

b. Not available.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

a + b: In my opinion there generally is a lack of awareness on these rules, which is further enhanced by lacking regulatory focus in the area. In support of this I would highlight two critical examples described earlier: a) prescribed duty on operators, in secondary legislation for the Electronic Communications Act, to retain users’ destination IP addresses for bill verification purposes, and b) prescribed exclusion, in the Electronic Communications Act, of all personal data and privacy legislation where lawful interception duties of operators are concerned (contrary to the material scope of application of the Personal Data Protection Act, which also applies in that area, as does the Council of Europe Convention 108 as ratified by Croatia). As for the cookie rule in Article 100 (4) of the Electronic Communications Act, without regulatory attention and guidance on practical implementation of legal requirements the rule is subject to arbitrary interpretation and can easily be ignored, and as such it in my opinion fails to establish the needed legal certainty.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
</table>

The definition of traffic data in the *Electronic Communications Act* is aligned with the ePrivacy Directive, *i.e.* these mean “*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the calculation and billing thereof*” – Article 2 (1) point 55 of the *Electronic Communications Act*. 

2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

According to Article 102 of the Electronic Communications Act:

“(1) Traffic data referring to subscribers or users which have been processed and stored by an operator of the public communications network or publicly available electronic communications services must be erased or made anonymous when they are no longer needed for the purpose of conveyance of communication, except in cases referred to in paragraphs 2, 3 and 5 of this Article, and Article 109, paragraph 3 and paragraph 5, item 4 of this Act.

(2) Traffic data necessary for the purposes of billing for electronic communications services provided to subscribers or users and for interconnection costs may be processed only until the expiry of the statute of limitations on debts in accordance with general legislation on civil obligations.

(3) For the purpose of marketing and sale of electronic communications services or the provision of special tariff services, the operator of publicly available electronic communications services may process the traffic data referred to in paragraph 1 of this Article in the manner and for the duration necessary for marketing and sale or provision of such services, if the subscriber or user to whom the data relate has given his/her prior consent. The subscribers or users may deny or withdraw their prior consent for the processing of traffic data at any time.

(4) The operator must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes referred to in paragraph 2 of this Article, and before obtaining the prior consent of the subscriber or user, of the types of traffic data which are processed and of the duration of such processing for the purposes referred to in paragraph 3 of this Article.

(5) The access to the processing of traffic data in accordance with the provisions of Articles 1, 2, 3 and 4 of this Article shall be restricted to authorised persons of the operators of public communications networks and publicly available electronic communications services handling billing, electronic communications network management, customer complaints, fraud detection, marketing and sale electronic communications services or providing special tariff services. The access to the processing of traffic data must be restricted to actions necessary for the purposes of such activities.

(6) The provisions of paragraphs 1, 2, 3 and 5 of this Article shall not apply to the notification of traffic data to the Ministry, Agency, the competent court and other competent state authorities pursuant to specific regulations for the purpose of resolution of disputes referred to in Articles 20 and 21 of this Act, in particular concerning access and interconnection, or for the purpose of resolution of disputes referred to in Article 51 of this Act.”

Article 102 of the Electronic Communications Act applies, in addition to operators of public communications networks / publicly available electronic communications services, also to providers of special tariff services (concept of ‘special tariff services’ substituted the concept of ‘value added services’ that was earlier in the Act implemented in line with the ePrivacy Directive, as explained in detail under A 3 above). In general the legal requirements in Article 102 of the Electronic
Communications Act correspond to those in Article 6 of the ePrivacy Directive, with certain exceptions. Apart from the difference concerning the definition of the provided services (see above), a minor difference would be the reference in the Electronic Communications Act to the activity of “marketing and sale of electronic communications services” as opposed to Article 6 (3) et seq. of the ePrivacy Directive, which only refers to marketing purposes.

The monetary fines prescribed for violation of this rule (misdemeanour) range from app. 6500 - 65000 Euros for legal persons and from 260 – 2600 Euros for natural persons.

To be noted is also Article 105 of the Electronic Communications Act on nuisance and malicious calls / SMS and MMS messages, which prohibits false representation of callers or senders of SMS messages and MMS messages and according to which users can report receiving such calls/messages to their operators. On the basis of such claims of users operators are obliged to establish the name and surname or company name and address of the end-user from whom such calls or messages originated and to store the data with identification of the caller / sender, date and time of the call or the attempt to establish the call / SMS and MMS messages, and send all this data to the police. No court order is here required.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, please see Article 102 (1) of the <em>Electronic Communications Act</em> above (under C2).</td>
<td></td>
</tr>
<tr>
<td>4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td></td>
</tr>
</tbody>
</table>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

There is no regulatory guidance, nor case law with respect to the implementation of Article 102 of the Electronic Communications Act in Croatia. According to HAKOM and AZOP, there have been no customer complaints and they conducted no interventions in line with their regulatory competencies (see above, under A1 and B9), upon complaints or by official duty, as regards compliance of operators with that provision. With respect to AZOP to be noted here is the earlier mentioned 2008 Annual report according to which it carried out inspections in the Croatian telecommunications sector also with respect to the relevant provisions of the Telecommunications Act, which was at the time in force.

While it did not supervise operators’ compliance with Article 102 of the Electronic Communications Act (transposing Article 6 of the ePrivacy Directive), HAKOM is of the view that operators do not store traffic data for longer than one year, because they are not able to deliver them to HAKOM for the purposes of resolving disputes in accordance with that Act (expiry of the statute of limitations for users in accordance with civil obligations law). Consequently, it considers this as a good indication that the traffic data are being deleted in accordance with requirements stipulated in the stated Article. As for the duty to inform and receive prior consent for the processing of traffic data for marketing purposes, HAKOM considers that the subscribers are informed on this and agree to such actions by signing the overall subscription agreement with the operator. It issued no guidance on what explicit informed consent entails in practice. HAKOM notes also a specific duty of operators pursuant to Article 24 of HAKOM’s Ordinance on manner and conditions for the provision of electronic communications networks and services (secondary legislation for the Electronic Communications Act), which was enacted with the purpose of protecting customers from excessive use, abuse and fraud in the public electronic communications network. It specifies a duty of operators to monitor regular behaviour of end-users during use of public communications services, and warn them as soon as possible of any unusual and sudden increase of costs for public communication services during each particular accounting period. Taking this duty into account it may be possible to interpret such use of customer traffic data as operator’s legal obligation, which presupposes the requirement for it to collect, store and use such traffic data for marketing purposes, i.e. on the basis of the data they could offer customers those tariff packages that would better suit their individual usage habits.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>The definition of location data in Article 2 (1) point 41 of the Electronic Communications Act closely follows the ePrivacy Directive, i.e. they include ‘any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’.</th>
</tr>
</thead>
</table>

2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Article 9 of the ePrivacy Directive is transposed into Article 104 of the *Electronic Communications Act*, as follows:

1. Location data other than traffic data, relating to subscribers or users of public communications networks or publicly available electronic communications services may only be processed when they are made anonymous, or with the prior consent of the subscribers or users in the manner and for the duration necessary for the provision of a special tariff service.

2. The operator must inform the subscriber or user, prior to obtaining their prior consent referred to in paragraph 1 of this Article, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the special tariff service. The subscriber or user shall be given the possibility to withdraw his/her consent for the processing of location data other than traffic data at any time.

3. Where prior consent of the subscribers or users referred to in paragraph 1 of this Article has been obtained, the subscriber or user must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of location data other than traffic data for each connection to an electronic communications network or for each transmission of a communication.

4. Processing of location data other than traffic data in accordance with paragraphs 1, 2 and 3 of this Article shall be restricted to authorised persons of the operators of public communications networks and publicly available electronic communications services, or to authorised persons of a third party providing the special tariff services, and must be restricted to actions necessary for the purpose of providing the special tariff services.

In addition to operators of public communications networks / publicly available electronic communications services, this rule applies also to providers of special tariff services (concept of special tariff services in the Act substituted the previously implemented concept of value added services in line with the ePrivacy Directive, as explained earlier).

With regard to the question who is obliged to provide location data processing information to users and ask for their consent, the text of the relevant rule of the Electronic Communications Act suggests that this would always be operator’s duty.

The monetary fines prescribed for violation of this rule (misdemeanour) range from app. 6500 - 65000 Euros for legal persons, and from 260 – 2600 Euros for natural persons.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

| Article 104 (1) of the *Electronic Communications Act* stipulates that location data other than traffic data, relating to subscribers or users of public communications networks or publicly available electronic communications services may only be processed when they are made anonymous, or with the prior consent of the subscribers or users in the manner and for the duration necessary for the provision of a special tariff service. |
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

There is no case law and no regulatory guidance on the implementation and/or application of location data rules.

   a. Not available. According to HAKOM and AZOP, there have been no customer complaints and they issued no ex officio decisions in line with their regulatory competencies (see above, under A1 and B9), upon complaints or by official duty, as regards compliance of operators with Article 104 of the Electronic Communications Act. With respect to AZOP, the earlier mentioned 2008 Annual report should be noted, which shows it carried out supervision in the Croatian telecommunications sector also with respect to provisions of the Telecommunications Act (which was in force at the time). The end-result was a general recommendation for all operators to create special procedures for protecting personal data of their subscribers to prevent abuse and to organize educational activities for their employees.

   b. Not available.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| Article 104 of the *Electronic Communications Act* is not the focus of regulatory attention and it is potentially ineffective in practice. There is no guidance helping to interpret the requirements of this Article, in particular in relation to providers of location based services. |
E. Unsolicited commercial communications

<table>
<thead>
<tr>
<th>1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the scope and substance of your national implementation</td>
</tr>
<tr>
<td>b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.</td>
</tr>
</tbody>
</table>

a. Article 13 of the ePrivacy Directive has been transposed into Article 107 (1) – (4) of the Electronic Communications Act, as follows:

“(1) The use of automated calling and communications systems without human intervention, facsimile machines or electronic mail, including SMS messages and MMS messages, for the purposes of direct marketing and sale may only be allowed in respect of subscribers or users who have given their prior consent.

(2) Trader, a natural or a legal person, may use details on electronic mail addresses obtained from its customers for the purpose of sale of products or services for direct marketing and sale of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of details on electronic mail addresses when they are collected and on the occasion of receiving any electronic message in case the customer has not initially refused such use of information.

(3) In any event, the practice of sending electronic mail, including SMS messages and MMS messages, for purposes of direct marketing and sale disguising or concealing the identity of the sender on whose behalf an electronic mail or message is sent, and which is contrary to the specific regulations on electronic commerce, as well as sending of electronic mail or messages without a valid electronic mail address or a number to which the recipient may send, free of charge, a request that such communications cease, or electronic mail or messages encouraging the recipients to visit websites which are contrary to the specific regulations on electronic commerce shall be prohibited.

(4) The provisions of paragraphs 1 and 2 of this Article shall not apply to calls made to legal persons for the purposes of direct marketing and sale.”

References to the above mentioned rule on unsolicited communications are also contained in the Electronic Commerce Act and Consumer Protection Act. Article 8 of the Electronic Commerce Act (which implements the E-Commerce Directive), which applies to information society service providers, prescribes that unsolicited electronic communications via email is only allowed with prior consent of the person to whom such communication was intended, in accordance with the law regulating telecommunications (electronic communications). Supervision over implementation of that Act (inspection) has recently been passed from the State Inspectorate to the Inspectorate of the Ministry of Finance - Customs Administration. Monetary fines envisaged in this Act for breaching the unsolicited communications rule are significantly lower than those prescribed in the Electronic Communications Act, ranging from app. 650 – 13100 Euros (legal person), 130 - 1300 Euros (natural person).
According to the new *Consumer Protection Act*, persistent and unwanted communication directed to the consumer via telephone, fax, e-mail or other means of remote communication, except as and to the extent justified by prescribed forced fulfilment of the contractual obligation, represent ‘*aggressive business practices*’ (unfair business practices), which are prohibited. Prescribed monetary fine for traders – legal persons ranges from app. 1300 – 13100 Euros. This provision is without prejudice to rules of that Act or regulations on the restriction or prohibition of use of certain means of distance communication, in certain circumstances, which are in conformity with EU rules (Article 38 (1) point 3, Article 38 (2)). In the area of distance contracts for financial services, the *Consumer Protection Act* introduced in 2014 (implementing Directive 2002/65/EC concerning the distance marketing of consumer financial service) also an explicit reference to the application of the rules on unsolicited electronic communications as prescribed in the law regulating electronic communications i.e. Article 107 of the *Electronic Communications Act* (Article 94 of the Consumer Protection Act). No monetary fine is currently envisaged in the *Consumer Protection Act* for breach of this rule. Supervision over implementation of this Act in Croatia is carried out by market inspectors at the Ministry of Economy.

The *Personal Data Protection Act* has its own marketing provision. According to Article 21 (applying only where personal data, i.e. of natural persons, are used for marketing purposes), the data subject has the right to object to the processing of his/her personal data for marketing purposes, in which case the data cannot be processed. The controller must inform data subjects in advance of any intent to process their personal data for marketing purposes and of their right to object to this.

In addition to the implementation of Article 13 of the ePrivacy Directive in Article 107 (1) – (4) of the *Electronic Communications Act*, the same Article further stipulates also obligations and rights specifically applicable operators providing electronic mail services with respect to their subscribers to: a) filter incoming emails to their subscribers, b) publish email address that users can use in case of abuse and procedures to resolve complains regarding email abuse, c) duty of operators to prohibit to their subscribers in subscriber’s contracts the sending of unsolicited communications and undertake appropriate measures to prevent abuse of e-mail account of their subscriber; d) procedure when the operator establishes that the subscriber sent unsolicited communications or that the subscriber’s e-mail account was abused, which may - depending on the seriousness of abuse - result in an issued warning to the subscriber or temporary disconnection of subscriber’s e-mail account, and in case of continued breach, entitlement of the operator to permanently delete that account and terminate the subscriber’s contract. These rules do not apply to subscribers where it was established that a third party abused the e-mail account, except in cases where the subscriber ignored the operator’s repeated warnings to undertake security measures. Further details are prescribed in secondary legislation, i.e. HAKOM’s *Ordinance on manner and conditions for prevention and suppression of abuse and fraud in provision of electronic mail services* (Official Gazette of the Republic of Croatia no. 42/09).

According to HAKOM also related to the topic of unsolicited communications is the particular procedure prescribed in Article 105 of the *Electronic Communications Act* on ‘*nuisance and malicious calls / SMS and MMS messages*’ that prohibits false representation of callers or senders of SMS messages and MMS messages and according to which users can report receiving such calls/messages to their operators. On the basis of such claims operators are obliged to establish the name and surname or company name and address of the end-user from whom such calls or messages originated and to store the data with identification of the caller / sender, date and time of the call or the attempt to establish the call / SMS and MMS messages, and send all this data to the
police. No court order is required.

b.
SMS and MMS messages are explicitly mentioned in the Article (in the scope of electronic mail messages). This Article has been transposed mainly in line with the ePrivacy Directive, with the exceptions of:

a) 1st and 3rd paragraph: similarly to Article 102, reference is made not only to (direct) marketing but to “direct marketing and sale” purposes. Note: in theory combining ‘sale purpose’ with ‘direct marketing’ could have the effect of lowering the scope of user protection if direct marketing is not considered to always include the (at least immediate) purpose of sale of a commercial product or service, e.g. unsolicited communications could be sent out with the purpose of creating or confirming mailing lists and/or collection of other data from recipients, for future direct marketing activities, for example.;

b) 2nd paragraph: usage of the concept of ‘trader’ (2nd paragraph), who may be a natural or legal person; there is no explicit reference to personal data protection rules;

c) 3rd paragraph: possibly extended scope of prohibited e-mails, incl. SMS and MMS messages pursuant to the Electronic Commerce Act, in relation to Article 13 (4) of the ePrivacy Directive which refers to Article 6 of Directive 2000/31/EC on information to be provided. Namely, prohibition here includes the practice of sending e-mails, incl. SMS and MMS messages for the purpose of ‘direct marketing and sale’ disguising or concealing the identity of the sender on whose behalf an electronic mail or message is sent, ‘and which is contrary to the specific regulations on electronic commerce’, as well as sending of e-mail or messages without a valid e-mail address or a number to which the recipient may send, free of charge, a request that such communications cease, or e-mail or messages encouraging the recipients to visit websites which are contrary to the specific regulations on electronic commerce.

The monetary fines prescribed for breach of this rule (misdemeanour) range from app. 13100-131000 Euros for legal persons, and from 1300 – 6500 Euros for natural persons.

According to the text of the relevant provision, Article 107 (1) - (4) applies to all domestic persons/bodies and thus also to webmail services and location based services, information society service providers (regardless of the fact if they are authorized to provide an electronic communications service or not).
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

According to Article 107 (1) of the *Electronic Communications Act*, the use of automated calling and communications systems without human intervention, facsimile machines or electronic mail, including SMS messages and MMS messages, for the purposes of direct marketing and sale may only be allowed in respect of subscribers or users who have given their prior consent.

With the exception of specified purpose of “direct marketing and sale”, this rule is in line with Article 13 (1) of the ePrivacy Directive, since prior consent of subscribers or users is required for the lawful sending of unsolicited communications via e-mail, including SMS and MMS messages, as well as via automated calling machines and fax. Although it is not explicitly prescribed in the Act, it can be inferred from the text of the rule that opt-in consent would not be required for those communication mechanisms that are not specified in Article 107 (1) of the *Electronic Communications Act*, e.g. non-automated (live) marketing calls and marketing communication by post.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

According to text of the rule (see above, under E1), opt-in consent would not be required for those communication mechanisms that are not specified in Article 107 (1) of the Electronic Communications Act, e.g. non-automated (live) marketing calls and marketing communication by post. It is worth noting that the earlier version of this Article pursuant to the 2008 Electronic Communications Act also covered non-automated calls, however, the requirement of prior consent in such cases was dropped with the 2011 amendment.

As for e-mails, according to Article 107 (2) of the Electronic Communications Act prior consent is not required for cases where traders use e-mail addresses obtained from their customers for the purpose of sale of products or services for direct marketing and sale of their own similar products, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of details on e-mail addresses when they are collected and on the occasion of receiving any electronic message in case the customer has not initially refused such use of information.

Furthermore, according to Article 107 (4) of the Electronic Communications Act prior consent is not required in cases of ‘calls’ made to legal persons for the purposes of direct marketing and sale. In such cases also the exception mentioned above (trader database) does not apply.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The definition of electronic mail in the Electronic Communications Act was transposed in line with the ePrivacy Directive, which means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient. The opt-in consent rule which is applicable to unsolicited communications received via e-mail, expressly incorporates a reference also to SMS and MMS messages.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. Upon complaints of interested parties, regulatory authorities carried out supervision procedures and issued decisions in cases of unwanted communications. A typical example could be found in HAKOM’s decisions in inspection proceedings prohibiting operators of special tariff services to send users promotional SMS messages without their prior consent (e.g. decision from April 7, 2014, class: UP/I-344-07/13-01/111, filing number: 376-04/AM-13-5 (DM) – in Croatian). Namely, users were complaining that they were receiving unsolicited SMS messages from such operators, e.g. claiming they won a certain prize and being asked to enter certain codes in order to collect their award, although they never provided their prior consent for this. According to HAKOM these SMS messages can often indecent and inappropriate, mostly representing marketing for special tariff services, and in some cases also children were receiving them. Before issuing such decisions (before the end of the inspection procedure) HAKOM has in its practice also issued, due to reasonable suspicion that a larger number of users to be exposed to significant harm, provisional measures ordering temporary blockage of incoming and outgoing traffic towards the short codes of operators of special tariff services for customer protection purposes (e.g. decision from December 10, 2013, class UP/I-344-07/13-01/111, filing number 376-04/AM-13-01 (DM) – in Croatian). HAKOM has also introduced a designated email address for users to report such unsolicited communications and conducted inspections on the basis of such complaints. With regard to complaints it is necessary to state the number from which the message was sent, date and time of receipt of the message, name and number of the message recipient, and message content showing that it is marketing - if possible, relevant screen shots could be attached to the complaint.

AZOP mostly received user complains concerning unsolicited communications. In cases where it estimates, upon a users’ complaint, that a breach of Article 107 of the Electronic Communications Act occurred, it cooperates with HAKOM and forwards those complaints to it. This applies to cases of unsolicited emailing, in particular where AZOP finds that the user in question could benefit from special protection on the basis of the earlier mentioned provisions of Article 107 (5) – (6) of the Electronic Communications Act (e-mail filters, procedure for resolving complaints to the operators concerning e-mail abuse).

AZOP provided a number of opinions on the direct marketing provision in the Personal Data Protection Act (Article 21 mentioned above) showing, for example, that AZOP would not take action in cases where unsolicited emails are sent to the company official e-mail address. It would instead advise the parties filing the complaint to ask the sender not to send them such emails any longer, but also instruct them to turn to HAKOM for help with respect to Article 107 (5) – (6) of the Electronic Communications Act. According to replies of AZOP to data subjects on the matter of receiving unwanted e-mails to their personal address, AZOP normally advises such data subjects, where they did not consent to receiving the emails, to ask the email sender that their email address data are no longer used in this way. In cases of repeated sending of such emails they are instructed to file a request to AZOP to establish the violation of rights (under the Personal Data Protection Act). The same applies in cases where data subjects complained about receiving unwanted calls (live, i.e. non-automated). In cases where data subjects - subscribers received unwanted marketing phone
calls (non-automated), even though their number was not kept secret, i.e. withheld from the public directory, AZOP pointed them to check the subscription contract with their operator (if they signed up to receive promotional calls) and if so, to file a request to their operator to remove them from this database. In case they would thereafter again receive such calls, AZOP would instruct them to file a request to establish violation of their rights (under the Data Protection Act).

As for relevant provisions on unsolicited communications in the Electronic Commerce Act and the Consumer Protection Act that refer to the relevant rule on unsolicited communications in the Electronic Communications Act, according to information from competent inspectorates no supervisions have yet been carried out. The relevant new rule in the Consumer Protection Act was recently adopted and no complaints have yet been filed (from consumers - natural persons. Also worth noting here is that, especially taking into account the general scope of application of Article 107 of the Electronic Communications Act, unsolicited communications complaints can always be directed to HAKOM - on the basis of that Act.

b. An example can be found in a decision of the Administrative Court in Zagreb confirming HAKOM’s decision, which found that the content provider of a service “SMS news” violated the provision on unsolicited communications when it was sending mentioned SMS content (messages) without recipients’ prior consent. Originally, the proceedings before HAKOM were initiated upon request of the operator whose subscribers / users were receiving such unsolicited communications. The court rendered its decision according to the older law, but which also required prior consent of the user for the lawful sending of unsolicited SMS messages (promotional). Decision is available at: http://www.hakom.hr/UserDocsImages/2010.g/Odluke/Presuda%20US%20RH%20br.%20Us.11334-nezeljena%20tel.%20priopcenja.pdf (in Croatian). There is also some case law pursuant to the earlier version(s) of the Electronic Communications Act that prohibited non-automated promotional phone calls to users without their prior consent (under the current law only automated phone calls require user’s prior consent).
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Electronic Commerce Act and Consumer Protection Act both refer to legal requirements for unsolicited communications in the Electronic Communications Act, and different bodies are in charge of supervision according to these acts. It is reasonable to expect ongoing efforts towards consistency of practice as regards interpretation of legal requirements of Article 107 (1)–(4) of the Electronic Communications Act and implementation thereof. In my opinion there is a need to redraft and align the various applicable rules, e.g. across different sectors, and sanctions for essentially the same violation of the rule on unsolicited communications, especially taking into account that Article 107 of the Electronic Communications Act applies to all natural and legal persons violating the rules, including information society service providers. By way of example, monetary fines envisaged in the Electronic Communications Act for violation of the rule on unsolicited communications are very strict, amounting from app. 13100-131000 Euros for legal persons, and from 1300 – 6500 Euros for natural persons, whereas the same violation (expressly only in relation to email) committed by an information society service provider pursuant to the Electronic Commerce Act, which refers to the Electronic Communications Act, prescribes a fine for violation of the rule ranging from app. 650 – 13100 Euros (legal person), 130 -1300 Euros (natural person).
COUNTRY REPORT

HUNGARY

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Peter Homoki, senior associate at Ormai és Társai CMS Cameron McKenna LLP Law Firm

Date: 18 August 2014
Contents

Part 1: Management summary ........................................................................................................... 3
Part 2: Answers to the questionnaire .................................................................................................. 4
Part 1: Management summary

Management Summary for Hungary
The transposition of the ePrivacy Directive into Hungarian law can be summarized as follows:

- Implementation is almost complete, however, there are certain discrepancies that stem from the fact that the scope of the ePrivacy Directive is not restricted to the regulation of the telecom sector, which caused some difficulties in implementing cookie related provisions, and a problem in implementing non-location traffic data requirements.

- Article 5.2 of the Directive is implemented only through generic data protection provisions, but not expressly. However, we do not see a major problem with this.

- With regard to cookie rules in Article 5.3, it is implemented in two different bodies of law. The Electronic Communications Act only covers electronic communications service providers, but the more generic E-Commerce Act covers all providers of "information society services". The latter one is generic enough to cover the same scope as the Directive.

- Currently, there is no regulatory or court practice related to the cookie or the non-location traffic data rules, nor legislation more detailed than the Directive.

- The overlap of the spam rules in Directive 2000/31/EC and the ePrivacy Directive is detrimental to the unified regulatory practice as well. Having three different authorities in Hungary that have the power to act in case of a spam, also has a negative effect on the regulatory practice.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

<table>
<thead>
<tr>
<th>Concordance table</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePrivacy Directive</td>
<td>Article 2 a) Section 188 point 26) Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td></td>
<td>Article 2 b) Section 157 (2) of Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td></td>
<td>Article 2 a) Section 188 point 49) of Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td></td>
<td>Article 2 d) Section 159 (6) of Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td></td>
<td>Article 2 g) No definition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 2 i) Section 156 (2) of Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td>Article 3</td>
<td>Section 1 (1) of Act C of 2003 on Electronic Communications Section 1 (1) of Act CVIII of 2001 on Electronic Commerce and on Information Society Services</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a> <a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.266670">http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.266670</a></td>
</tr>
<tr>
<td>Article 5.1</td>
<td>Section 155 (1)-(4) of Act C of 2003 on Electronic Communications</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658">http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.252658</a></td>
</tr>
<tr>
<td>Article 5.2</td>
<td>Implemented more generally by Section 6 (5) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information</td>
<td><a href="http://njt.hu/cgi_bin/njt_doc.cgi?docid=139217.266691">http://njt.hu/cgi_bin/njt_doc.cgi?docid=139217.266691</a></td>
</tr>
<tr>
<td>Article</td>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Article 5.3</strong></td>
<td>Section 155 (4) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 13/A (3) of Act CVIII of 2001 on Electronic Commerce and on Information Society Services</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.1</strong></td>
<td>Section 157 (1) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.2</strong></td>
<td>Section 157 (2)-(3) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.3</strong></td>
<td>Section 157 (4) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.4</strong></td>
<td>Section 15 (1) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 154 (7) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.5</strong></td>
<td>Section 157 (9) and (10) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 6.6</strong></td>
<td>Section 157 (9) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 9.1</strong></td>
<td>Section 156 (13)-(15) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 9.2</strong></td>
<td>Not implemented.</td>
<td></td>
</tr>
<tr>
<td><strong>Article 9.3</strong></td>
<td>Not implemented, but generally the requirements follow from more general data protection rules in Section 10 (1) and (3) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.</td>
<td></td>
</tr>
<tr>
<td><strong>Article 13.1</strong></td>
<td>Section 162 (1) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 13.2</strong></td>
<td>Section 157 (4) of Act C of 2003 on Electronic Communications</td>
<td></td>
</tr>
<tr>
<td><strong>Article 13.3</strong></td>
<td>Section 6 (1) and (4) of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 14 (4)-(6) of Act CVIII of</td>
<td></td>
</tr>
</tbody>
</table>
### 2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Please see the table below for the definitions. We see that the actual scope of the ePrivacy Directive is considerably wider than what would be allowed under Hungarian legislation for electronic communications, and this affects the Hungarian implementation as well.

This difference is palpable regarding the personal scope of the legislation. With some exceptions, the Act C of 2003 on Electronic Communications ("Act") in Hungary sets out obligations mainly for service providers, operators and the national regulatory authority. Regarding users of electronic communications services, the Act and the executive decrees contain provisions only in relation to their relationships with service providers and operators (that is, mainly in relation to subscriber relationships).

The Act and its executive decrees contain no provisions on users’ obligations towards other users. As such, the confidentiality obligation is defined as the obligation of the service provider, and not as an obligation of users towards other users. That is, the Act contains the confidentiality obligations of electronic communications service provider and operators, and confidentiality obligations of other parties are enforced by generic data protection provisions, and also provisions of criminal code etc. – but not the legislation on electronic communications. Confidentiality obligation is effective against everyone, due to protection under e.g. criminal code. For "traffic data (Article 6)", it is sufficient to restrict the implementation to ECS providers and operators.

For "non-traffic data" (Article 9) and maybe for value-added services it is not enough. This approach of legislation is in line with other similar acts in Hungary (e.g. postal rules, energy rules) – sectoral provisions do not contain obligations that seriously affect the conduct of general public, but only provisions that regulate the industry itself (but sectoral provisions do include sectoral specific consumer protection provisions.)

However, the ePrivacy Directive is not using this approach. In the ePrivacy Directive, provisions of confidentiality (Article 5.1), cookie (Article 5.3) and non-traffic location data (Article 9) affect all users, not just providers of electronic communications services and operators of electronic communications networks. E.g. cookies are stored on terminal equipment of subscribers or users not by electronic communications service providers or operators of such network, but by other users (by a specific group of users: operators of websites and other servers accessible through internet).

This legislative approach of implementing certain provisions in "industry specific laws" therefore prevents effective implementation of cookie (Article 5.3) and (non-traffic) location data (Article 9) related provisions of the Directive in the Act, and also provisions that relate to value added services in article 6.3 and 6.5.

Therefore, the above provisions of the Directive are currently not binding the same scope of persons in Hungary as it is provided for in the Directive:

   a) Cookie related provisions are implemented in Section 13/A (3) of Act CVIII of 2001 on Electronic Commerce and on Information Society Services (which originally implemented the E-Commerce Directive 2000/31/EC), as an obligation of providers of "information society services" (http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.266670).

   b) Provisions on "location data other than traffic data" are implemented only when processed by electronic communications service providers. The same is true for value added services data: in the Electronic Communications Act, these provisions only obligate electronic communications service providers.

Considering the wide definition of electronic communications and services, from a regulatory point
of view this opens the "genie's bottle", because in a supposedly industry specific legislation, we start to regulate aspects that are not industry specific. Such an approach could show that in the future, under e-communications industry specific provisions, the legislator could even regulate on what applications people use and how – where the sole regulatory point is that an electronic communications network is used. More bluntly phrased, we could say that such provisions unnecessarily blur the line of regulating the network only vs. regulating the content. (N.B.: Other EU regulatory instruments of the telecom market, e.g. directives 19-22/2002/EC seem to be in line with the "industry specific provisions" only codification approach.)

<table>
<thead>
<tr>
<th>English term</th>
<th>Identifier of Hungarian legal provision</th>
<th>Term in Hungarian and English translation of definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>electronic communications network</td>
<td>Section 188 point 19) of Act C of 2003 on Electronic Communications</td>
<td>elektronikus hírközlő hálózat: ‘Electronic communications network’ shall mean transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals between specific termination points by wire, radio, optical or other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.”’</td>
</tr>
<tr>
<td>operator of electronic communications network</td>
<td>Section 188 point 20) of Act C of 2003 on Electronic Communications</td>
<td>elektronikus hírközlő hálózat üzemeltetője ‘Electronic communications network operator’ shall mean a natural or legal person or unincorporated business association providing or authorized to provide, a public electronic communications network or an associated facility’.</td>
</tr>
<tr>
<td>electronic communications service</td>
<td>Section 188 point 13) of Act C of 2003 on Electronic Communications</td>
<td>elektronikus hírközlési szolgáltatás ‘Electronic communications service’ means a service normally provided for remuneration which consists wholly or mainly in the conveyance and, where applicable, switching or routing of signals on electronic communications networks, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and electronic communications services; furthermore, it does not</td>
</tr>
<tr>
<td>provider of electronic communication services</td>
<td>include information society services, as defined in specific other legislation, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.'</td>
<td></td>
</tr>
<tr>
<td>Section 188 point 14) of Act C of 2003 on Electronic Communications</td>
<td>elektronikus hírközlési szolgáltató 'Provider of electronic communications services' shall mean the operator of an electronic communications network and any natural or legal person engaged in providing electronic communications services.’</td>
<td></td>
</tr>
</tbody>
</table>
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

| VoIP is subject to regulatory provisions as long as the service provider wishes its service to be considered as an electronic communications service. E.g. the service provider may only request assignment of telephone numbers if the service is registered as a communications service with the NRA. The authority practice is that VoIP providers may provide such a service as an over-the-top (OTT) service, which is considered to be an information society service only. As long as they do not use standard ITU numbering resources for accessing endpoints, they do not violate provisions of the Electronic Communications Act (e.g. Skype.) So the ambiguity inherent in the definition of electronic communications services is also present in the Hungarian legislation (actually, even before any harmonization obligations with the European Communities, Hungary had similar problems of giving a proper reasoning why email (including webmail or any other mail user agent) is not subject to the same telecommunications regime, which was also a problem in the USA etc.) Therefore, the remarks about the scope of implementing legislation set out in our response above to question 3 applies to all services that are not electronic communications services, including webmail and location based services that are independent of an electronic communications service. That means that cookie provisions of the Directive are implemented in a way that apply to webmail and location based services providers as well (we presume that they qualify as information society service providers under EU law). However, other provisions of the Directive are implemented by the Electronic Communications Act, and that Act applies only to service providers of electronic communications services. Nevertheless, obligations of confidentiality and other general rules of data protection also apply to service providers of non-ECS VoIP, webmail and location based services, so we can say that these aspects are sufficiently protected, even though they do not fall within the scope of the implementing legislation. |
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

The Electronic Communications Act covers electronic communications activities carried out or directed at the territory of Hungary (Section 1 (1)). The provisions of the Act CVIII of 2001 on Electronic Commerce and on Information Society Services (hereinafter: "E-commerce Act", this is the national law implementing the E-commerce Directive of 2000/31/EC) which implements cookie provisions is applicable to information society services directed at and provided from the territory of Hungary (Section 1 (1)). Cross-border situations have only arisen in relation to the generic act implementing data protection regulation (Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, hereinafter "Data Protection Act"), but those cases were not specific to the E-Privacy Directive, but generic data protection cases. One such case is Weltimmo s.r.o, which is currently before the European Court of Justice waiting for a preliminary decision. It is about a Slovak commercial entity operating a website that advertises only Hungarian real estate and in Hungarian language. The legal issue at stake is whether the Hungarian data protection authority had the powers to fine the operator (for forwarding data of customers publishing advertisements to third parties, including for debt collection, and not providing the possibility to delete the advertisements etc.)

In relation to spam issues, the authority usually terminates procedures when it turns out that foreign parties were involved (i.e. sender of spam is not Hungarian). The reason is that there is a large number of such cases and continuing the procedure would cost too much.

6. Please describe and give references to any form of 'guidance' on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

| a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases) |
| b. national courts through rendering of case law |

There has been no specific guidance or published concrete cases where the definitions were affected (including court case law). (Of course, there have been numerous authority decisions when interpreting the definition of certain types of electronic communications services, but not insofar as is relevant to this report).
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

|   | a. We see that from a theoretical point of view, there is a major problem in the definition of electronic communications services and operators: what is and what is not considered to be electronic communications services? Where is the clear line between an operator of a network and someone that is a service provider? E.g. these are recurring problems as to hotels serving IT services to their guests, or lessors to their lessees, providers of IT network etc. The same problem can be seen in relation to certain computer related services not being considered to be electronic communications services, and also in relation to why OTT providers like Google are not subject to the same regulatory burden and consumer protection regime as "classic" telecom service providers. However, this problem relates to more generally the theoretical underpinning of the telecom regulatory regime (including the roots of liberalisation back in the USA at the time of AT&T divestiture, and also disputes at ITU), and is not a problem that could or should be addressed under the e-Privacy Directive. With regard to the e-Privacy Directive, the main definition/scope problem is related only to Article 5.3 (cookie) and Article 9 (non-traffic location data): these obligations are not dealt with by industry-specific legislation. | b. With regard to the definition of electronic communications services and operators, this problem would need a theoretical recast of the current EU telecom regulatory regime. Should there be any similar undertakings by the Commission, this should be done only based on an international common understanding of what a telecom regulatory regime should be covering and what should remain unregulated. Considering the problems ITU had in reaching such a consensus, it is not a very probable outcome at present. With regard to cookie and location data provisions, these should be put into the generic data protection regulation. |
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Section 155 (1)-(4) of Electronic Communications Act

“(1) Service providers shall take appropriate technical and organizational measures - jointly with other service providers if necessary - in order to block any unauthorized attempt to intercept, store or monitor communications transmitted and any related traffic data and to prevent any unauthorized or accidental access to communications transmitted and any related traffic data (privacy of communications).

(2) Service providers must use in their operations for providing electronic communications services only the type of electronic communications apparatus which have sufficient facilities to ensure the privacy of communications.

(3) Service providers shall be authorized to obtain and store communications transmitted on their network only to the extent absolutely necessary for the provisions of services for technical reasons.

(4) On the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user’s or subscriber’s prior consent granted in possession of clear and comprehensive information about implications.”

"Communications” as a term is defined only in relation to data retention obligations (under Section 159/A), which does not apply to Section 155. It is currently defined as the following in Section 159/A:

“(6) For the purposes of this Section, communication means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service, including unsuccessful call attempts. For the purposes of this Section, this shall not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.”

(Compared to the EU definition, the Hungarian version includes “unsuccessful call attempts” as well.)

In Hungarian, “communications” in Section 159/A. is defined as “kommunikáció”, while Section 155 uses a different Hungarian term, “közlés”. The official Hungarian translation of Article 5.1 of the Directive uses the term “közlés”. Therefore, even if there is a definition of “communications” under Electronic Communications Act, it does not apply to the interpretation of Article 5.1 of the Directive, only to the provisions implementing the Data Retention Directive.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

There is no specific implementation of this provision in sector specific legislation, only the generic rules of the Data Protection Act apply and are used for this purpose:

Section 6 (5) of Data Protection Act: “Where personal data is recorded based on the consent of the data subjects, the controller shall - unless otherwise provided for by law - be able to process the data recorded where this is necessary:

a) for compliance with a legal obligation pertaining to the controller, or
b) for the purposes of legitimate interests pursued by the controller or by a third party, if enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data, without the data subjects further consent, or after the data subject having withdrawn his consent”.

3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Section 155 of the Electronic Communications Act contains a generic reference to these exceptions, two are related to governmental surveillance ((5) and (6) below) and also the "malicious or nuisance calls" exception (as defined by Article 10 of e-Privacy Directive):

“(5) The investigating authorities and the internal affairs division that investigates professional misconduct and criminal acts, and the anti-terrorist organizations defined by the Act on the Police (hereinafter referred to as investigating authorities), and national security agencies may monitor, intercept and store communications by virtue of another act, and the frequency management authorities when exercising their powers conferred under Subsection (3) of Section 11, or may otherwise intrude communication for surveillance purposes.

(6) Service providers shall inform the competent national security agency - with the exception of data disclosure and inspection as specified in Section 42 of Act CXXV of 1995 on National Security Agencies - concerning any request it has received for information relating to the protected telephone numbers of the agencies marked as classified information.

(7) In the event of any alleged threat of murder or physical violence or blackmail, the user or subscriber threatened may authorize in writing the investigating authority to tap into the telephone conversations, electronic communications, e-mail messages and any other form of communications by virtue of the provisions of specific other legislation on his/her end terminal to investigate and to identify the persons involved in such communications within the period of time set in the user’s authorization.”

The specific powers for surveillance and the procedural safeguards are defined in a number of separate acts (including the Criminal Procedure Code, statutory acts for each different bodies etc.) The bodies entitled to surveillance are rather heterogeneous: police (including general police bodies at national and county level, and also special police bodies like the Counter Terrorism Center etc.); the public prosecutor, the National Tax and Customs Authority and the national security services (Constitutional Protection Office, Military National Security Service, Information Office and their technical body, the Special Service for National Security.)
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The first two cases mentioned above would be breaches of confidentiality. Hungarian legislation doesn’t explicitly address “automated breaches of confidentiality without human intervention”. In principle such breaches of confidentiality will be considered as an infringement of private secrets (which includes business secrets etc.) under civil law (Section 2:46 of Act V of 2013 of the Civil Code), infringement of data protection rules (Data Protection Act, including Section 5), criminal law (Breach of Private Secrets and Breach of Correspondence Secrets, Sections 223-224 of Act C of 2012 on the Criminal Code, Section 219 on the misuse of personal data).

The differentiation between traffic data and content date is very clear based on what guarantees there are for governmental surveillance. Criminal protection for correspondence secrets set out above is only available for content data. However, unauthorised access to traffic data on a mass scale would also be a breach of data protection provision that is punishable under criminal law as "misuse of personal data" (but not all misuse of personal data is a crime.)

b. Yes, see our answer a) above.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. There are two different implementing provisions. The Electronic Communications Act only covers electronic communications service providers, but the more generic E-Commerce Act covers all providers of "information society services" (which is generic enough to cover the same scope as the Directive):

Section 155 (4) of Electronic Communications Act:

“On the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user’s or subscriber’s prior consent granted in possession of clear and comprehensive information about implications”.

Section 13/A (3) of E-commerce Act:

“In addition to what is contained in Subsection (2), service providers shall be authorized to process personal data in connection with providing the service, to the extent absolutely necessary for technical reasons. Where all relevant conditions remain unaltered, service providers shall install equipment for the provision of information society services - and operate under all circumstances - with facilities to ensure that the processing of personal data takes place only when it is absolutely necessary for providing the services and to meet the objectives set out in this Act; however, under no circumstances may they exceed the extent required in terms of time and volume”.

b. No, there is no such distinction, and no differentiation as regards the type of device.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

There are no specific provisions in law that address this issue, nor any guidance issued by the authorities concerned (other than the Article 29 Working Party opinion 04/2012, which would also be taken into account by the data protection authority, but so far, no decisions have expressly addressed that question).

There was one opinion issued by the data protection authority in March 2013, that used the word cookie, but this only generally approved the privacy terms of the operator providing information about their cookie use, so this is not relevant in this regard.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

They are implemented by a word-for-word translation of the e-Privacy Directive exemption, see our answer to question 6 above. Other than the one set out in question 6 above, neither of the authorities concerned have issued any opinion or guidance. It is important to note that although the cookie rule is implemented in Hungary by the E-commerce Act, currently there is no competent authority assigned to that rule, so it is only the generic data protection authority that is authorised to act upon any non-compliance. (The National Media and Infocommunications Authority who has powers to act in relation to spam under E-commerce Act does not have the same clear power in relation to cookies.)
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice? Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

There is no practice of compliance with cookie rules. It is usually only multinational companies who have a separate cookie policy or cookie provision in place (due to their mother company having something similar already in place.) Currently, most probably awareness of people with regard to cookie use is not strong enough. There had been no survey and no data regarding cookie acceptance.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Regarding cookies, there are no guidances, interpretations or individual cases.</td>
</tr>
<tr>
<td>b.</td>
<td>None.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. While acknowledging that there is a serious problem with cookies being placed on terminals without giving proper information to the users, my personal view is that regulatory provisions on cookies are premature, and the technical prerequisites that would enable an efficient regulation by law are missing. As long as the different technical purposes for which a website operator may use a cookie is as wide as it currently is, it would be very hard to provide concise and unified regulation of “cookies” as such, while also providing helpful information to users. Even though the rules themselves are clear (together with the opinion of the Article 29 working party), they are not able to make a considerable difference for users. In a large number of cases, operators just show the pop-up cookie acceptance to be on the safe side, and give very generic reasons like "cookies are important for the operation of this website", without any actual information content. Such pop-ups do not contain actual information to the user that would help him to become more informed on what the results of his decisions will be. Most probably the medium is not suitable for this kind of experience, because nobody is really accustomed to this kind of use at the beginning of browsing a webpage.

Personal data of users are generally not at risk due to the operators of these websites: regardless of the proliferation of such sometimes unnecessary "accept my cookies" pop-ups, third parties providing advertisements still quite often placing evercookies on computers without most of the users being aware of that, or even of the existence of these third parties.

As long as the "accept my cookies pop-ups" are not able to give any meaningful information to the users, they are just a nuisance for both users and website operators, and provide a regulatory cost without much benefit.

The problem of cookies and its regulation could more efficiently be handled with a better cooperation between technical measures and regulation. In nascent form, such technical measures are already present within browsers and the “Do Not Track” header information. However, this is not enough, e.g. use of “Do Not Track” is not mandatory, even if we set in a browser that third party cookies are not allowed, the advertisers may fake themselves as first party cookies, or sometimes operators are not able to clearly warn users what functions they are not able to provide without a specific cookie. Having a regulatory background for specific categories of cookies (something similar to the categories of opinion 04/2012) could also help in guiding the practice of advertisers and developers of browser, and could result in having to ask less questions from the users, while at the same time, preserving their freedom of choice. Regardless of the specific technical measures, approvals granted in a predictable and non-obtrusive form, with “deny all” filters for specific categories of cookies seems to be more desirable than the current methods used.

Usefulness of these provisions is also limited in a way similar to that of spam provisions: the lack of efficient enforcement outside the EU. So even if the EU norm for cookies becomes very clear and very strict, e.g. requiring prior approval in the browser similar to prior approval for direct marketing, the formidable problems of enforcement would still persist.

b. Technical standardisation of cookies that can be placed and categorisation of cookies should strongly be enhanced at the international level (W3C, ISO, IEEE etc.) before the current rules on cookies could be improved.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Electronic Communications Act provides a list of traffic data instead of giving a general definition:

“Section 157 (2) Electronic communications service providers shall be authorized to process the following data for subscribers and users for the purposes of billing for calls, collecting the related charges and for keeping the subscriber contracts up to date:

a) the data referred to in Paragraph a) of Subsection (5) of Section 129;
b) the telephone number or other identifier of the subscriber terminal;
c) the address of the subscriber and the type of terminal equipment;
d) total units chargeable for the billing period;
e) calling and called subscriber numbers;
f) the type of calls or other services, their direction, start time, the duration of conversations or the size of data transmitted, the International Mobile Equipment Identity (IMEI) of the network and cell providing the service and of the telephone set used for making use of the service provided in the case of mobile radio telephone networks, and for IP networks the identifiers used;
g) the date of call or other services provided;
h) data connected with the payment of charges or charges in arrears;
i) events of the termination of a subscriber contract if terminated with debts outstanding;
j) data relating to other, non-electronic communications services, in particular to the billing of charges therefor, that may be used by subscribers and users in the case of telephone services;
k) data the service provider has obtained in connection with the unlawful use of subscriber terminal equipment, or any attempt to do so, for accessing subscriber services in the electronic communications network, in particular when such equipment has been barred by its rightful owner.”
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Similarly to the definition, the Hungarian Act lists the type of data that can be processed for the traffic data purpose as well.

With regard to Article 6.5, the Hungarian version does not explicitly provide for ‘fraud detection’, but requires providers of electronic communications services to disclose data to relevant authorities, which may include ‘fraud detection’ as well.

Otherwise, the content is very similar to that of the Directive.

Section 157 (1)-(4) of Electronic Communications Act

“(1) With the exceptions set out in Subsection (2) of this Section and in Subsection (1) of Section 159/A, traffic data relating to subscribers and users processed and stored by the provider of electronic communications services while providing such services must be erased or made anonymous when it is no longer needed.

(2) Electronic communications service providers shall be authorized to process the following data for subscribers and users for the purposes of billing for calls, collecting the related charges and for keeping the subscriber contracts up to date:

a) the data referred to in Paragraph a) of Subsection (5) of Section 129;

b) the telephone number or other identifier of the subscriber terminal;

c) the address of the subscriber and the type of terminal equipment;

d) total units chargeable for the billing period;

e) calling and called subscriber numbers;

f) the type of calls or other services, their direction, start time, the duration of conversations or the size of data transmitted, the International Mobile Equipment Identity (IMEI) of the network and cell providing the service and of the telephone set used for making use of the service provided in the case of mobile radio telephone networks, and for IP networks the identifiers used;

g) the date of call or other services provided;

h) data connected with the payment of charges or charges in arrears;

i) events of the termination of a subscriber contract if terminated with debts outstanding;

j) data relating to other, non-electronic communications services, in particular to the billing of charges therefor, that may be used by subscribers and users in the case of telephone services;

k) data the service provider has obtained in connection with the unlawful use of subscriber terminal equipment, or any attempt to do so, for accessing subscriber services in the electronic communications network, in particular when such equipment has been barred by its rightful owner.

(3) The data referred to in Subsection (2) may be processed for the purposes mentioned in Subsection (2) until the term of limitation established by Subsection (2) of Section 143 for claims arising from subscriber contracts.

(4) Providers of electronic communications services may use the type of data referred to in Subsection (2) for the provision of value added services or for marketing purposes subject to the subscriber’s or user’s prior consent, to the extent necessary for the provision of such services or for marketing purposes. Providers of electronic communications services shall provide the possibility to users or subscribers to withdraw their consent at any time.”
Section 154 (7) of Electronic Communications Act
In addition to the information to be communicated according to the Act on the Right of Informational Self-Determination and on Freedom of Information, service providers shall enable the end-users to have access to information concerning the type of personal data the service provider is processing and the objectives at any time before and during the use of the electronic communications services.

Section 157 (9) of Electronic Communications Act:

“(9) The data referred to in Subsection (2, see traffic data above), to the extent required for the purpose of data processing, may be transferred - within the time limit prescribed in Subsection (3) for retaining data - to:

a) the persons involved in billing operations, management of claims and management of sales, and in client information on behalf of the provider of electronic communications services;

b) the bodies authorized under legal regulation to settle disputes arising in connection with billing and sales;

c) court bailiffs governed by the Act on Judicial Enforcement;

d) the body authorized under specific other legislation to obtain such data if the data subject is unable to give his consent for reasons beyond his control, with a view to protecting the vital interests of the data subject or of another person or in order to prevent or avert any emergency posing significant threat to the life or physical integrity, or the possessions of persons;

e) the consumer protection authority as provided for in the Consumer Protection Act.

(10) Providers of electronic communications services shall be required to disclose or make available the data in their possession according to Subsection (2) upon request made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, to the extent required to discharge their respective duties”. 
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Yes, but only as set out in Section 157 (1) of the Electronic Communications Act as set out in Section 2 above.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

No, there have been no such cases that relevant regulatory authority is aware of.
<table>
<thead>
<tr>
<th>5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?</th>
</tr>
</thead>
<tbody>
<tr>
<td>When similar rules on traffic data were first implemented in 2002 (that was before Hungary joining the EC, so that implementation were not based on the current EU regulatory regime, but the directive 97/66/EC), larger network operators in Hungary have made considerable investments in aligning their accounting systems with the than new rules and more specifically, with a new, sector specific interpretation of more generic data protection rules. Later on, these rules had to be changed in Hungary only slightly. Therefore there had been no major (visible) problems in Hungary in complying with these rules.</td>
</tr>
</tbody>
</table>
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Hungarian rule does not include the word “or by an electronic communications service” and the restriction of the “user” to being a user of a “publicly available” service. But these differences are not material. Also, due to the problems of scope detailed in A/3 above, the Hungarian rule applies only to electronic communications service providers and operators, but the same restriction is not true for the ePrivacy Directive (see Article 9.3).

Section 188 point 49) of Act C of 2003 on Electronic Communications

“‘Location data’ shall mean any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of an electronic communications service.”
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

The Hungarian Act does not have a specific provision that says that “such personal data may only be controlled if they are either anonymized or based on the consent of the user”. There is an express provision that says that the informed consent of the user is required for such controlling, but the option of anonymization is not specifically mentioned as it is done in Article 9.1 of the Directive. (But we see that this is not an important difference, because if the data is anonymized, the data will no longer be personal data.)

Section 156 (13)-(15) of Electronic Communications Act

“(13) Where the provision of a value added service requires that traffic or location data are forwarded, the service provider must inform the subscribers or users concerning the type of data required, the purpose and duration of data processing, and as to whether or not the data is to be disclosed to third persons.

(14) Providers of electronic communications services shall be authorized to process traffic or location data - exclusive of the data processing operations described in Section 158 - only upon the prior consent of the subscribers or users to whom the data are related, and only to the extent and for the duration as it is necessary for the provision of value added services.

(15) Users and subscribers shall have the right to withdraw their consent mentioned in Subsection (14) at any time.”

Article 9.2 is not implemented ("... the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication...") There is a similar provision under Section 156 (15) above: users and subscribers shall have the right to withdraw their consent mentioned in Subsection (14) at any time, but we consider this to be a different provision.

Article 9.3 is only implemented by way of more general requirements of data protection rules in Section 10 (1) and (3) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information:

Section 10 (1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data controller within the scope specified by this Act and other legislation on data processing. The data controller shall be held liable for the legitimacy of his instructions.

(3) The data processor may not make any decision on the merits of data processing and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and
safeguard personal data according to the instructions of the controller.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Yes, but the conditions can be derived from Section 156 (15) (if there is no authorisation to process the data, data processing for that purpose shall cease, based on more generic data protection rules.)
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There have been no guidance or cases on this subject.</td>
</tr>
<tr>
<td>b.</td>
<td>There is no case law on location data.</td>
</tr>
</tbody>
</table>
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| Hungarian law does not sufficiently protect individuals against illegitimate processing of location data because the scope of the implementing act is limited to telecom service providers (operators). |
### E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

<table>
<thead>
<tr>
<th>a. The Hungarian regulation is rather complex. We have one level of protection and regulation at the consumer law level, which is based on advertising rules, and encompasses all commercial communications, regardless of the channel used. This was introduced in 2008, at the time of implementation of Directive 2006/114/EC. However, there was already an existing anti-spam legislation and a wide ranging practice at the NMHH, the electronic communications authority, with special spam related powers based on the implementation of 2000/31/EC Directive. This is still the most experienced authority in relation to the anti-spam fight in Hungary, and most of the cases are published by this authority. They have very good contacts with the telecom service providers, and are able to act upon any spam sent from IPs assigned to Hungarian telecom companies. There is also the general data protection authority (as sending an unsolicited email is also an act of control of personal data). As a result, Hungarian anti-spam regulations are more complex and wider ranging than the e-Privacy Directive and the E-commerce Directive combined.</th>
</tr>
</thead>
</table>
| b. Hungarian rules on spam are more extensive, which is mainly due to the combined approach of three different directives (see a. above). The general prohibition is mentioned by Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, and it contains some more detailed technical rules for the consent (including keeping a registry etc.):

   “(1) Unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as direct marketing), such as through electronic mail or equivalent individual communications - subject to the exception set out in Subsection (4) - , only upon the express prior consent of the person to whom the advertisement is addressed.

   (2) The statement of consent may be made out in any way or form, on condition that it contains the name of the person providing it, and - if the advertisement to which the consent pertains may be disseminated only to persons of a specific age - his place and date of birth, furthermore, any other personal data authorized for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information.

   (3) The statement of consent referred to in Subsection (1) may be withdrawn freely any time, free of charge and without any explanation. In this case all personal data of the person who has provided the statement must be promptly erased from the records mentioned in Subsection (5), and all advertisements mentioned in Subsection (1) must be stopped.

   […]

   (5) Advertisers, advertising service providers and publishers of advertising shall maintain records on the personal data of persons who provided the statement of consent referred to
in Subsection (1) to the extent specified in the statement. The data contained in the aforesaid records - relating to the person to whom the advertisement is addressed - may be processed only for the purpose defined in the statement of consent, until withdrawn, and may be disclosed to third persons subject to the express prior consent of the person affected.

(6) The notice of withdrawal mentioned in Subsection (3) and the notice to unsubscribe as specified in Subsection (4) may be transmitted by way of the postal service or by electronic mail, with facilities to ensure that the person sending the notice is clearly identifiable.

(7) In the advertisement disseminated by way of the means specified in Subsections (1) and (4), a clear and prominent statement shall be inserted to inform the person to whom it is addressed concerning the address and other contact information to which the statement of consent for receiving such advertisement and the aforesaid notice to unsubscribe has to be sent, furthermore - in the case referred to in Subsection (4) - the advertisement material sent on behalf of the same advertiser and addressed to the same person after 1 October 2009 for the first time must contain a return envelope for sending the notice to unsubscribe in the form of registered mail with postage prepaid and with notice of delivery.

(8) The consignment sent for requesting the statement of consent mentioned in Subsection (1) may not contain any advertisement, other than the name and description of the company.”

Regarding other definitions, under the E-commerce Act, the most important term is "electronic advertiser" ("the person on whose behalf the electronic communication is published, or who orders the publication of electronic communication for his own purposes"), but they have joint and several liability with the publisher of electronic communications (who sends the spam), the provider of communications (i.e. creative agency), and also, with the telecom service provider as long as the latter does not provide the address (IP) data required by the authority.

“(6) The electronic advertiser, the provider of communications, and the publisher of electronic communications shall be subject to collective liability for any infringement of the provisions contained in Section 6 of the [advertising rules prohibiting direct comm]. Liability for damages caused by such infringement lies with the electronic advertiser, the provider of electronic communications, and the publisher of electronic communications jointly and severally".
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

There is opt-out only in two cases:

a) for direct (postal) mail; and
b) for providers of electronic communications services to use contact data for their own marketing purposes as defined in Article 13.2.

Prior consent is required for all others, including automated calling systems.

Section 157 (4) of Act C of 2003 on Electronic Communications

“Providers of electronic communications services may use the type of data referred to in Subsection (2) for the provision of value added services or for marketing purposes subject to the subscriber’s or user’s prior consent, to the extent necessary for the provision of such services or for marketing purposes. Providers of electronic communications services shall provide the possibility to users or subscribers to withdraw their consent at any time”.

Section 162 (1) of Act C of 2003 on Electronic Communications

Applying the automated calling system free of any human intervention, or any other automated device for initiating communication with prospective subscribers, for the purposes of direct marketing, information, public-opinion polling and market research in respect of a subscriber shall be subject to the prior consent of the subscriber.

Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities

Section 6 (1):

"Unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as direct marketing), such as through electronic mail or equivalent individual communications - subject to the exception set out in Subsection (4) - only upon the express prior consent of the person to whom the advertisement is addressed."
<table>
<thead>
<tr>
<th>3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, see our answer 2 above.</td>
</tr>
</tbody>
</table>
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

With regard to spam, electronic mail is only indirectly defined by Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities under Section 6 (1):

"Unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as direct marketing), such as through electronic mail or equivalent individual communications - subject to the exception set out in Subsection (4) -, only upon the express prior consent of the person to whom the advertisement is addressed."

This means that the same rules apply to email as for MMS/SMS etc., regardless of channel used (as long as we are talking about electronic communications only.)
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. There are several general guidance documents published:

1. For advertisers:
   a) an FAQ on generic rules on commercial communications in email
      [http://nmhh.hu/cikk/4077/Az_elektronikus_hirdeteskuldes_szabalyai](http://nmhh.hu/cikk/4077/Az_elektronikus_hirdeteskuldes_szabalyai) (all links are in Hungarian):
      E.g. in terms of informed consent, what should the approval contain at a minimum; an explanation of the obligation of entities subject to spam laws to keep a register of persons giving such an approval and to provide access to the content of such registration at the request of the authority etc.
   b) on illegality of certain practices, giving examples of what are illegal
      [http://nmhh.hu/cikk/4089/Az_engedelykero_hozzajarulast_kero_elektronikus_uzenetekrol](http://nmhh.hu/cikk/4089/Az_engedelykero_hozzajarulast_kero_elektronikus_uzenetekrol),
      [http://nmhh.hu/cikk/4094/A_nyilvanos_helyeken_weboldalakon_kozzetett_elektronikus_elerhetos_ekkre_tortenoe_hirdeteskuldesrol](http://nmhh.hu/cikk/4094/A_nyilvanos_helyeken_weboldalakon_kozzetett_elektronikus_elerhetos_ekkre_tortenoe_hirdeteskuldesrol)
   c) on lawful use of "recommending"/"invitation" features of websites
      [http://nmhh.hu/cikk/4094/A_nyilvanos_helyeken_weboldalakon_kozzetett_elektronikus_elerhetos_ekkre_tortenoe_hirdeteskuldesrol](http://nmhh.hu/cikk/4094/A_nyilvanos_helyeken_weboldalakon_kozzetett_elektronikus_elerhetos_ekkre_tortenoe_hirdeteskuldesrol)
   d) on political communications (which are also subject to anti-spam rules)

2. For users (how to submit complaints):
   [http://nmhh.hu/tart/index/1037/Elektronikus_hirdetes](http://nmhh.hu/tart/index/1037/Elektronikus_hirdetes)

3. With regard to decisions, there have been numerous decisions, e.g. in 2012, there were 496 cases initiated (by users reporting or ex officio), with 24 cases ending with a condemnation of the spammer
   in 2013, the same numbers were 479 and 21.
   In 2014, until 27 May, there were 514 cases and 10 convictions.
   (See the annual reports for electronic advertisings at:
   [http://nmhh.hu/tart/index/390/Eves_beszamolok](http://nmhh.hu/tart/index/390/Eves_beszamolok))
   Most of the cases which ended without convictions were terminated due to the IP address used for spam being from a foreign country. (Hungarian telecom service providers do provide IP address data to the regulatory authority.)
   90% of the cases reported concern email, c. 9% are SMS related. No cases on chat, instant messaging or Facebook.
   Most of the spam subjects are related to commercial communications (products, or travel offers, trainings, databases and web-marketing services etc.)
   A list of decisions published is available at
   [http://nmhh.hu/tart/index/210/Ehirdetessel_kapcsolatos_hatarozatok](http://nmhh.hu/tart/index/210/Ehirdetessel_kapcsolatos_hatarozatok)

b. There were court cases, two decided by the supreme court, but these were not specific to certain category of providers or sectors, they were related to generic advertisers (one was advertising his book, the other its websites). Cases are published by the courts, but not freely available on the internet.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| The major problem with the Hungarian regulation is that most of the spam is not coming from Hungary (or even the EU), but from USA and other third party jurisdictions, which makes the spam law ineffective in more than 90% of the cases of spam reported. |
| A second issue is that instead of the three authorities that can act (NMHH, data protection authority and the consumer protection authorities), a single authority should be appointed. This could render the application of spam rules more unified, efficient and more predictable. |
| Case law of the NMHH is very strong, thanks to its powers to request IP data from Hungarian telecom service providers (using the header information of the spam concerned.) |
COUNTRY REPORT

Ireland

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Peter McNally, Spark Legal Network

Date: [ ] September 2014
Contents

Part 1: Management summary .................................................................................................................. 3
Part 2: Answers to the questionnaire ..................................................................................................... 4
Management Summary for Ireland

- In general, the measures transposing the e-privacy directive in Ireland (S.I. 336) reflect closely the provisions in the directive. Most of the definitions are identical to those in the directive, and most of the differences between the transposing regulations and the e-privacy directive are minor and are due to legislative drafting styles.

- Regulatory competence under S.I. 336 is split between ComReg and the Data Protection Commissioner, with the latter being the more relevant to the aspects covered by this study. There is, however, some degree of overlap between their competencies, which is catered for satisfactorily by a memorandum of understanding between the two bodies.

- The Data Protection Commissioner is quite active in providing guidance to users as to their rights but also to undertakings as to how they can ensure compliance. For example, it publishes illustrative case studies commenting on the outcome and noting the important lessons. It also gives guidance on, inter alia, a template to use for ensuring consent to cookies.

- The Irish measures do not deal specifically with new technologies such as VOIP, so the impact of the regulations on these will be a matter for interpretation if or when they arise. However, interestingly, with respect to unsolicited commercial communications, the Irish regulations contain specific provisions regarding communications to mobile phones.

- In general, the Irish regulations transposing the e-privacy directive, together with the regular guidance published the data protection commissioner, are quite clear and satisfactory.
Part 2: Answers to the questionnaire
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- The ePrivacy Directive was transposed into national law by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, S.I. No. 336 of 2011.
  - S.I. No. 336 of 2011
  - Some of the terms used in S.I. No 336 of 2011 rely on definitions provided in S.I. No. 333 of 2011, which transposes the framework directive.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language

b. the English translation of the short name

c. the part or the provision(s) of the ePrivacy Directive it supervises

d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Commissioner</td>
<td>n/a</td>
<td>Investigates and enforces compliance with provisions dealing with:</td>
<td><a href="http://www.dataprotection.ie/viewdoc.asp?DocID=4">http://www.dataprotection.ie/viewdoc.asp?DocID=4</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security of processing (reg 4 of S.I. 336 of 2011);</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Confidentiality of communications (reg 5 of S.I. 336 of 2011);</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Traffic data (reg 6 of S.I. 336 of 2011);</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Location data</td>
<td></td>
</tr>
</tbody>
</table>
other than traffic data (reg 9 of S.I. 336 of 2011);  
- Directories of subscribers (reg 12 of S.I. 336 of 2011);  
- Unsolicited Communications (reg 13 of S.I. 336 of 2011) 
- National directory database (reg 14 of S.I. 336 of 2011); and 
- Internal procedures (to be adopted by providers) where the scope of rights and obligations are restricted (Reg 16(1) of S.I. 336 of 2011)

| Commission for Communications Regulation | ComReg | Subject to the performance by the Data Protection Commissioner of its functions under S.I. 336 of 2011, ComReg monitors compliance and of and issues directions for effective implementation of the following provisions:  
- Itemised billing (reg 7);  
- Presentation and restriction of |
| National Consumer Agency | n/a | ComReg shall, where appropriate, consult and co-operate with the National Consumer Agency on matters of common interest | http://www.consumehelp.ie/ |

Explanation:

- The Data Protection Commissioner is specifically tasked with the protection of privacy and personal data. Thus, it has been assigned functions in relation to those provisions which relate to data protection.
- ComReg is the regulatory body for telecommunications, and is charged with implementing the technical and practical functioning of the regulations. As well as its general function of regulating the spectrum, promoting competition etc, it has a function of protection consumers.
- There is some overlap in terms of sections of the act for which the Data Protection Commissioner and ComReg have competence. However, their roles in relation to these
provisions are slightly different.
- Regulation 33 of S.I. 336 of 2011 requires the Data Protection Commissioner and ComReg to cooperate in relation to the exercise of their functions under the regulations.

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The definition of electronic communications service is provided in the regulation 1 of S.I. 333 of 2011 (which transposes the framework directive). The definition is identical to the definition in the framework directive.

The definition of electronic communications network is provided in the regulation 1 of S.I. 333 of 2011 (which transposes the framework directive). The definition is almost identical to the definition in the framework directive, save for the explicit inclusion of network elements which are not active:

“electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed”.

The provisions of S.I. 336 of 2011 apply to “undertakings”. An undertaking is defined in regulation 1 of S.I. 333 as “a person engaged or intending to engage in the provision of electronic communications networks or services or associated facilities”.

4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its
Regulations apply to “the provision of publicly available electronic communications services in public communications networks” – Reg 3 of S.I. 336 of 2011.

ComReg’s Review of the VOIP Framework, 06/13 states that the definition of electronic communications network in the framework directive should be interpreted to include VOIP.

S.I. 336 of 2011 only applies to processing of personal data “in connection with the provision of publicly available electronic communications services in public communications networks”. Public communications network is defined as an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points. The implication is that while VoIP, webmail and location based services are not explicitly dealt with in the legislation, the test as to whether they fall within the scope of the legislation is whether the provision of such services can be regarded as being the provision of publicly available electronic communications services in an electronic communications network which is used “mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points”. In practice, a court charged with deciding whether or not a particular type of service falls within this definition would listen to input from technical experts in order to decide on a case-by-case basis.

5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

S.I. 336 of 2011 applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications in the State and “where relevant the European Union” – Reg 3 of S.I. 336 of 2011.

Thus, the regulations apply to the provision of publicly available electronic communications networks in the State. It may also apply to those provided elsewhere in the EU “where relevant”. However, the term “where relevant” is not elaborated upon.

In general, Irish law is applicable on the territory of the State, subject to Article 29.8 of the Irish Constitution which provides that State may exercise extra-territorial jurisdiction in accordance
with the generally recognised principles of international law.

In practice, the Irish Data Protection Commissioner occasionally cooperates with authorities in other jurisdictions on the basis of 1981 Council of Europe Convention on Data Protection. An example of this is provided on its website (Case Study 7-98) in relation to unsolicited commercial communications.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. The Data Protection Commissioner has published guidance on its website relating to meaning of “consent” to cookies. For cookie usage, there should be a prominent notice on the homepage informing users about the website’s use of cookies with a link through to a Cookie Statement containing information sufficient to allow users to make informed choices and an option to manage and disable the cookies. Practically, for Irish website operators the following suggestions for minimum compliance with the requirements are set out:

(i) Consent may be obtained explicitly through the use of an opt-in check box which the user can tick if they agree to accept cookies.

(ii) Consent may also be obtained by implication

Not all cookies require consent to be used. These are cookies essential to delivering the service requested by the user - session cookies, authentication cookies (for the duration of the session,) and user security cookies. For example, for storage of items in a shopping cart on an online website advance consent will not be required. This will generally be the case where the cookie is stored only for as long as the "session" is live and will be deleted at the end of the session.

b. It is rare for such cases to come before the national courts, as they are usually settled through dialogue between the data protection commissioner and the party which is alleged to have infringed the regulations, usually instigated on foot of a complaint. However, complaints sometimes lead to prosecution in the courts, and the data protection commissioner records such cases under the Case Study Section of its website along with those case studies which are settled prior to the initiation of court proceedings.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The rules are clear and logically consistent due to the fact that they are very similar to the provisions of the directive, and many of the aspects which need clarifying are clarified by the data protection commissioner.

b. There are no major issues affecting the effectiveness of the legal framework which relate specifically to the Irish transposition. One aspect which could be improved (at EU and national level) is a resolution of the current situation pertaining to the data retention rules concerning traffic data. The current situation sees undertakings under an obligations to simultaneously delete or anonymise data once they are no longer necessary for certain purposes, but to retain them for up to 2 years pursuant to the Communications (Retention of Data) Act 2011.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Article 5.1 of the ePrivacy Directive is transposed by regulation 5(1) and 5(2)(a) of S.I. 336 of 2011. The transposition is almost identical. However, the national provision is expressed as being “without prejudice” to the following national provisions:

- **Section 98 of the Postal and Telecommunications Services Act 1983** – which sets out the offence of intercepting (or attempting or enabling interception) post or telecoms communications, and also certain exceptions, such as in the course of duties (installing cables etc), by a member of police for the purposes of a police investigation, in pursuance of a direction from the minister, or under “other lawful authority”.

- **Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993** – this section allows the minister to authorise an interception for the purpose of a criminal investigation or in the interests of the security of the State.

Communication is defined in regulation 2 of S.I. 336 of 2011. The definition is identical to the definition in the ePrivacy Directive.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Regulation 5(2)(b) transposes this exception verbatim.

There is nothing significant to note in relation to the transposition and substance of this exception in Ireland.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Section 98 of the Postal and Telecommunications Services Act 1983 – which sets out the offence of intercepting (or attempting or enabling interception) post or telecoms communications, and also certain exceptions, such as in the course of duties (installing cables etc), by a member of police for the purposes of a police investigation, in pursuance of a direction from the minister, or under “other lawful authority”.

Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 – this section allows the minister to authorise an interception for the purpose of a criminal investigation or in the interests of the security of the State.

4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

   a. Irish law does not specifically mention automated breaches of confidentiality. Reg 5(1) of S.I. 336 prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is prohibited. The term “person” includes both natural persons (individuals) and persons other than natural persons (companies etc). However, it is likely that in the event of an automated breach, liability would be imputed to the individual or company which controls (or ought to control) or owns the technology which executed the automated breach.

   b. The postal and telecoms legislation mentioned under question 3 (above) relates to the protection of private electronic communications (as well as non-electronic communications) and provides exceptions to confidentiality in certain limited situations.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

<table>
<thead>
<tr>
<th>a.</th>
<th>Regulations 5(3), 5(4) and 5(5) of S.I. 336 transpose the requirements concerning cookies. They reflect the requirements of Art 5.3 of the directive. However, Reg 5(3) fleshes out the term “clear and comprehensive information” by requiring the information to be “both prominently displayed and easily accessible” and stating that such information must include the purposes of the processing. Reg 5(4) deals with the method used for giving consent, and states that it should be as user-friendly as possible. Where technically possible, browser-settings can be used to give consent to cookies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>The Irish legislation does not distinguish between different types of cookies or mention the term “cookies”. Rather, it copies the terms used in the directive. However, the Data Protection Commissioner provides guidance, particularly in relation to 3rd party cookies: “Where third party cookies are being used, it is not sufficient to simply refer the user to third party websites. In such situations or where there are many cookies being created or read by the site (or its partners) we recommend the inclusion in the Cookies Statement of a tabulated explanation of all cookies with the following details: Type; Name; A description of their purpose; Their expiry dates; Links to advertising networks’ opt-out mechanisms for third party cookies.”</td>
</tr>
</tbody>
</table>
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

In relation to consent, Reg 5(3) fleshes out the term “clear and comprehensive information” by requiring the information on which consent is based to be “both prominently displayed and easily accessible” and stating that such information must include the purposes of the processing.

Reg 5(4) deals with the method used for giving consent, and states that it should be as user-friendly as possible. Where technically possible, appropriate browser-settings can be used to give consent to cookies. However, the data protection commissioner gives guidance that the term “appropriate” browser settings does not include default browser settings.

The Data Protection Commissioner has published guidance on its website, indicating that there should be a prominent notice on the homepage informing users about the website's use of cookies with a link through to a Cookie Statement containing information sufficient to allow users to make informed choices and an option to manage and disable the cookies. Practically, for Irish website operators the following suggestions for minimum compliance with the requirements are set out:

(iii) Consent may be obtained explicitly through the use of an opt-in check box which the user can tick if they agree to accept cookies.

(iv) Consent may also be obtained by implication.

7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Regulation 5(5) transposes the two exceptions mentioned.

The data protection commissioner gives guidance that the following cookies are exempt from the
consent requirement: Cookies essential to delivering the service requested by the user - session cookies, authentication cookies (for the duration of the session,) and user security cookies. For example, for storage of items in a shopping cart on an online website advance consent will not be required. This will generally be the case where the cookie is stored only for as long as the "session" is live and will be deleted at the end of the session.

8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

In 2013, the Data Protection Commissioner carried out a “cookie sweep”, where it audited 80 websites. The inspection teams found that there was a reasonably high awareness of, and compliance with, data protection principles in the organisations that were inspected. Notwithstanding this, the majority of organisations had areas where immediate remedial action was necessary. It was noted with satisfaction that the majority of the data controllers audited have demonstrated a willingness to put procedures in place to ensure they are meeting their data protection responsibilities in full.

The cookie sweep also led to a revision of the guidance on the Data Protection Commissioner’s website, which is now quite comprehensive.

9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. As mentioned above (Q5 and Q6) the data protection commissioner has provided quite detailed guidance on cookies, in particular as to how the requirements can be complied
b. We are not aware of any.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>The Irish rules are generally quite clear. They track the provisions of the directive, adding specifics where necessary to protect users. For example the requirement to provide “clear and comprehensive information” about the purposes of processing where cookies are used (Art.5(3) of the directive) is fleshed out in the national provisions by requiring the information on which consent is based to be “both prominently displayed and easily accessible”. This gives an added protection to users.</td>
</tr>
<tr>
<td>b.</td>
<td>The current rules relating to cookies seem to be effective. The regulations are technologically neutral insofar as they do not distinguish between cookies, leaving the data protection commissioner scope to clarify with guidance, allowing for flexibility as the technological situation changes. So far, the only specific type of cookies for which he has given guidance is 3rd party cookies.</td>
</tr>
</tbody>
</table>
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Traffic data” is defined in Regulation 2(2) of S.I. 336. The definition is identical to the definition provided in the directive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation 6 of S.I. 336 transposes the traffic data requirements of the directive. The provisions of regulation are in line with those of Art 6 of the directive.</td>
</tr>
</tbody>
</table>

Regulation 6(1) mentions that the provisions are subject to the Communications (Retention of Data) Act 2011.

In relation to the period for which data can be retained (i.e. the period during which the bill may be lawfully challenged and payment pursued), the Irish regulations set out specifically that if proceedings are brought before the end of this period, the traffic data may be retained until the proceedings are finally determined. “Determined” means either the time limit for appeal expires, the appeal is withdrawn, or the appeal is finally determined.

An interesting point of transposition arises in the case of processing traffic data for the purpose of marketing electronic communications services or for the provision of value added services. Here, the provisions of the transposing regulations are the same as those in the directive, save for the insertion of the words “are informed of” in the national provision:

“An undertaking shall ensure that users and subscribers are informed of and given the possibility to withdraw their consent for processing of traffic data...”

This would seem to place a positive obligation on the undertaking to ensure that the users or subscribers are informed of the possibility to withdraw consent, rather than just requiring them to provide for the possibility. The Data Protection Commissioner’s website confirms this:

“The subscriber must be informed in advance of the types of traffic data to be used, how long it will be used for and be given the possibility to withdraw at any time the consent they may have given for the use of their traffic data. A user must be informed of the means by which they can...”
withdraw their consent.”

3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Regulation 6(1) of SI 336 requires the undertaking to erase traffic data or make it anonymous when it is no longer needed for the purpose of the transmission of a communication.

This is subject to the retention long enough for billing purposes or long enough to allow for any legal proceedings relating to billing.

It is also subject to the requirements of the Communications (Retention of Data) Act 2011, which imposes the obligation on undertakings to retain data.

4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

We are not aware of any such cases.

5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Irish provisions are very similar to what is provided for in the directive. In relation to withdrawal of consent to processing of traffic data, the Irish regulations go further than the directive which requires that users be given the opportunity to withdraw consent at any time, by ensuring that users are “informed of and given the possibility to withdraw their consent”. Thus, the Irish provisions are logically consistent, and contain nothing which contradicts or frustrates the provisions in the directive. However, they insert an extra safeguard to ensure that users are aware of their rights, an essential prerequisite for relying on them.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>Location data is defined in Regulation 2(2) of S.I. 336. The definition is identical to the definition in the directive.</th>
</tr>
</thead>
</table>

2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

<table>
<thead>
<tr>
<th>The legal requirements in the Irish regulations for processing location data other than traffic data are identical to those in Article 9 of the Directive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is an exception, whereby the police (investigating malicious phone calls) or emergency services responding to an emergency can override the decision of a caller to block his caller ID.</td>
</tr>
<tr>
<td>The provision states that “no person shall process location data other than traffic data...unless...”, rather than specifying that “undertakings shall not...”. Thus, the provision applies to third parties harvesting data, or any other person processing location data other than traffic data.</td>
</tr>
</tbody>
</table>

3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>According to regulation 9 of S.I 336, any person processing location data must either anonymise it, or obtain the consent of the user/subscriber. So, if consent is not obtained, it must be anonymised in order to process it. Similarly, if consent is withdrawn, it must be anonymised.</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no provision explicitly requiring deletion of location data. However, the term “processing” includes “keeping” or “storing” the data. Thus, doing nothing actively with the data but allowing it to remain in storage will be classed as processing. So, the data must be anonymised (in the absence of consent), or deleted.</td>
</tr>
</tbody>
</table>
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. The data protection commissioner’s website gives guidance on the rights of users and subscribers in relation to caller ID, such as when they have the right to block their number, and also the circumstances in which this decision to block the number can be overridden.

   b. We are not aware of any.

5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The Irish provisions reflect those in the directive. The exceptions are clear and limited and balance the right to privacy with the user with certain public interested. In addition, the data protection commissioner gives clear guidance on the application of the exceptions to assist users who wish to know the scope and limitations of their rights.
1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. The provisions on unsolicited communications are transposed by Regulation 13 of S.I. 336. The Irish provisions are more detailed than those in Article 13.

   The first interesting point to note is that the Irish provisions prohibit “using or causing to be used” electronic communications networks for certain unsolicited communications.

   The Irish regulations make specific reference to unsolicited communication via calls or SMS to mobile phones. In addition, there are different provisions which apply depending on whether the recipient is a natural, or non-natural person, and also depending on the type of communication (automated call, ordinary telephone call, fax, email).

   Regulation 13(1) provides for a general prohibition where the subscriber or user is a natural person, whereby the communication (whether by automated calling machine, fax, or email) can only be made if the subscriber or user has notified the sender that he or she consents to the communication. Regulation 13(5) prohibits telephone calls to users or subscribers where they have notified the caller that they do not consent, or where they have registered in the National Directory Database (thus the Irish legislation chooses the second option in Art 13(3) of the Directive. Regulation 13(6) provides for opt-in consent in relation to automated and non-automated calls to mobile phones. Regulation 13(8) provides that both the notification and the registration in the National Directory Database are to be free of charge.

   In relation to non-natural persons, Reg 13(3) provides that automated calls or faxes cannot be made where the subscriber notifies that they do not consent, or where the subscriber is registered in the National Directory Database. Reg 13(4) provides that email communication is prohibited where the subscriber or user has notified the sender that they do not consent.

   Regulation 13(2) provides for an exception to the prohibition in Regulation 13(1) in relation to emails where the sender of an email reasonably believes that the email address is used by the user in the context of commercial or official activity.
Art 13(2) of the directive which sets out an exception in relation to existing customers is given effect by Regulation 13(11). However, regulation 13(11)(d) provides a specific time-limit of 12 months.

b. The Irish regulations provide for an exception Reg 13(2) for email communications made to a natural person where the sender reasonably believes the email address is used by the user in the context of a commercial or professional activity.

The Irish regulations are also more precise in giving a time limit of 12 months for the exception regarding communications to existing customers.

In addition, the national regulations specifically address communication to mobile phones.

The national regulations provide protection for non-natural persons in accordance with Art 13(5) of the directive which requires Member States to ensure that “the legislation interests of subscribers other than national persons...are sufficiently protected”.

2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Regulation 13(10) sets out the requirements for sending unsolicited communication.

- In the case of a call, the caller must include the name of the person making the call, and if applicable, the name of the person on whose behalf they are calling;
- In the case of an automated call or fax, the name, address and telephone number of the person making the communication must be provided, and if applicable, the name, address and telephone number of the person who they are representing;
- In the case of email, there must be a valid email address at which the person can be contacted.

Regulation 13(12) prohibits the sending of emails which disguise or conceal the identity of the sender, which encourage recipients to visit certain websites, or which do not have a valid address to which the recipient may send a request for communication to cease.

Regulation 13(1) provides for a general prohibition where the subscriber or user is a natural person, whereby the communication (whether by automated calling machine, fax, or email) can only be made if the subscriber or user has notified the sender that he or she consents to the
Regulation 13(5) prohibits telephone calls to users or subscribers where they have notified the caller that they do not consent, or where they have registered in the National Directory Database (thus the Irish legislation chooses the second option in Art 13(3) of the Directive. Regulation 13(6) provides a similar prohibition in relation to automated and non-automated calls to mobile phones. Regulation 13(8) provides that both the notification and the registration in the National Directory Database are to be free of charge.

As noted under question 1 above, the Irish regulations provide an exception in respect of emails sent to a natural person in the event of a reasonable belief that it was an email address used for commercial or official purposes.

The onus for establishing consent to the communication rests on the person making the communication.

### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Yes.

The opt-in rule applies (pursuant to Reg 13(1) to the following communications methods to natural persons:

- Automated calling machines;
- Fax;
- Email

One such exception is provided in regulation 13(11) dealing with communications to existing customers (the criteria are the same as those in Art 13(2) of the directive, but the time limit is set at 12 months). Another exception is where the sender of an email reasonably believes that the email is destined for an email address which is used for commercial or official activity.

Generally the rule for legal persons is opt-out, which can be done by (1) notifying the person making the communication that they do not consent, or by (2) registering their “opt-out” in the National Directory Database.

The regulations do not distinguish between natural and legal persons in respect of:

- Non-automated telephone calls (opt-in, either by notifying the caller or by registering opt-in with National Directory Database)
- Telephone calls or automated machine calls to mobile phones (opt-in, either by notifying the caller or by registering opt-in with NDD)
- SMS messages (the opt-in must be done by notifying the person making the
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Yes.

For SMS messages, automated calls, faxes and emails to natural persons an opt-in is required. However, the opt-in cannot be effected by registering with the NDD, but only where the person making the communication is notified of the consent by the subscriber. This differs from non-automated phone calls where the subscriber/user is required to “opt-out” by notifying lack of consent to the person making the communication, or by registering opt-out in the NDD.

Interestingly, the definition of electronic mail in the regulations is identical to that in the directive, thus including SMS messages. However, Regulation 13(7) specifically refers to SMS messages.

Electronic mail also covers MMS, text messages, voicemail etc.

5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?


One interesting point is that where a subscriber who has registered an opt-out in the NDD subsequently gives consent, he cannot expect the opt-out to endure. However, it works both ways, and the person making the communication needs to regularly check the NDD
in case the subscriber has re-registered the opt-out since giving the consent. The website also provides links to real case studies dealing with direct marketing via post, email, telephone and fax.

One case study involves direct marketing by tesco to its own internet shopping customers. Regulation 13(11)(c)(ii) allows the customer to opt-out each time a message is sent. Several customers chose to do so by clicking “unsubscribe”, but to no avail. Upon investigation, it was discovered that this was happening due to a flaw in tesco’s manual system of unsubscribing customers. The data protection commissioner uses the case as an example of the positive obligation on direct marketers to ensure that their systems are fit for purpose.

b. We are not aware of any.

6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions generally appear to be consistent. However, the text of the provisions relating to unsolicited communications are far from clear, and reader-friendly, which may confuse the reader as to when the opt-in rule applies and when the opt-out rule applies. Clarity is provided by the data protection commissioner on its website. Notwithstanding this, it is suggested that the rules would be clearer if all the communications requiring opt-in were listed together and if all the communications requiring opt-out were listed together. Alternatively, clarity and simplicity could be provided by requiring opt-in for all communications.

For the perspective of legislative drafting, the definition of email includes SMS. The general prohibition against unsolicited communications at Reg 13(1) of S.I. 336 refers to electronic mail, and requires opt-in. There is an exception in 13(2) where the sender reasonably believes that the email address is used by the recipient in a commercial context. However, Reg 13(7) contains a separate prohibition dealing with SMS, with no such exception applying. This might be inconsistent.

In addition, Reg 13(7) provides for opt-in consent for both natural and legal persons in respect of SMS, whereas for emails to legal persons, consent is opt-out (Reg 13(4)). This is probably due to the scope of Reg 13(70, which goes beyond direct marketing communications to include “an SMS message for a non-marketing purpose which includes information intended for the purpose of direct marketing”.

29
COUNTRY REPORT
ITALY

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Prof. Giusella Finocchiaro – University of Bologna – Studio Legale Finocchiaro

Date: 1.9.2014
Contents

Part 1: Management summary ................................................................. 3

Part 2: Answers to the questionnaire ....................................................... 4
Part 1: Management summary

Management Summary for Italy

- Directive 2002/58/EC has been transposed into Italian legislation by the Personal Data Protection Code as amended by the Legislative Decree (Decreto legislativo or D. Lgs.) of 28 May 2012, n. 69. The transposition is completely in line with the Directive.

- The Legislative Decree of 28 May 2012, n. 69 has modified some of the Data Protection Code provisions and in particular some of the definitions contained in art. 4 of the Code.

- There are no other pieces of legislation implementing the ePrivacy Directive. Therefore the legislation appears to be coherent and homogenous. From a more general perspective, provisions protecting confidentiality are provided by the Italian criminal legislation, as mentioned in the Report, and by the Italian intellectual property law of 22 April 1941, n. 633.

- The implementation of art. 5.3 of the ePrivacy Directive regarding the use of cookies, as amended by Directive 2009/136/EC of 25 November 2009, has brought some changes in practice. Some of the operators are starting to provide the subscribers with comprehensive information in order to collect their consent. Nevertheless, the effectiveness of the legislation is still to be improved.

- The processing of traffic and location data is mostly managed by international operators, who adopt the European standards in their activities. The effectiveness of the legislation on traffic and location data in Italy is slowly evolving, but the process is far from being completed.

- The Italian legislation regarding unsolicited e-mail is complex. It is formally coherent with the requirements imposed by the ePrivacy Directive, but it is not sufficiently effective in practice.

- The Italian legislation on data protection is well framed and ensures that data processing operations are carried out in compliance with the ePrivacy Directive. Nonetheless, the Data Protection Code enforces an extremely complex set of rules and it is characterized by a very formal approach, which not always results in successful application in practice.

- The Italian Data Protection Authority (the competent authority with regard to ePrivacy) has issued many documents (decisions, guidelines, etc.) on ePrivacy issues.
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English

Personal Data Protection Code Legislative Decree no. 196 of 30 June 2003 (as amended by the Legislative Decree of 28 May 2012, n. 69)

- the short title of the law in English

Data Protection Code

- the URL linking to the text of the implementing legislation (if available)

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932 (Data Protection Code in English)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject

- Directive 2002/58/EC has been transposed into Italian legislation by the Personal Data Protection Code (hereafter the “Data Protection Code”) as amended by the Legislative Decree (Decreto legislativo or D. Lgs.) of 28 May 2012, n. 69.
- There are no other pieces of legislation implementing the ePrivacy Directive.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>From a general point of view, the entire Data Protection Code</td>
<td><a href="http://www.garanteprivacy.it/web/guest/home/docweb/-">http://www.garanteprivacy.it/web/guest/home/docweb/-</a></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Art. 122 of the Data Protection Code</td>
<td><a href="http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932">http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932</a></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Art. 126 of the Data Protection Code</td>
<td><a href="http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932">http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932</a></td>
</tr>
</tbody>
</table>

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website
<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autorità Garante per la protezione dei dati personali</td>
<td>Data Protection Authority</td>
<td>All provisions transposed in the Data Protection Code</td>
<td><a href="http://www.garanteprivacy.it">www.garanteprivacy.it</a></td>
</tr>
</tbody>
</table>

- The Italian Data Protection Code is enforced by the Supervisory Authority for Personal Data Protection (*Garante per la Protezione dei Dati Personali*, or *Garante*). The *Garante* maintains a register of databases, conducts audits and enforces the law. The *Garante* can also audit databanks not under its jurisdiction, such as those relating to intelligence activities. Enforcement actions the *Garante* carries out are mainly based on the reaction to complaints lodged by data subjects for failure to exercise their rights (access, rectification, deletion) and on inspection or audit activities that are carried out either *ex officio* (based on an annual action plan identifying specific sectors and/or processing operations) or following complaints and reports. In 2005, the *Garante* issued guidelines on privacy issues related to RFID tags, loyalty cards, digital TV (*e.g.*, pay-per-view) and video-telephoning.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Networks, services and providers which fall within the scope of the legislation are defined in art. 4, par. 2 of the Data Protection Code (as amended by the Legislative Decree of 28 May 2012, n. 69) as follows:

“c) ‘electronic communications network’ shall mean transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or by other electromagnetic means, including satellite networks, fixed (circuit-and packet-switched, including Internet) and mobile terrestrial networks, networks used for radio and television broadcasting, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, and cable television networks, irrespective of the type of information conveyed;

d) ‘public communications network’ networks, including telecommunications services and transmission services in networks used for broadcasting, to the extent that this is provided for in Article 2, letter c) of Directive 2202/21/EC of the European Parliament and of the Council of 7 March 2002”.

There is no a definition of “provider” in the relevant Italian legal framework.

The scope of legislation is not different from the ePrivacy Directive.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

Yes, according to the above cited text of Art. 4, par. 2 of the Data Protection Code, VoIP webmail and location based services fall within the scope of the implementing legislation.

In particular, art. 121 of the Data Protection Code, transposing art. 3 of the ePrivacy Directive, establishes that the provisions relating to the electronic communication services apply to “the processing of personal data in connection with the provision of publicly accessible electronic communication services on public communications networks”. According to art. 4, paragraph 2, under e) of the Data Protection Code, “electronic communications service shall mean a service which consists wholly or mainly in the conveyance of signals on electronic communications networks”. Electronic communications networks are defined in art. 4, paragraph 2, letter c) of the Data Protection Code as transmission systems and switching or routing equipment and other resources which permit the conveyance of signals by fixed and mobile terrestrial networks, including Internet.

The definitions just mentioned are in line with the definitions provided for in article 2 of the ePrivacy Directive. According to Italian law services such as VoIP, webmail and location based services fall within the scope of the Data Protection Code.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

<table>
<thead>
<tr>
<th>Being the scope of legislation defined by the Data Protection Code, art. 5 of the Code applies. It provides as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;1. This Code shall apply to the processing of personal data, including data held abroad, where the processing is performed by any entity established either in the State’s territory or in a place that is under the State’s sovereignty.</td>
</tr>
<tr>
<td>2. This Code shall also apply to the processing of personal data that is performed by an entity established in the territory of a country outside the European Union, where said entity makes use, in connection with the processing, of equipment, whether electronic or otherwise, situated in the State’s territory, unless such equipment is used only for purposes of transit through the territory of the European Union. If this Code applies, the data controller shall designate a representative established in the State’s territory with a view to implementing the provisions concerning processing of personal data.</td>
</tr>
<tr>
<td>3. This Code shall only apply to the processing of personal data carried out by natural persons for exclusively personal purposes if the data are intended for systematic communication or dissemination. The provisions concerning liability and security referred to in Sections 15 and 31 shall apply in any case&quot;.</td>
</tr>
</tbody>
</table>

Therefore the legislation applies to both entities established in Italy, and those from outside the EU who use equipment in Italy, as also provided for in art. 4 of the European Data Protection Directive 95/46/EC of 24 October 1995.

There have been no cases identified which apply this principle.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

<table>
<thead>
<tr>
<th>a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. national courts through rendering of case law</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a. The DPA issued some guidelines regarding the implementation of this legislation. They are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali – (Guidelines concerning the Communication of Personal Data Breaches) Consultazione</td>
</tr>
</tbody>
</table>
Implementing Measures with Regard to the Notification of Personal Data Breaches – 4 April 2013, doc. web n. 2414592, [link](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2414592)

Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies - 8 May 2014, [link](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654)

*Internet: Garante privacy, no ai cookie per profilazione senza consenso* (Internet: DPA, no to cookies without consent) [link](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231)

FAQs on COOKIES, [link](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2146935)

b. No relevant court cases have been identified.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>The rules are consistent. They are part of the Data Protection Code and are homogeneous.</td>
</tr>
<tr>
<td>b.</td>
<td>The rules are also quite complicated. From a more general point of view, the Italian legislation concerning data protection is very complex: the Data Protection Code is constituted of about 200 articles, the DPA has also issued many decisions, many guidelines and many authorisations. This legal framework is extremely focused on formal requirements. For this reason the effectiveness of the Data Protection Code is and will be hard to achieve. The effectiveness of the law could be improved by focusing more the practical aspects and on how to ensure technological security in the data processing.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The principle of confidentiality, from a general point of view, is intrinsic in the Data Protection Code in which the ePrivacy Directive has been implemented.

It is also reaffirmed in art. 32 of the Data Protection Code, providing obligations applying to providers of publicly available electronic communications services.

Art. 32 states: “1. The provider of a publicly available electronic communications service shall take technical and organisational measures under the terms of Section 31 that are adequate in the light of the existing risk, in order to safeguard security of its services and with a view to taking the steps set forth in Section 32-bis hereof, also by way of other entities that have been tasked with delivering the said service.

1-bis. Subject to compliance with the obligations set forth in Sections 30 and 31 hereof, any entity operating on electronic communications networks shall ensure that personal data may only be accessed by authorised personnel for legally authorised purposes.

1-ter. The measures referred to in paragraphs 1 and 1-bis above shall ensure the protection of traffic and location data and of any other personal data stored or transmitted against destruction, whether accidental or not, loss or alteration, whether accidental or not, and unauthorised or unlawful storage, processing, access or disclosure, and they shall also ensure implementation of a security policy.

2. Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force.

3. In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform contracting parties and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1, 1-bis and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards”.

The Data Protection Code formulates a definition of electronic communications in art. 4, paragraph 2, letter a)”electronic communication shall mean any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable or identified subscriber or user receiving the information”.
The definition of “electronic communication” is in Art. 4, par. 2, a) of the Data Protection Code. It provides as follows: “‘electronic communication’ shall mean any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable or identified contracting party or user receiving the information”.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Art. 122, par. 1 of the Data Protection Code provides that “Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with the simplified arrangements mentioned in section 13(3). This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service”.

Art. 123, par. 2 provides that Providers shall be allowed to process traffic data that are strictly necessary for contracting parties’ billing and interconnection payments for a period not in excess of six months in order to provide evidence in case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.

The two articles of the Data Protection Code cited above delineate a specific scope of application, which is in line with art. 5.2 of the ePrivacy Directive. Lawful business practices aiming to provide evidence of a commercial transaction are allowed according to art. 123, paragraph 2 of the Data Protection Code. Additional provisions on the recording of communications and the related traffic data in the field of the employment contracts are contained in the Italian labour legislation. Italian Courts have provided a great number of decisions on the subject. Italian labour law regarding the possibility of monitoring e-mail and telephone correspondence of employees is complex and it is articulated in more than one act (amongst which is the Law of 20 May 1970, n. 300 (Statuto dei lavoratori)).
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Art. 132 of the Data Protection Code provides that “Without prejudice to Section 123(2), telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes”.

Also Art. 46 -49 of the Data Protection code could be relevant, providing exceptions in case of processing operations performed for judicial reasons; Art. 53 -57 of the Data Protection code could be relevant, providing exceptions in case of processing operations performed by the police; Art. 58 of the Data Protection code could be relevant, providing exceptions in case of processing operations performed for the State defence and for security reasons.

In accordance with the above mentioned articles, some principles of the Data Protection Code (as for instance, consent) in particular circumstances do not apply.

Art. 132 on “Traffic Data Retention for Other Purposes” provides that: “The defendant or the person under investigation may directly request the provider to make available the data relating to the subscriptions entered into by his/her client according to the arrangements specified in Section 391-quater of the Criminal Procedure Code without prejudice to the requirements set out in Section 8(2), letter f), with regard to incoming phone calls.

The Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, also in connection with requests lodged by foreign investigating authorities, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties.

Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence”.
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. Art. 4, par. 2, g-bis) of the Data Protection Code provides the following definition of “personal data breach”, as “a security breach leading, accidentally or not, to the destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in the context of the provision of a publicly available communications service”.

There are no specific provisions concerning “automated” data breaches. They would fall under “personal data breaches”.

Art. 32-bis of the Data Protection Code provides obligations applying to providers of publicly available electronic communications services.

Art. 123 and art. 132 of the Data Protection Code specifically deal with traffic data, but they do not address personal data breaches.

In summary, automated breaches of confidentiality are not specifically addressed by national legislation.

b. Long before the ePrivacy Directive was introduced the Italian legislator introduced provisions in the Criminal Code incriminating interception of content of private communications and telecommunications (Law 547 of 23 December 1993).

There are no specific provisions concerning the interception of MAC addresses and the capturing of payload data. The provisions mentioned sub a) and b) would apply. In other words, general provisions on personal data protection and provisions of the Criminal Code on computer crimes would apply.

However, it would be worth also to mention that the Italian Data Protection Authority has recently issued an Act on Mobile Remote Payments, of 22 May 2014 (Provvedimento generale in materia di trattamento dei dati personali nell’ambito dei servizi di mobile remote payment - 22 maggio 2014): http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3161560
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

Art. 122, par. 1 of the Data Protection Code entitled “Information Collected with Regard to Contracting Parties or Users” implements art. 5.3. of the Directive. It provides: “Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with the simplified arrangements mentioned in section 13(3). This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service. In order to determine the simplified arrangements referred to herein, the Garante shall also take account of the proposals put forward by the nationally most representative consumer and industry associations involved in order to also ensure that the mechanisms implemented make the contracting party or user actually aware”.

Summarizing, informed consent is required, unless data is processed only for technical reasons.

b. In the decision issued by the Italian DPA, entitled “Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies” - 8 may 2014, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654 simplified measures on informed consent are provided and the use of banners is allowed. More specifically, the abovementioned decision establishes practical measures on the implementation of the information consent rule. A reasonably sized banner is to be displayed on the screen when the user accesses a home page or any other page of the website. Such banner shall contain information regarding the use of cookies. In particular, it should be mentioned if the website uses profiling cookies to send advertising messages in line with the user's online navigation preferences. It should also be mentioned whether the website allows third parties to send cookies, that on the extended information notice page the user may refuse to consent to the installation of whatever cookies and that if the user continues browsing by accessing any other section or selecting any item on the website (e.g. by clicking a picture or a link), he or she confirms his or her consent to the use of cookies. A link to an extended information notice should also be available on the banner. The extended information notice should give information on the use of technical cookies, on the tools available to select the cookies to be enabled, on the possibility for the user to configure browser settings as a further mechanism to select the preferred use of cookies by the website, including at least a reference to the procedure to be followed to configure those settings.

Implementing these measures will take substantial resources and time. Therefore the DPA considered it appropriate to lay down a one-year implementation term as from publication of the
decision mentioned in the Official Journal.

There is a distinction between technical cookies, profiling cookies, publishers and third parties cookies. Different kinds of information should be given for different types of cookies.

In particular, users' prior consent is not necessary to install technical cookies, whilst information under art. 13 of the Data Protection Code has to be provided. Profiling cookies, used to send advertising messages in line with the preferences shown by the user during navigation, are considered highly invasive. Therefore Italian legislation requires users to be informed appropriately on the use of cookies so that users can give their valid consent. These cookies are referred to in Article 122, paragraph 1 of the Data Protection Code, where it is provided that "Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on the condition that the contracting party or user has given his consent after being informed in accordance with the simplified arrangements mentioned in art. 13”.

As far as cookies of third parties, the above mentioned DPA decision on Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies establishes that publishers are not required to include, on the home page of their websites, any notices relating to the cookies installed by third parties via the publishers' websites. In fact, the DPA considered that a different provision would make the information notice provided by a publisher highly ambiguous and would make it difficult for users to read and understand the information contained in such a notice. Nevertheless the publisher is required to mention that the website allows sending third party cookies, if this is the case.

The Data Protection Code does not make any distinction between the types of device used.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Art. 122, par. 2 of the Data Protection Code provides that “With a view to giving the consent referred to in paragraph 1 above, specific configurations of software or devices may be used that should be user-friendly as well as unambiguous vis-à-vis the contracting party or user”.

In order to simplify the application of the above mentioned provision, the Italian DPA published the following documents:

- Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies - 8 May 2014, [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654). This allows for simplified informed consent and the use of banners.

- FAQs on COOKIES, [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2146935](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2146935). This guidance gives answers to common questions on cookies. It is a document issued for informational purposes.

- In the document Internet: Garante privacy, no ai cookie per profilazione senza consenso [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231) a graphic example of possible banner is included.

The Data Protection Code does not make any distinction between the type of device and / or cookie used.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

In accordance with Art. 122, par.1 of the Data Protection Code the application of the provision requiring consent above cited “(...) shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service”.

This kind of cookies is named “technical cookies” in the above mentioned act issued by the Italian DPA, entitled “Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies” - 8 may 2014, [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654)

Different cookies may require different kinds of information and consent.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

Assessing the compliance and enforcement of cookies rules is currently quite difficult, since we do not have any evidence or statistics about the practical implementation of the new rule.

In my personal experience, consent is sometimes required by international operators (e.g. Google). They use different ways for obtaining the consent in practice. Sometimes a pop-up bar is used and sometimes links are provided. As far as the Italian operators, they often do not apply the new cookie law. The implementation process has just started and it will require a longer period of time in order to be effective.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. As mentioned above, in order to simplify the application of the mentioned provision, the Italian DPA published the following documents:

- Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies - 8 May 2014, [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654)

- FAQs on COOKIES, [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2146935](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2146935)

- In the document *Internet: Garante privacy, no ai cookie per profilazione senza consenso* [http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231](http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231) there is a graphic example of possible banner.

b. We are not aware of national courts decisions on the matter.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>These rules are consistent and appropriate.</td>
</tr>
<tr>
<td>b.</td>
<td>We do not see possible improvements.</td>
</tr>
</tbody>
</table>
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic data is defined by Art. 4, par.2, under h) of the Data Protection Code as follows: “‘traffic data’ shall mean any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”. It is the same definition as the one provided by the Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Art. 123 and art. 132 of the Data Protection Code specifically deal with traffic data.

Art. 123 provides that:

"1. Traffic data relating to contracting parties and users that are processed by the provider of a public communications network or publicly available electronic communications service shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication, subject to paragraphs 2, 3 and 5.

2. Providers shall be allowed to process traffic data that are strictly necessary for contracting parties' billing and interconnection payments for a period not in excess of six months in order to provide evidence in case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 2 to the extent and for the duration necessary for such services or marketing, on condition that the contracting party or user to whom the data relate has given his/her prior consent. Such consent may be withdrawn at any time.

4. In providing the information referred to in Section 13, the service provider shall inform a contracting party or user on the nature of the traffic data processed as well as on duration of the processing for the purposes referred to in paragraphs 2 and 3.

5. Processing of traffic data shall be restricted to persons in charge of the processing who act – pursuant to Section 30 – directly under the authority of the provider of a publicly available electronic communications service or, where applicable, the provider of a public communications network and deal with billing or traffic management, customer enquiries, fraud detection, marketing of electronic communications or the provision of value-added services. Processing shall be restricted to what is absolutely necessary for the purposes of such activities and must allow identification of the person in charge of the processing who accesses the data, also by means of automated interrogation procedures.

6. The Authority for Communications Safeguards may obtain traffic and billing data that are necessary for settling disputes, particularly with regard to interconnection or billing matters.”

This provision is not different from the one in the Directive.

Art. 132 of the Data Protection Code provides that “Without prejudice to Section 123(2), telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the
provider for twelve months as from the date of the communication with a view to the same purposes".
<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</th>
</tr>
</thead>
</table>
| As mentioned above, Art. 123 of the Data Protection Code provides that: “1. Traffic data relating to contracting parties and users that are processed by the provider of a public communications network or publicly available electronic communications service shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication, subject to paragraphs 2, 3 and 5”.
|
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>There are many decisions on this issue by the Italian DPA.</td>
<td></td>
</tr>
<tr>
<td>The Italian Data Protection Authority adopted the act “Security in Telephone And Internet Traffic Data - 17 January 2008”, in <a href="http://garanteprivacy">http://garanteprivacy</a>, doc. web n. 1502599, as amended by Document of 24 July 2008 (doc. web n. 1538224) determining the measures and arrangements to be adopted by providers of electronic communications services. This act provides technical and security measures to be adopted by providers.</td>
<td></td>
</tr>
<tr>
<td>Regarding telephone and Internet traffic data retention, the Italian Data Protection Authority required national providers of communications services to adopt an internal provision indicating the maximum period of data retention (Prescrizione sulla conservazione dei dati di traffico (Wind) (H3G) (Telecom Italia) (Vodafone) - 10 January 2008, in <a href="http://garanteprivacy">http://garanteprivacy</a>, doc. web n. 1484695, n. 1484726, n. 1524263, n. 1484758; see also: “Dati di traffico tic e Internet: no a conservazione illimitata”, 21 October 2009 and 19 November 2009, in <a href="http://garanteprivacy">http://garanteprivacy</a>, doc. web n. 1683093 e n. 1695368.</td>
<td></td>
</tr>
<tr>
<td>In 2011, the Italian Data Protection Authority sanctioned with a fine of 420,000 euro a well-known provider of communication service for not having respected a specific order of the Authority, in relation to the anonymization or the erasure of the data according by art. 132 of the Personal Data Protection Code (Decision of 6 December 2011, in <a href="http://garanteprivacy">http://garanteprivacy</a>, doc. web n. 1885236).</td>
<td></td>
</tr>
</tbody>
</table>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Yes, they are. However they also require relevant investments. In particular, technical measures on anonymisation may require relevant modifications of the information system.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Location data is defined in Art. 4, par. 2, lett. i) of the Data Protection Code as follows: “'location data' shall mean any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service”.

This provision exactly transposes the one in the Directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Art. 126 of the Data Protection Code entitled “Location” Data provides the following.

“1. Location data other than traffic data, relating to users or contracting parties of public communications networks or publicly available electronic communications services, may only be processed when they are made anonymous, or with the prior consent of the users or contracting parties, which may be withdrawn at any time, to the extent and for the duration necessary for the provision of a value added service.

2. The service provider must inform the users or contracting parties, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

3. Where consent of the users or contracting parties has been obtained for the processing of location data other than traffic data, the user or contracting party shall continue to have the possibility, using a simple means and free of charge, of requesting to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

4. Processing of location data other than traffic data in accordance with paragraphs 1, 2 and 3 shall be restricted to persons in charge of the processing acting pursuant to Section 30 under the authority of the provider of the publicly available communications service or, as the case may be, the public communications network or of the third party providing the value added service. Processing shall be restricted to what is necessary for the purposes of providing the value added service and must ensure identification of the persons in charge of the processing that access the data also by means of automated interrogation operations”.

This provision exactly transposes the one in the Directive.

In accordance with the Data Protection Code, users must be informed if data are transmitted to third parties.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Art. 126 of the Data Protection Code entitled “Location” Data, above reported, provides the following.

“1. Location data other than traffic data, relating to users or contracting parties of public communications networks or publicly available electronic communications services, may only be processed when they are made anonymous (...)”.

This is an application of data minimization principle, contained in Art. 3 of the Data Protection Code.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on 'location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. The Italian Data Protection Authority issued a decision concerning a prior checking application submitted by Air Pullman S.p.A. (a company managing public transportation services) in relation to a satellite location system, in http://garanteprivacy, doc. web n. 1672796. This decision allows processing of personal data on “driving patterns” and personal data recorded via the “black box”.

Data processing may be carried out providing that:

- data subjects are provided with detailed explanations on the nature of the processed data and the features of the system by having regard to the different purposes to be achieved;

- access to the processed data is only allowed to persons that have been entrusted therewith by the company and are lawfully entitled to access the data on account of their tasks;

- the data are kept for no longer than necessary to achieve the purposes in question. In particular, location information - after being anonymised as appropriate - may only be processed for monitoring and planning the public transport service as aggregate data;

- the company notifies the processing to the DPA as regards, in particular, location data.

Another decision was adopted by the Italian Data Protection Authority in relation to vehicle geo-location and employer-employee Relations: provision of 4 October 2011, in http://garanteprivacy, doc. web n. 2444921.

In relation to these issues see also the Italian Data Protection Authority, provision of 7 March 2013, in http://garanteprivacy, doc. web n. 2471134, provision of 1 August 2012, in http://garanteprivacy, doc. web n. 1923293, etc., confirming the main principles of informed consent, limited access to personal data, minimisation and notification.

b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| Yes, they are. |
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

<table>
<thead>
<tr>
<th>a. Art. 130 of the Data Protection Code is entitled “Unsolicited Communications”. It provides as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“1. Without prejudice to the provisions made in sections 8 and 21 of legislative decree no. 70 dated 9 April 2003, the use of automated calling or communications systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the contracting party’s or user’s consent.</td>
</tr>
<tr>
<td>2. Paragraph 1 shall also apply to electronic communications performed by e-mail, facsimile, MMS- or SMS-type messages or other means for the purposes referred to therein.</td>
</tr>
<tr>
<td>3. Except as provided for in paragraphs 1 and 2, further communications for the purposes referred to therein as performed by different means shall be allowed in pursuance of Sections 23 and 24 as well as under the terms of paragraph 3-bis below.</td>
</tr>
<tr>
<td>3-bis. By way of derogation from Section 129, processing by telephone and mail of the data referred to in Section 129(1) for the purposes set forth in Section 7(4), letter b., shall be allowed in respect of any entities that have not exercised their right to object, via simplified mechanisms including the use of electronic networks, by having the respective telephone numbers and other personal data as per Section 129(1) entered in a public opt-out register.</td>
</tr>
<tr>
<td>3-ter. The register as per paragraph 3-bis (see below for further information) shall be set up by a decree of the President of the Republic to be adopted in pursuance of section 17(2) of Act no. 400 dated 23 August 1988 following a resolution by the Council of Ministers, after obtaining the opinions of the Council of State and the competent Parliamentary Committees –to be rendered within thirty days of the respective requests—as well as the opinion of the Authority for Communications Safeguards with regard to the issues falling under the latter Authority’s scope of competence—to be rendered within the same deadline; the following general standards and principles shall have to be followed:</td>
</tr>
<tr>
<td>a. the register shall be set up with and managed by a public body and/or organization that has vested competences in this area;</td>
</tr>
<tr>
<td>b. the body and/or organisation in charge for setting up and managing the register shall have to rely on the human resources and tools it holds at its disposal; alternatively, setting up and management of the register may be committed to third parties, which shall undertake to be liable for all the relevant financial and organisational charges, by way of a contract for the supply of services in</td>
</tr>
</tbody>
</table>

accordance with the Code of Public Contracts relating to works, services and supplies as per legislative decree no. 163 dated 12 April 2006.

The entities resorting to the register in order to carry out their communications shall be charged an access tariff based on the actual operational and maintenance costs. The Ministry for Economic Development shall determine the said tariffs by an order;

c. The technical arrangements applying to operation of the register shall be such as to enable every user to request that the respective number be entered in the register via simplified mechanisms including the use of electronic networks and/or the telephone;

d. The technical arrangements applying to operation of and access to the register shall be such as to enable selective queries that should not allow transferring the data contained in the said register, whereby all the operations shall be logged and the access data shall be stored;

e. The timeline and arrangements for entering and updating information in the register shall be set forth, whereby no distinction shall be drawn in terms of industry sector and/or type of commodity, and the maximum period shall be laid down during which the validated data contained in the register may be used; it shall be provided that the data are entered in the register for an indefinite amount of time and may be removed therefrom at any time via simple mechanisms and free of whatever charge;

f. any entities processing data for the purposes mentioned in section 7(4), letter b., shall be required to ensure presentation of calling line identification and provide the appropriate information to users, with particular regard to the possibility and arrangements to have their data entered in the register so as to object to being contacted in future;

g. It shall be provided that inclusion in the register does not prevent processing of the data that have been acquired via other channels and are processed in compliance with sections 23 and 24.

3-quarter. Supervision and control over organisation and operation of the register as per paragraph 3-bis and the relevant data processing operations shall be committed to the Italian data protection authority.

4. Subject to paragraph 1, where a data controller uses, for direct marketing of his/her own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, said data controller may fail to request the data subject’s consent, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications. The data subject shall be informed of the possibility to object to the processing at any time, using simple means and free of charge, both at the time of collecting the data and when sending any communications for the purposes referred to in this paragraph.

5. In any event, the practice of sending communications for the purposes referred to in paragraph 1 or anyhow for promotional purposes by disguising or concealing the identity of the sender, or in breach of section 8 of legislative decree no. 70 dated 9 April 2003, or without a valid address to which the data subject may send a request to exercise the rights referred to in Section 7, or by encouraging recipients to visit websites that contravene the said section 8 of legislative decree no. 70/2003, shall be prohibited.

6. In case of persistent breach of the provisions laid down in this Section, the Garante may also order the provider of electronic communications services, under Section 143(1), letter b), to implement filtering procedures or other practicable measures with regard to the electronic contact details for
electronic mail used for sending the communications”.

This provision is in line with the Directive. It is more detailed than the Directive: it distinguishes different communication means and chooses between the opt-out and opt-in regime depending on the means of communication.

Art. 130 of the Data Protection Code states that data processing may be allowed if prior consent was given. However, this article provides some exceptions. The first exception is the following: the opt-out regime is allowed for processing by telephone and ordinary mail of data contained in directories of contracting parties. An opt-out register is put unto place under the control of the DPA. The second exception concerns the case regulated by Art. 13.2 of the Directive and is completely in line with it.


Par. 2 specifies technical means as for instance e-mail, facsimile, MMS-or SMS-type messages.

Par. 3-bis, 3-ter, 3-quater provide an opt-out regime for processing by telephone and mail (ordinary mail, not email) of data contained in directories of contracting parties. The provision explicitly required the creation of a public opt-out register (“Registro delle opposizioni”). Art. 3-bis and art. 3-ter were implemented by the Presidential Decree (Decreto del Presidente della Repubblica) of 7 September 2010, n. 178. Nevertheless the expected result was not achieved. The public opt-out register is not effective and it is daily criticized by subscribers and operators on the net. More information on the register are available at the following address: http://www.registrodelleopposizioni.it/en

On the same issue, the Consumers’ Code (Legislative Decree n. 206 of 6 September 2005) expressly refers to the Data Protection Code, stating that the Data Protection Code applies.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Legal requirements are provided by Art. 13 of the Data Protection Code, above reported.

As already mentioned, as a general rule informed prior consent is required. However, two exceptions are provided. The first exception is that the opt-out regime is allowed for processing by telephone and ordinary mail of data contained in directories of contracting parties. An opt-out register is put unto place under the control of the DPA. The second exception concerns the use of e-mail in the case regulated by Art. 13.2 of the Directive and it is completely in line with it.

More generally, Art. 130 is completely in line with the Directive. The definitions are the same.

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Yes. The opt-out mechanism applies in case of processing by telephone and mail (ordinary mail, not email) of data contained in directories of contracting parties, as provided by Par. 3-bis, 3-ter, 3-quater of Art. 130.

The opt-out mechanism also applies in the case provided by Par. 4, when a data controller uses, for direct marketing of his/her own products or services, electronic contact details for electronic mail supplied by a data subject in the context of the sale of a product or service, on condition that the services are similar to those that have been the subject of the sale and the data subject, after being adequately informed, does not object to said use either initially or in connection with subsequent communications.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

<table>
<thead>
<tr>
<th>The Data Protection Code mentions different kinds of means. Informed prior consent is required for electronic communications performed by e-mail, facsimile, MMS-or SMS-type messages or other means not expressly mentioned in Art. 130, par. 2.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The opt-out regime applies in case of processing by telephone and mail (ordinary mail, not email) of data contained in directories of contracting parties (Par. 3-bis, 3-ter, 3-quater of Art. 130). The opt-out regime also applies in the case regulated by Art. 13.2 of the Directive and concerns e-mail.</td>
</tr>
<tr>
<td>There are no specific provisions concerning other means of communication such as bluetooth messages, banners, instant messaging, newsfeeds, social media outreach.</td>
</tr>
</tbody>
</table>
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?


The Data Protection Authority with the Provision 18 July 2002 (in http://www.garanteprivacy.it, doc. web n. 1065819) stated that that in case of commercial e-mail sent without informed data subject’s consent, all the personal data must be deleted immediately.

With the general act of 29 May 2003 (in http://www.garanteprivacy.it, doc. web n. 1589969), “Spamming: How to Lawfully Email Advertising Messages”, the Data Protection Authority stated that e-mail addresses contain personal information that must be processed in compliance with the relevant regulations; their use for promotional and/or advertising purposes is only allowed if the data subject has given his or her prior free, specific and informed consent thereto.

The Italian Data Protection Authority, issued a general act on 16 February 2006, entitled “Unsolicited Telephone Services: Enhancing the Safeguards for Citizens” in http://garanteprivacy, doc. web n. 1290.

The Italian DPA also issued other provisions of 30 May (http://garanteprivacy, doc. web n. 1412598, n. 1412586, 1412610), ordering to national providers of electronic communications services to adopt specific measures in order to ensure that promotional calls made only if a specific consent was expressed. See also in relation to data subject’s consent the provision of 29 September 2011, in http://garanteprivacy, doc. web n. 1851415.

b. The “Giudice di pace” of Napoli, 10 of June 2004, in Guida dir., 2004, 32, p. 78, recognized the liability and the consequent damages suffered as a result of spamming; similar decision was taken by “Giudice di pace” of Napoli, 29 of September 2005, in Corr. merito, 2006, 2, p. 169, according to which: “the spamming calls, in addition to violating and disturbing the peace and privacy, causes discomfort, damage and inconvenience, continuous distractions, stress and anxiety. Sms sent daily, even several times a day, offering news and useless content, speculative, promotional, repetitive and annoying, acts to disturb and annoy the user significantly, usurping his time and causing serious personal injury, assets, existential and loss of ‘chance’. So, the injured mature an indisputable right to compensation for any damage suffered, also due to clogging of the memory of the phone that can not receive important messages relating to their social life”.


The decision of the Supreme Court, Criminal Section, of 24 May 2012, n. 23798, in Ced Cassazione 2012, recognizes a potential liability under criminal law by unlawful processing of personal data (art. 167 of the Italian Data Protection Code) as a result of the “spamming”. According to this decision, the crime of unlawful processing of personal data is integrated by an improper use of a database, containing the list of subscribers to a newsletter to which unauthorized advertising messages were sent by another operator.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

These rules are quite complicated. It is quite difficult for operators understand how and why different rules should be applied to different technical means.
COUNTRY REPORT

LITHUANIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Milda Macenaite, Tilburg Institute for Law, Technology and Society (TILT),
Tilburg University, the Netherlands

Date: 18 August, 2014
Contents

Part 1: Management summary ........................................................................................................3
Part 2: Answers to the questionnaire ............................................................................................4
Part 1: Management summary

The transposition of the ePrivacy Directive into Lithuanian law can be summarized as follows:

- Lithuania transposed the provisions of the ePrivacy Directive into Section IX entitled “Processing of Personal Data and Protection of Privacy” of the Law on Electronic Communications in 2004. The supervision and enforcement of this section is carried out by the State Data Protection Inspectorate. The Communications Regulatory Authority, as the national regulator of communications, is the supervisory authority for all the remaining provisions of the Lithuanian Law on Electronic Communications.

- The provisions with regard to the scope of the ePrivacy Directive (the definitions of networks, services, and providers), have been transposed almost literally. Territorially, the Law on Electronic Communications is applicable to electronic communications activities carried out in the Republic of Lithuania (there is no legal requirement of establishment), but such requirement exists according to the Law on Legal Protection of Personal Data for the electronic communications service and network providers to be considered as “data controllers”. As far as application of the Law on Electronic Communications to specific services is concerned, the Communications Regulatory Authority provides guidance and consultations to electronic communication networks and service providers on case by case basis.

- Art. 5.3 of the ePrivacy Directive (about “cookies” etc.) has been more or less literally transposed into Lithuanian law. It generates multiple questions with regard to its application in practice. The State Data Protection Inspectorate issued two public recommendations in order to introduce practical guidelines for data controllers and data subjects in this domain. The recommendation for data controllers is largely based on the early documents of the Art. 29 WP and reflects initial “strict” interpretation of Art 5.3., requiring a freely given, informed and explicit consent. There is no indication of moving towards a lighter regime for cookies, recently chosen by some European DPAs (e.g. the CNIL, the ICO or the Dutch DPA), recognising that consent may result from the Internet user merely continuing to browse the website, once the Internet user is clearly informed about cookies. Despite this strict normative stance, the Inspectorate does not carry out systematic monitoring or enforcement actions in relation to cookies and similar tracking technologies.

- Lithuania has recently changed the transposed rules on traffic and location data. There is no longer a requirement to anonymise such data. Whether or not the rules are applied in practice, is not systematically inspected. There are issues of practical application of rules in relation to the categories of traffic data retained for the purpose of the investigation, detection and prosecution of serious crimes.

- The provisions of the Law on Electronic Communications with regard to unsolicited direct marketing communications are in line with the ePrivacy Directive. The scope of related provisions in addition to subscribers is extended also to “registered users of electronic communication services” (i.e. a person, who is not a subscriber to publicly available electronic communications services, identifiable according to the identification code of the user of electronic communications and information provided at the moment of registration). In 2014, the Inspectorate announced a public consultation on prior consent of the data subject when using electronic communications services for the purposes of direct marketing and clarified that prior explicit consent of the subscriber or user concerned should be obtained before unsolicited communications for direct marketing purposes are addressed to them. This position is in line
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC has been fully transposed into Lithuanian legislation by the Law of 15 April 2004 on Electronic Communications (No. IX-2135)

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article</td>
<td>Description</td>
<td>Law</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valstybinė duomenų apsaugos inspekcija</td>
<td>State Data Protection Inspectorate</td>
<td>Section IX, entitled “Processing of Personal Data and Protection of Privacy” (except provisions of articles 63 (5), 65(4) and 70(7)), of the Law of 15 April 2004 on Electronic Communications. These are provisions on confidentiality, cookies, traffic data, location data, unsolicited communications.</td>
<td><a href="http://www.ada.lt">www.ada.lt</a></td>
</tr>
<tr>
<td>Ryšių reguliavimo tarnyba</td>
<td>Communications Regulatory Authority</td>
<td>All remaining provisions of the Law of 15 April 2004 on Electronic Communications</td>
<td><a href="http://www.rrt.lt">www.rrt.lt</a></td>
</tr>
</tbody>
</table>

Explanation:
- As far as the provisions transposing the ePrivacy Directive are related to privacy and personal data protection, supervision is exercised by the State Data Protection Inspectorate (www.ada.lt).
- The Communications Regulatory Authority of the Republic of Lithuania (hereinafter – RRT) (www.rrt.lt) is, as the national regulator of communications, the supervisory authority for all the remaining provisions of the Lithuanian Law on Electronic Communications.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The scope of the Law on Electronic Communications is the same as in the ePrivacy Directive. Article 3.16 of the Law on Electronic Communications defines **electronic communication network** as:

"transmission systems and (or) switching or routing equipment, other facilities, including passive network elements, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and (or) television broadcasting (re-broadcasting), and cable television and microwave multi-channel distribution system networks, irrespective of the type of information conveyed”.

The difference between the Lithuanian definition of “electronic communications network” and the definition of this concept in the ePrivacy Directive (taken from the Art. 2(a) of the Framework Directive) is the specification of networks used for television broadcasting – cable television, microwave multi-channel television networks.

The law distinguishes between “public” and “non-public” electronic communication networks. The “public communication network” according to Article 3.74 is considered “an electronic communication network that is used entirely or mainly to provide electronic communications services, including network of electronic communications that supports the transfer of information between network connection points”.

Article 3.15 contains a definition of an **electronic communication service**:

“a service normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (re-broadcasting). Electronic communications services exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services and do not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.”

This definition is a taken from the E-Privacy Directive without any modifications.

Article 3.32 of the Law on Electronic Communications further defines the concept of **operator** as “an undertaking providing or authorised to provide a public communications network or an associated facility”.

It is important to note, that the data or activities addressed by the provisions of the ePrivacy Directive involve the processing of personal data. As such the scope of these provisions is also determined by the (scope of the) Law on Legal Protection of Personal Data.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

For a service to be regarded as an “electronic communication service” in the sense of the Lithuanian Law on Electronic Communications, it should consist “wholly or mainly in the conveyance of signals on electronic communications networks”. Electronic communications services exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services and do not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

In practice, in order to apply this provision a particular service provision package should be evaluated and its principal matter should be established. If the emphasis is on content (service is more content-oriented than transport-oriented), the service does not fall under the scope of the law.

The VoIP and webmail services would fall within the scope of the Law on Electronic Communications. Not all location based services will be considered as electronic communication services, for example those services that consist in the conveyance of signals using satellite, like GPS, would be excluded.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

The Law on Electronic Communications is applicable to electronic communications activities carried out in the Republic of Lithuania. In essence, there is no legal requirement of establishment, but in practice foreign entities that carry out electronic communications activities in the Republic of Lithuania normally have an establishment in the territory of Lithuania. However, in case an electronic communications service provider did not have an establishment in Lithuania but still provided services on the Lithuanian territory, in theory the Law on Electronic Communications would be applicable.

In addition, however, the electronic communications service and network providers also have to be considered as “data controllers” under the Lithuanian Law on Legal Protection of Personal Data (transposing the Directive 95/46/EC). Under this regime the Lithuanian data protection rules are applicable to the processing of personal data where:

“1) personal data are processed by a data controller established and operating in the territory of Lithuania, as a part of activities thereof. Where personal data are processed by a branch office or a representative office of a data controller of a Member State of the European Union or another state of the European Economic Area, established and operating in the Republic of Lithuania, such a branch office or representative office shall be bound by the provisions of this Law applicable to the data controller;
2) personal data are processed by a data controller which is established in the territory other than the Republic of Lithuania, but which is bound by the laws of the Republic of Lithuania by virtue of international public law (including diplomatic missions and consular posts);
3) personal data are processed by a data controller established and operating in a country which is not a Member State of the European Union or another state of the European Economic Area (hereinafter referred to as a “third country”), where the data controller uses personal data processing means established in the Republic of Lithuania, with the exception of the cases where such means are used only for transit of data through the territory of the Republic of Lithuania, the European Union or another state of the European Economic Area. In the case laid down in this subparagraph, the data controller must have its representative, that is, an established branch office or a representative office in the Republic of Lithuania which shall be bound by the provisions of this Law applicable to the data controller.” (Law on Legal Protection of Personal Data of 11 June 1996)
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

| a. The Communications Regulatory Authority provides guidance and consultations to electronic communication networks and service providers regarding the geographical and material scope of application of the Law on Electronic Communications on case by case basis. As for the application of the Law on Electronic Communications to specific services, the Communications Regulatory Authority examines in each single case whether the conveyance of signals on electronic communications networks exists, and thus whether the Law on Electronic Communications applies. Sometimes, explanations or public consultations on specific services are published, such as an explanation on how the Law applies to VoIP services (available at http://www.rrt.lt/lt/veikla_23/ukio-subjektu-prieziura/ukio-subjektu-veiklos-qwp9/konsultavimas-del-teises-whk4.html) or pubic consultation on regulatory guidelines for VoIP service providers (available at http://www.rrt.lt/lt/viesosios-konsultacijos/kitos-viesosios-konsultacijos.html).

b. We are not aware of any court cases in Lithuania with regard to the interpretation of the material or geographical scope of the Law on Electronic communications. |
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

| a. | The Law on Electronic Communications uses several different terms to note the user of the electronic communications services (the actual user of the electronic communications services and the registered user of the electronic communications services). The actual user can be considered only a natural person, while the subscriber and the registered user also a legal person. This causes complexity and generates questions in practice as to how the user can be protected in relation to the Law on Legal Protection of Personal Data. The subscriber being a legal person is not protected under the latter law, which aims to safeguard the inviolability of an individual’s private life in the course of processing personal data. |
| b. | Given the complexity in relation to the term “user” mentioned above, this aspect should better be revised or clarified in Lithuania. |
### B. Confidentiality obligations

<table>
<thead>
<tr>
<th><strong>1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?</strong></th>
</tr>
</thead>
</table>

Article 63 entitled “Confidentiality of Communication” in the Law on Electronic Communications states:

> 1. Listening, tapping, storage or other kinds of interception or surveillance of the content of communications and the related traffic data, without the consent of the actual users of electronic communications services, shall be prohibited, except when legally authorised to do so in accordance with Article 66 and 77 of this Law. It shall be prohibited to disclose the content of information transmitted over electronic communications networks and/or related traffic data without the consent of the actual users of electronic communications services or to create conditions for gaining access to such information and/or related traffic data, except cases provided by law.”

Article 3.36 of the Law on Electronic communications defines ‘communication’ as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service”. This does not include any information conveyed as part of a broadcasting service over an electronic communications network except to the extent that constitutes conveyance of the individualised information to the identifiable subscriber or user of public electronic communications.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

| This provision has been transposed in Article 63.2 of the Law on Electronic Communications. |
| "Paragraph 1 of this Article shall not apply to recording of information and related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of conclusion or execution of a commercial contract or other commercial transaction that in accordance with the law can have legal consequences." |
| Before the recording takes place, the actual users of electronic communications services shall be informed about such recording and its purpose. Content of the recorded communications and related traffic data can be stored no longer than the period within which the transaction can be legally contested. |
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The Law on Electronic Communications provide several exceptions to the confidentiality principles:

- the principle of confidentiality does not prevent temporal storage of conveyed communications, which is necessary for the provision of services (e.g. voicemail, electronic mail, etc.) (Art. 61.2)
- the principle of confidentiality does not apply to recording of information and related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of conclusion or execution of a commercial contract or other commercial transaction, that in accordance with the law can have legal consequences. However, there is an obligation to inform the actual user of the electronic communications services about such recording and its purpose before it takes place and to save the recorded information no longer than the period within which the validity of a contract can be disputed (Art. 61.2)
- the confidentiality of radio communication is not breached where a communication has been received as radio disturbances and this is reported to the Communications Regulatory Authority for identification purposes. Radio monitoring conducted by the Communications Regulatory Authority shall not be considered a breach of confidentiality of radio communication. The employees of the Communications Regulatory Authority shall be prohibited from disclosing, disseminating or using the content of non-public radio communications received and reporting about them. (Art. 61.5)

In light of Article 15(1) of the ePrivacy Directive, the following legal provisions allow the law enforcement institutions and courts to break the confidentiality of communications for the purposes of prevention, investigation and detection of crimes.

Pursuant to Article 77 of the Law on Electronic Communications, undertakings providing electronic communications networks and/or services must submit, in accordance with the procedure established by the law, to operational investigation services, pre-trial investigation institutions designated by the Government, prosecutors, courts or judges information which is available to them and which is necessary to prevent, investigate and detect criminal acts. Such information shall be submitted, immediately and free of charge, by undertakings providing electronic communications networks and/or services to the main institutions of operational investigation services and pre-trial investigation institutions designated by the Government in electronic form in response to their enquiries.

Pre-trial investigation institutions designated by the Government shall provide their subdivisions and/or other pre-trial investigation institutions with access to such information in accordance with the procedure established by the Government. All persons taking part in the exchange of information shall make necessary arrangements to ensure data security in accordance with the procedure and conditions set forth by the Government; the additional equipment necessary for this purpose shall be obtained from and maintained by Government funds. If the information presented by an undertaking providing electronic communications networks and/or services needs to be confirmed for a pre-trial investigation purposes, the pre-trial investigation officer shall directly
address the undertaking in writing and the undertaking shall provide a written response.

When information is necessary for the above-mentioned purposes, undertakings providing electronic communications networks and/or services shall, on instruction from an institution (operational investigation service) authorised by the Government, store such information for a longer period than normally allowed by law (6 months from the date of the communication), but no longer than additional six months. Such storage is paid for by state funds in accordance with the procedure established by the Government.

Where there is a reasoned court ruling, undertakings providing electronic communications networks and/or services must provide operational investigation services, in accordance with the procedure established by the law, and pre-trial investigation institutions, in accordance with the procedure established by the Code of Criminal Procedure, with technical possibilities to exercise control over the content of information transmitted by electronic communications networks. Equipment necessary for this purpose shall be obtained from and maintained by Government funds.

A Government authorised institution (operational investigation service) shall organise and provide, in accordance with the procedure established by the Government, each operational investigation service and, in the event of criminal proceedings, each pre-trial investigation institution with a technical opportunity to exercise independent control over the content of information transmitted by electronic communications networks.

According to laws on criminal procedure, search or survey of citizens’ homes, seizure of their property, interception of their correspondence in post or telegraph offices is permissible strictly on the grounds and in the procedures established by law. Article 154 of the Code of Criminal Procedure further specifies the procedure of control, recording and storage of information transmitted via telecommunication networks. Pursuant to Article 154(1) of the Code, the right of a pre-trial investigation officer to intercept telephone conversations and monitor and record other information transmitted via telecommunication networks is conditional on an order issued by a pre-trial judge on a prosecutor’s request, when there are grounds to believe that information obtained in this way may disclose a serious or grave crime planned, committed or being committed, or less serious crimes specified in specific articles of the Criminal Code, or if there is a danger that violence, coercion or other illegal actions may be used against parties to the proceedings or their family members. In cases of extreme urgency, a prosecutor’s order is enough to authorise these actions. In this case, consent of the pre-trial judge must be obtained within three days of the start of such actions. If such consent is not obtained, the actions that have been initiated must be discontinued and all the recordings destroyed without delay. The Law imposes restrictions on the interception of telephone conversations or other information transmitted via telecommunication networks and the duration of such actions. Such actions may not continue more than six months; in exceptional cases, this period may be extended by up to three months and only once (Article 154(3) of the Code of Criminal Procedure)
4. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Lithuanian legislation does not explicitly address “automated breaches of confidentiality without human intervention”. In principle such breaches of confidentiality will be considered as an infringement of Article 61 of the Law on Electronic Communications Law unless they fall under the exceptions provided in Article 77.

The protection of content of the communications and other data (traffic data) are treated differently in Article 154.3 of the Code of Criminal Procedure. The article allows the control and recording of information transmitted via electronic communications networks, except its content, if there is grounds to believe that in such a way it is possible to gather data about non serious crimes, foreseen in specific articles of the Criminal Code.

b. Pursuant to Article 22 of the Constitution of the Republic of Lithuania, the private life of a human beings, personal correspondence, telephone conversations, telegraph messages, and other communications are inviolable. Information concerning the private life of a person may be collected only upon a justified court decision and only according to the law. The law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity.

Article 166 of the Criminal Code foresees responsibility for violation of inviolability of a person’s correspondence. It states:

“1. A person who unlawfully intercepts a postal item or package sent by post or via a provider of courier services or unlawfully intercepts, records or observes a person’s messages transmitted by electronic communications networks or unlawfully records, wiretaps or observes a person’s conversations transmitted by electronic communications networks or otherwise violates inviolability of a person’s correspondence shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two year.

2. A legal entity shall also be held liable for an act provided for in this Article.”

Protection of individuals against unauthorised or unlawful interference in their personal or family life, privacy of home, confidentiality of correspondence, unlawful attempts on their honour and dignity is guaranteed in specialised laws, too, e.g. the Law on Police Activities requires that police officers respect and protect human dignity, enforce and protect human rights and freedoms (Article 21(1)).

In a more general way (without reference to personal data), Article 198 of the Criminal Code criminalises unlawful Interception and Use of Electronic Data. Pursuant to this article “1. A person...
who unlawfully observes, records, intercepts, acquires, stores, appropriates, distributes or otherwise uses the electronic data which may not be made public shall be punished by a fine or by imprisonment for a term of up to four years."
<table>
<thead>
<tr>
<th>5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the scope and substance of your national implementation</td>
</tr>
<tr>
<td>b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a. Article 5.3 of the ePrivacy Directive is implemented in Article 63.4 of the Law on Electronic Communications. It states:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Storage of information, or gaining access to information already stored, in the terminal equipment of a subscriber or an actual user of electronic communication services is only allowed on condition that the subscriber or actual user of electronic communications services concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the Law on Legal Protection of Personal Data, including information about the purposes of the processing. This shall not prevent any technical storage or use of data for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as necessary in order for the provider of an information society service requested by the subscriber or actual user of electronic communication services to provide the service.”</td>
</tr>
</tbody>
</table>

<p>| b. The text of the Article 63.4 quoted above does not distinguish between types of cookies or between categories of end equipment. |</p>
<table>
<thead>
<tr>
<th>6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 63.4 of the Lithuanian Law on Electronic Communications does not contain an answer to these questions and there are no court decisions yet interpreting this provision and applying it to concrete situations. However, in 2011, the Inspectorate issued two public recommendations regarding the use of cookies and similar technologies for data controllers and data subjects (available at: <a href="http://www.ada.lt/images/cms/File/naujienu/slapuk_DV.pdf">http://www.ada.lt/images/cms/File/naujienu/slapuk_DV.pdf</a> and <a href="http://www.ada.lt/images/cms/File/naujienu/slapuk_DS.pdf">http://www.ada.lt/images/cms/File/naujienu/slapuk_DS.pdf</a>). In the recommendation for data controllers, the Inspectorate provides guidance on how to comply with Article 63.4 of the Law on Electronic Communications. As regards specific ways (e.g. pop-up screens or consent bars) to gain user’s or subscriber’s consent, there are no explicit requirements but data controllers are urged to be creative and find the most user-friendly and comfortable ways to do so. Browser setting, consent bars, pop-up windows and registration for a website are examples that the Inspectorate provides for data controllers to obtain consent before the cookie is placed and/or information stored in the user's terminal equipment is collected. Currently browser settings, however, are considered by the Inspectorate as not meeting the requirements for valid consent, and thus is seen more as a future option. The recommendation also foresees which information needs to be provided to users or subscribers before obtaining consent for cookies. In addition to the information specified in Article 24 of the Law on Legal Protection of Personal Data, such information is: information about cookies and data they will collect, and the purpose of such collection; information about the possibility to revoke consent and explanation how to do so; other additional information (e.g. from which sources personal data will be collected, to whom and for what purposes they will be transferred) to the extent necessary to ensure fair personal data processing and respect for the user rights. The recommendation does not differentiate between types of cookies and devices. It does not allow cookies to be placed before an individual provides consent, as consent must be obtained before the cookie is placed and/or information stored in the user's or subscriber’s terminal equipment is collected (prior consent) and informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user or subscriber.</td>
</tr>
</tbody>
</table>
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

According to the public recommendation of the Inspectorate regarding the use of cookies and similar technologies for data controllers, consent is not necessary for “first party” cookies used to sustain technical structure and content of a website, also, for cookies remembering personal preferences in a web shop trolley, SessionID cookies, or other cookies used to provide services requested by the user. Although these cookies do not require consent, there is still the obligation to inform users about their use. Analytics cookies aimed to gather statistical information about the use of the website do not fall under this exception to the informed consent.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The practical implementation of the new rules on cookies is still very diverse. Website operators deploy various consent and notice mechanisms (e.g. often only a notice that various types of cookies are being used by the website, a notice that by using the website, the user agrees to cookies being set by the websites), but often consent – if obtained at all – is not valid under the Law on Legal Protection of Personal Data. Also, often there is a lack of information as to how the users can signify and later withdraw their wishes regarding cookies, no possibilities to choose to accept all or some or decline cookies, or options for the user to subsequently change a prior preference regarding cookies.

In some cases, access to certain websites is made conditional on acceptance of cookies and users do not retain the possibility to continue browsing the website without receiving cookies or by only receiving some of them.

The Inspectorate did not yet conduct on-site and on-line inspections aimed at verifying compliance with the legal requirements in relation to cookies and similar tracking technologies. Until now, it has only touched upon the issue in the context of onlines shops. In 2012, on its own initiative the Inspectorate carried out preventive inspections in selected 23 online shops. Amongst other provisions, compliance with the cookie provision (Article 61.4 of the Law on Electronic Communications) among online shopping service providers was inspected. It was concluded that 22 from 23 inspected online shops gathered the data of their users, including their personal data, via cookies without providing them clear and comprehensive information about the use of cookies and their purposes, as well as without obtaining prior consent to place a cookie on the user’s terminal equipment. The Inspectorate required to terminate the indicated violations by issuing orders to all the 22 online shops.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

| a. The Inspectorate issued two public recommendations regarding the use of cookies and similar technologies for data controllers and data subjects (available at: http://www.ada.lt/images/cms/File/naujienu/slapuk_DV.pdf and http://www.ada.lt/images/cms/File/naujienu/slapuk_DS.pdf). In the recommendation for data controllers, the Inspectorate provides some (not very comprehensive) guidance on how to comply with Article 63.4 of the Law on Electronic Communications. The recommendation is a welcomed first step, but lacks more detailed practical guidelines on how to apply the rules with regard to the use of cookies on various devices and in various circumstances. The recommendation – 5 pages – builds on the Article 29 WP Opinion 2/2010 on online behavioural advertising, and does not take into account more recent documents (Article 29 Working Party Working Document 02/2013 providing guidance on obtaining consent for cookies, and Opinion 04/2012 on Cookie Consent Exemption). The recommendation for data subjects provides advices for the users of electronic communication services in relation to cookies (how to set browser settings and to control/delete cookies). |
| b. Not available. |
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

a. Without additional detailed guidance of the Inspectorate the provisions of the Lithuanian legislation transposing Art. 5.3 of the ePrivacy Directive are too vague to allow a consistent application in practice by service providers. Before the Inspectorate has taken a position and explained some of the concrete cookie use cases and consent mechanisms, many parties in the industry were confused and did not know how to implement the rules. However, even after the explanation, there is still no certainty as to whether or not a particular solution implemented by the website operator fulfils all the requirements for valid consent.
Moreover, it is not clear what is considered as “necessary in order for the provider of an information society service requested by the subscriber or actual user of the electronic communication services to provide the service”. Lithuanian implementation eliminates the word “strictly” necessary, as present in Article 5.3 of the ePrivacy Directive, and thus, formally does not explicitly require storage of or access to information to be essential, for this exemption to apply. This causes additional uncertainty. Several categories, such as “shopping basket” cookies on a merchant website, session ID cookies for the term of the session are mentioned by the Inspectorate as falling under the consent exemption, but the Inspectorate’s position in relation to other types of cookies (e.g. authentication cookies, multimedia player session cookies, load balancing cookies and persistent user interface customization cookies) is not very clear.

b. Effectiveness can be improved through more detailed guidance and better enforcement (inspections carried out by the Inspectorate and fines for non-compliance) by the Inspectorate.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Article 3.57 of the Law on Electronic Communications defines traffic data as “data processed for the purpose of the conveyance of a communication on an electronic communications network and (or) for the billing thereof”. The definition is the same as in the ePrivacy Directive.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Articles 65-67 of the Law on Electronic Communications foresee the following requirements for public communications network and (or) service providers for the lawful processing of traffic (and location) data:

- Restriction to process only the traffic data necessary for the purposes of subscriber or service user identification, service provision, billing and payments. This restriction is not applicable for data retained to investigate serious and very serious crimes (as required by the Data Retention Directive).
- Obligation to notify the State Data Protection Inspectorate about generated and processed data;
- Obligation to provide information to subscribers or registered users of the electronic communications services about the data to be processed, the purpose of such processing and retention period. Such information should be provided before the data are processed and (or) consent is obtained;
- For the purpose of marketing electronic communications services or for the provision of value added services a provider of publicly available electronic communications services may process traffic data or transfer such data to third parties (if they are factual providers of value added services to respective subscribers or actual users of electronic communications services) if the subscriber or the actual user of electronic communications services to whom the data relate has given his consent. Subscribers or actual users of electronic communications services shall be given the possibility to modify, stop or withdraw their consent for the processing of data at any time.
- Obligation to provide location data (including traffic data) without the consent of the subscriber or the actual user of electronic communications services to the Emergency Response Centre.
- Obligation to restrict processing of traffic data to persons acting under the authority of providers of public communications networks and publicly available electronic communications services to the extent necessary to perform their direct functions.
- Competent authorities have the right to receive, in accordance with the procedure and conditions set out in legal acts, information about traffic data with a view to settling disputes between providers of electronic communication services and service users.

The main difference from the ePrivacy Directive is the specification of the possibility to transfer traffic data to third parties (if they are factual providers of value added services to subscribers or actual users of electronic communications services) for the purpose of marketing or for the provision of value added services if the subscriber or the actual user of electronic communications services to whom the data relate has given his consent.

Specific requirements apply to data generated and retained for the purpose of the investigation, detection and prosecution of serious crimes (Article 7 of the Data Retention Directive). Providers of publicly available electronic communications services or of a public communications network have to respect the following data security principles with respect to data retained:

(a) the retained data shall be of the same quality and subject to the same security a
| (b) | the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure; |
| (c) | the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only. |
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Pursuant to Article 66.9 of the Law on Electronic Communications, traffic data should be destroyed at the end of the period of retention. Such retention period is six months from the date of communication or from the termination of the contract with the subscriber or registered user of electronic communications services, except for the cases where the bill is lawfully challenged or the data are necessary for the collection of payment.

Until 2011, there was a following specific requirement to anonymise traffic data: “traffic data relating to subscribers and/or actual users of electronic communications services processed and stored by the provider of a public communications network and/or public electronic communications services must be erased or modified in such a way that it would not be possible to establish, either directly or indirectly, the identity of the subscriber or actual user when the data is no longer needed for the transmission of information, except for the exceptions referred to in Articles 64 and 77 of this Law.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

We are not aware of any such cases.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Law on electronic Communications does not explicitly require to anonymise traffic data.
### D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
</table>
| The term “location data” is defined in Article 3.81 of the Law on Electronic Communications as “data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of an actual user of electronic communications services”.  
The definition includes all and not only “publicly available” communication services, as the ePrivacy Directive, and refers to the “actual user” instead of the “user” of electronic communications services”. |
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Articles 65-67 of the Law on Electronic Communications foresee the following requirements for public communications network and (or) service providers for the lawful processing of location (and traffic) data:

- Restriction to process only data necessary for the purposes of subscriber or service user identification, service provision, billing and payments. This restriction is not applicable for data retained to investigate serious and very serious crimes (as required by the Data Retention Directive).

- Obligation to notify the State Data Protection Inspectorate about generated and processed data;

- Obligation to provide information to subscribers or registered users of the electronic communications services about the data to be processed, the purpose of such processing and retention period. Such information should be provided before the data are processed and (or) consent is obtained;

- Obligation to provide location data (including traffic data) without the consent of the subscriber or the actual user of electronic communications services to the Emergency Response Centre.

- Obligation to restrict processing of location data to persons acting under the authority of providers of public communications networks and publicly available electronic communications services to the extent necessary to perform their direct functions.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Pursuant to Article 66.9 of the Law on Electronic Communications, location data should be destroyed at the end of the period of retention. Until 2011, when the Law on Electronic Communications was amended, there was a requirement to anonymise location data. Article 65 stated:

“Where location data other than traffic data, relating to subscribers of public communications networks or publicly available electronic communications services or to actual users of electronic communications services, can be processed, such data may only be processes when they have been modified in such a way so that it is not possible to establish, either directly or indirectly, the identity of the subscriber or actual user or with the consent of the subscriber or actual user to the extent and for the duration necessary for the provision of a value added service.”
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Not available.</td>
</tr>
<tr>
<td>b</td>
<td>We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.).</td>
</tr>
</tbody>
</table>
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

The Law on electronic Communications does not explicitly require to anonymise location data.
E. Unsolicited commercial communications

<table>
<thead>
<tr>
<th>1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the scope and substance of your national implementation</td>
</tr>
<tr>
<td>b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.</td>
</tr>
</tbody>
</table>

Article 13 of the ePrivacy Directive is transposed by Article 69 of the Lithuanian Law on Electronic Communications.

“Article 69. Direct Marketing

1. The use of electronic communications services, including electronic mail, for the purposes of direct marketing may only be allowed in respect of subscribers or registered users of electronic communication services who have given their prior consent.

2. A person who obtains from customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with the procedure and conditions set out in the Law on Legal Protection of Personal Data, may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. The practice of sending electronic mail for purposes of direct marketing concealing the identity of the sender on whose behalf the communication is made in violation of the requirements set forth in the Law on Information Society Services, or without a valid address to which the recipient may send a request that such communications cease, or inviting to visit internet websites, which do not comply with the requirements set forth in the Law on Information Society Services, shall be prohibited.”

b. The transposing provisions are in line with the ePrivacy Directive. The scope of the implementing provisions in addition to subscribers is extended also to “registered users of electronic communication services”. This notion is defined by Article 3.49 of the Law on Electronic Communications and means a person, who is not a subscriber to publicly available electronic communications services, identifiable according to the identification code of the user of electronic communications and information provided at the moment of registration.

The Law on Electronic Communications does not use the term “unsolicited communications” but “direct marketing”. This term is defined in the Law on Legal Protection of Personal Data according to which direct marketing is “an activity intended for offering goods or services to individuals by post, telephone or any other direct means and/or for obtaining their opinion about the offered goods or services.” (Article 2.13)
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Article 14 of the Law on Legal Protection of Personal Data regulates personal data processing for the purposes of direct marketing. According to this Article, personal data may be processed for the purposes of direct marketing only:

- after the data subject gives his (prior) consent
- if a period for the storage of personal data is set when collecting such data
- if the data controller provided a clear, free-of-charge and easily realisable possibility for the data subject to give or refuse giving his consent for the processing of his personal data for the purposes of direct marketing.

In addition, Article 27 of the same Law requires the data controller to inform a data subject about his right to object to the processing of his personal data when data are or are intended to be processed for the purposes of direct marketing without providing reasons for such objection.
### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

In line with Art. 13 of the ePrivacy Directive, Article 69 of the Law on Electronic Communications and Article 14 of the Law on Legal Protection of Personal Data does not require separate opt-in consent, if:

- the customer’s electronic contact details were obtained from the sale of a product or service in accordance with the procedure and conditions set out in the Law on Legal Protection of Personal Data.
- the electronic contact details were used exclusively for similar products or services of the same seller or provider
- when collecting the contact details, the customers was afforded a clear, free-of-charge and easily realisable opportunity not to give consent or refuse giving consent
- if initially the customer has not objected against such use of the data, at the time of each offer.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

| Article 3.11 of the Law on Electronic Communications defines electronic mail as: “a text, voice, sound, image or other form message sent over a public communications network which can be stored in the network or in the service recipient’s terminal equipment until it is collected by the service recipient”. |
| This definition covers not only electronic mail through the internet, but also MMS/SMS/text messages, voice mail, etc., in line with the definition of “electronic mail” in the ePrivacy Directive. |
| The Law on Legal Protection of Personal Data defines direct marketing as “an activity intended for offering goods or services to individuals by post, telephone or any other direct means and/or for obtaining their opinion about the offered goods or services.” (Article 2.13) |
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. On 17 April 2014, the Inspectorate announced a public consultation on prior consent of the data subject when using electronic communications services for the purposes of direct marketing (available in Lithuanian at: https://www.ada.lt/go.php/Viesosios-konsultacijos2020). In this public consultation the Inspectorate clarifies that prior explicit consent of the recipients should be obtained before unsolicited communications for direct marketing purposes are addressed to them. Any communication (e.g. via phone or e-mail) for the purposes of gaining consent to provide direct marketing offers is not allowed without consent of the subscriber or registered electronic communications service user. Therefore, it is prohibited to call or send an email to an individual asking whether he agrees getting direct marketing offers.


b. In a key case No. N3-733-06 of 22 June 2006, the Supreme Administrative Court of Lithuania stated that according to Article 69.1 of the Law on Electronic Communications (transposing Article 13 of the ePrivacy Directive) consent of the subscriber or user concerned should be gained before the means of direct marketing are employed, and not at the same time.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Although Article 13.5 of the ePrivacy directive requires to ensure, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected, there are no special rules applicable to legal persons to protect them from unsolicited communications. Under the Law on Legal Protection of Personal Data only natural persons must be informed as data subjects about their right to object to the processing of their personal data and have the right to object to the processing of their personal data without providing reasons for such objection where the data are or are intended to be processed for the purposes of direct marketing. In this case, the data controller must suspend processing of personal data, except in the cases laid down in laws, without delay and free of charge, and duly notify the data recipients.

Moreover, the Law on Electronic Communications is applicable to both the subscriber and to the registered user of electronic communication services. However, in practice it is not easy to apply the Law on Legal Protection of Personal Data to the registered users: they cannot lodge a complaint to the Inspectorate, unless the subscriber has officially declared that a certain person uses a specific phone number (registered on the subscriber’s name) in a telecommunications services contract.

Also, in some cases it is difficult to distinguish between direct marketing and advertising (i.e. dissemination of information in any form and by any means related to individual business, financial or professional activities in order to promote the supply of goods or services). In the latter case, different rules in relation to consent, set forth in the Law on Advertising, are applicable. Article 13 of this Law permits advertising by phone, telefax, telex, electronic mail only with the advertising consumer’s consent or per his request. It also prohibits to directly supply advertising to a specific person if his dissagreement has been clearly stated.

The legal rules on direct marketing are not very effective in practice. The number of (ever more aggressive) telemarketing calls and unsolicited electronic emails is very high, and current legal rules and fines have no deterrent effect. Also, only a limited number of users report illegal direct marketing cases to the competent authorities. In 2011-1013, Lithuanian competent authorities received 62 complaints related to telemarketing cases (data from the Ministry of Justice). The effectiveness of the rules on direct marketing could be improved by foreseeing higher sanctions for the violations of the Law on Electronic Communications (currently such fines range from 500 to 2000 Litas – around €145-580) and by holding liable also legal entities for unlawful direct marketing acts. Currently, only a data protection officer, an employee who carried out direct marketing or a head of the company in person can be held liable for illegal direct marketing activities.
COUNTRY REPORT

Luxembourg

For the Study

*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Jos Dumortier, time.lex

Date: 8 September 2014
Contents

Part 1: Management summary ........................................................................................................3

Part 2: Answers to the questionnaire .............................................................................................4
Part 1: Management summary

Management Summary for Luxembourg

- The e-Privacy Directive has been transposed into the national law of Luxembourg by Law of 30 May 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure. The Act of 30 May 2005 has been amended by the Act of 27 July 2007 and further amended by the Act of 24 July 2010 which is a transposition of Directive 2006/24/EC of 15 March 2006. In addition, the Act of 28 July 2011 transposed certain provisions of Directive 2009/136/EC.

- Responsibility for enforcement of the legislation lies principally with the data protection commission (Commission nationale pour la protection des données) but the national regulatory authority for electronic communications (in Luxembourg this is the “Institut Luxembourgeois de Régulation) also has an impact of this topic because it is competent for the protection of consumers of public electronic communications networks and services.

- Luxembourg has transposed all the specified articles of the Directive into domestic law.

- A problematic area of application concerns the application of the legislation to cookies and similar devices. A number of criticisms have been expressed centring on the notion of consent and the extent to which this can be a viable proposition especially in the context of what might be regarded as legacy websites. There is concern that the Directive attempts to retrofit data protection measures into a technical environment where they may not be effective.

- In respect of the handling of traffic and location data the legislation seems to be working reasonably well but there is a tension between the periods of time for which retention of this data might be permitted under data protection principles and the retention requirements introduced under the data retention Directive and now continued in the United Kingdom by the Data retention and Investigatory Powers Act 2014.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)


The Act of 30 May 2005 has been amended by the Act of 27 July 2007 and further amended by the Act of 24 July 2010 which is a transposition of Directive 2006/24 / EC of 15 March 2006 (“data retention”). In addition, the Act of 28 July 2011 transposed certain provisions of Directive 2009/136 / EC as, for example, the new provision with regard to “cookies”.

In addition to these specific regulations, there is always also the requirement to comply with the provisions of the general legislation on the protection of personal data. In Luxembourg this legislation is mainly included in the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article</td>
<td>(Scope)</td>
<td>Article 1 of the Law of 30 May 2005 protecting personal data in the electronic communications sector</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Article</td>
<td>5.1 (Confidentiality)</td>
<td>Article 4 of the Law of 30 May 2005 protecting personal data in the electronic communications sector</td>
</tr>
<tr>
<td>Article</td>
<td>5.2 (Business exception)</td>
<td>Article 4, 3 d) of the Law of 30 May 2005 protecting personal data in the electronic communications sector</td>
</tr>
<tr>
<td>Article</td>
<td>5.3 (Cookies)</td>
<td>Article 4, 3 e) of the Law of 30 May 2005 protecting personal data in the electronic communications sector (as amended by the Law of 28 July 2011)</td>
</tr>
<tr>
<td>Article</td>
<td>6 (Traffic data)</td>
<td>Article 5 of the Law of 30 May 2005 protecting personal data in the electronic communications sector</td>
</tr>
<tr>
<td>Article</td>
<td>9 (Other location data)</td>
<td>Article 9 of the Law of 30 May 2005 protecting personal data in the electronic communications sector</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
</table>

Explanation:

Article 12 of the Law of 30 May 2005 protecting personal data in the electronic communications sector is very clear. It states: “The National Data Protection Commission set up by Article 32 of the Law of 2 August 2002 on the protection of persons with regard to the processing of personal data shall be responsible for the application of the provisions of this Law and of the regulations enacted for the implementation thereof”.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Article 2 of the Law of 30 May 2005 protecting personal data in the electronic communications sector contains, among others, the following definitions:

“(i) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(j) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. The provider of a public communications network is hereinafter referred to as the "operator";

(k) "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. The supplier of electronic communications services is hereinafter referred to as the "service provider".”

The corresponding definitions in the Framework Directive (to which the ePrivacy Directive refers) are:

“(a) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(d) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;
"electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

The definitions of the Luxembourg law are thus 100 % identical to the ones used in the framework of the ePrivacy Directive.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

The answer to this question entirely depends on the fact whether or not the services mentioned do consist wholly or mainly in the conveyance of signals on electronic communications networks and doesn’t fall within the definition of “information society service”.

An information society service is defined (under Luxembourg and EU law) as follows: “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”.

For the purposes of this definition:

— ‘at a distance’ means that the service is provided without the parties being simultaneously present,

— ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,

— ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

In Annex V of Directive 1998/34/EC (to which the ePrivacy Directive indirectly refers for the definition of “information society service”, one finds some examples of services that are not considered as “information society service”.

Among these examples are mentioned:

“Services which are not provided via electronic processing/inventory systems:

(a) voice telephony services;

(b) telefax/telex services;

(c) services provided via voice telephony or fax;

(d) telephone/telefax consultation of a doctor;

(e) telephone/telefax consultation of a lawyer;

(f) telephone/telefax direct marketing.”
These services are excluded because they are not provided via “electronic processing/inventory systems”. This term refers to devices, such as computers, that can be used to store and process information.

Recital (10) of the Framework Directive also states: “Voice telephony and electronic mail conveyance services are covered by this Directive. The same undertaking, for example an Internet service provider, can offer both an electronic communications service, such as access to the Internet, and services not covered under this Directive, such as the provision of web-based content.”

As a result, services such as webmail (defined as an e-mail client implemented as a web application running on a web server) will probably be considered as an information society service because the service doesn’t consist – mainly or wholly – in the conveyance of e-mail messages.

Services such as VoIP will be considered as information society service if they are provided in the form of a web application (services such as Skype). They will be considered as an electronic communications service if they are provided as a traditional voice telephony service.

Location-based services will generally be considered as information society services but if they consist wholly or mainly in the transmission of signals (e.g. GPS) they will fall within the definition of “electronic communication service”.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The territorial scope of the Law of 30 May 2005 protecting personal data in the electronic communications has not been defined by the legislator in Luxembourg. The territorial scope can however be deducted from the Law of 27 February 2011 on electronic communications services and networks. Article 22 of this Law states: “L’entreprise qui ne fournit pas de service de communications électroniques et n’exploite pas de réseau de communications électroniques au Luxembourg n’est pas obligée de notifier ses activités à l’Institut pour demander l’accès ou l’interconnexion”

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a.

Explicit guidance on the interpretation of the definitions mentioned in this section could not be found. Some conclusions on how the definitions are interpreted implicitly in practice can be deducted from the application of the notification duty established by article 8 of the Law of 27 February 2011.

This provision states: “Any natural or legal person who intends to provide networks or electronic communications services shall, not later than twenty days before commencing the provision, notify their intent to the Institute. The notification uniquely identifies the company and contains a description of networks or services to be provided, as well as the launch date planned activities. This information is recorded by the Institute in a publicly accessible electronic register”.

How this notification duty is applied in practice can be demonstrated by taking a look in the “publicly accessible electronic register” established by this provision (see [http://www.ilr.public.lu/communications_electroniques/registrepublic/Registre_public_2014_07_24.pdf](http://www.ilr.public.lu/communications_electroniques/registrepublic/Registre_public_2014_07_24.pdf)). Services provided by companies such as Microsoft, Google, Yahoo, Skype, etc. are not listed in the public register. One can therefore conclude that the NRA in Luxembourg doesn’t consider such services as “electronic communications services”. On the contrary typical VoIP service providers such
as Voipgate or Visual Online have notified their services to the NRA in Luxembourg.

As for the territorial scope, in practice the Law of 30 May 2005 will be applied to network operators providing public communications networks on the territory of Luxembourg and service providers providing public communications services on that territory. This can be deducted from the fact that network operators and service providers not established in Luxembourg but providing public electronic communications networks or services on that territory (e.g. Swiss-based BeeOne, Brussels-based Belgacom, London-based Bloomberg, Paris-based Bouygues, etc. ) notify their activities in Luxembourg to the NRA (the Institut Luxembourgeois de Régulation) under the Law of 27 February 2011.

b. No case law could be found with regard to the scope of the Law of 30 May 2005.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>The distinction between public electronic communications networks and information society services is becoming blurred.</td>
</tr>
<tr>
<td>b.</td>
<td>A possible solution would be to integrate most of the provisions of the ePrivacy Directive in the general data protection (proposed) Regulation and make them applicable to all controllers and processors of personal data.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

<table>
<thead>
<tr>
<th>Article 4 of the Law of 2005 (as amended) states what follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“1. Each service provider or operator shall ensure the confidentiality of communications, and of the traffic data relating thereto, effected by means of a public communications network and publicly available electronic communications services.</td>
</tr>
<tr>
<td>2. No person other than the user concerned may listen to, tap or store communications or the traffic data relating thereto, or engage in any other kinds of interception or surveillance thereof, without the consent of the user concerned.</td>
</tr>
<tr>
<td>3. Paragraph 2:</td>
</tr>
<tr>
<td>(a) shall not preclude technical storage which is necessary for the conveyance of a communication, without prejudice to the principle of confidentiality;</td>
</tr>
<tr>
<td>(b) shall not apply to judicial authorities acting in the context of Article 67-1 of the Code of Criminal Procedure to and to authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences;</td>
</tr>
<tr>
<td>(c) shall not apply to communications, or the traffic data relating thereto, made to the single European emergency number 112 or the emergency numbers determined by the Institute solely for the purposes of (a) enabling messages to be listened to again in the event of problems of comprehension or ambiguity as between the caller and the person called, (b) permitting the documentation of false alarms, threats and improper calls and (c) the production of evidence where there is any dispute as to the course or conduct of action taken by way of assistance.</td>
</tr>
<tr>
<td>Traffic data relating to the communications referred to above, including location data, shall be erased once the assistance has been provided. The content of such communications is to be erased on the expiry of a maximum period of six months;</td>
</tr>
<tr>
<td>(d) shall not affect the recording of communications and of the traffic data relating thereto where such recording is carried out in the context of lawful business practices for the purpose of providing evidence of a commercial transaction or any other commercial communication.</td>
</tr>
<tr>
<td>Parties to such transactions shall be informed in advance of the fact that such recordings may be...</td>
</tr>
</tbody>
</table>
made, of the reason or reasons for which communications are recorded and of the maximum period for which the recordings may be retained. Recorded communications are to be erased as soon as the object is achieved and at all events upon the expiry of the legally prescribed period for contesting the transaction;

(e) shall not apply where electronic communications networks are used with a view to storing information or accessing information stored in a subscriber's or user's terminal equipment, provided that such "cookies" or devices are used for legitimate purposes, that the subscriber or user has given his consent after having received clear and full information, inter alia regarding the purpose of the processing. The methods used to provide this information et to offer the right to object should be as usage-friendly as possible. If technically possible and effective, the consent of the subscriber and of the user may be expressed by using appropriate settings of a browser of another application.

This provision shall not preclude storage or technical access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

4. Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question."

Note: for the application of these provisions and according to Art. 2 d) of the Law “communication” means “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information”.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Article 4 d) of the Law of 2005 (as amended) states that the rule of confidentiality “shall not affect the recording of communications and of the traffic data relating thereto where such recording is carried out in the context of lawful business practices for the purpose of providing evidence of a
commercial transaction or any other commercial communication”.

As it is mentioned in Recital 23 of the ePrivacy Directive confidentiality of communications should also be ensured in the course of lawful business practice. However, where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction or of any other business communication. As stated by the CNDP on its website, “brokers can record orders received by email”. See http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/dispositions-comm-electr/index.html

It is evident that the general data protection legislation applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

The legislator in Luxembourg consequently transposed Art. 5.2 of the ePrivacy Directive as such, without adding anything to the wordings of the Directive.

3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The main exception to the confidentiality principle in the context of Art. 15(1) of the ePrivacy Directive is the one mentioned in Art. 4 b) of the Law of 2005, for “judicial authorities acting in the context of Article 67-1 of the Code of Criminal Procedure et (...) authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences”.

In addition Luxembourg transposed Directive 2006/24 / EC of 15 March 2006 by the Act of 24 July 2010. The Directive made it mandatory for member states to introduce “data retention” while leaving a substantial margin of transposition to national legislators, e.g to determine the duration of the retention period as long as this remains between a period of 6 months minimum and 24 months maximum. The Luxembourg Parliament has opted for the minimum duration of 6 months. In return for this conservation, the service provider and the operator must make every effort to prevent third-party access to the data.

The Act of 24 July 2010 also provides that the retained data can only be used for the prosecution of criminal offenses which include a misdemeanor for which the maximum is greater than or equal to one year’s imprisonment.
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

<table>
<thead>
<tr>
<th>a. The legislation in Luxembourg doesn’t distinguish between confidentiality breaches with or without human involvement. Interception of MAC addresses or capturing content data from unencrypted wifi networks would thus constitute a breach of confidentiality if all the other requirements for the application of Art. 4 of the Law of 2005 are fulfilled. The law doesn’t distinguish between the content of communications and other data relating to it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. In 1982 Luxembourg introduced the Law of 11 August 2011 on the protection of private life. This law protects the confidentiality of telephone conversations, letters, messages, etc.</td>
</tr>
</tbody>
</table>


Articles 1 and 2 of this Law state what follows:

“**Art. 1**

Everyone has the right to respect for his private life. Judges may, without prejudice to the damage suffered, prescribe any measures, such as sequestration, seizure and others adapted to prevent or stop an attack on the privacy of private life; these measures may, if there is an emergency, be ordered in chambers.

**Art. 2.**

Is punished with imprisonment from eight days to one year and a fine of 2,501 to 50,000 francs, or one of these penalties, any person who willfully infringed the intimacy of the private life of others.

1 by listening or enable listening, recording or enable recording, transmitting or enable transmitting, by means of any device, words spoken in private by any person without the consent of the latter;
2 by observing or enable observing, using any device, a person in a place not accessible to the public without the consent of the latter, by fixing or enable fixing or by transmitting or enable transmitting in those conditions the image of that person;

When the acts specified in this article were made during a meeting in the full knowledge of its participants, their consent is presumed;

3 by opening without the consent of the person to whom it is addressed or from whom it emanates, a message sent or forwarded in a sealed envelope, or, by reading, by any device, the content of such a message or removing such a message.

The provisions of n° 1 of this Article shall not apply to any person responsible for the maintenance and monitoring of a public or private telephone network, listening in the exercise of its functions to ensure the proper functioning of the communication.

The penalties provided for in this section apply to everyone who does not respect the privacy of the communication listened to under these circumstances.”
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>a.</strong></td>
<td>the scope and substance of your national implementation</td>
</tr>
<tr>
<td><strong>b.</strong></td>
<td>whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?</td>
</tr>
</tbody>
</table>

**a.** Art. 4 (e) of the Law of 2005 is worded as follows: “(the confidentiality principle) shall not apply where electronic communications networks are used with a view to storing information or accessing information stored in a subscriber’s or user’s terminal equipment, provided that such "cookies" or devices are used for legitimate purposes, that the subscriber or user has given his consent after having received clear and full information, inter alia regarding the purpose of the processing. The methods used to provide this information et to offer the right to object should be as usage-friendly as possible. If technically possible and effective, the consent of the subscriber and of the user may be expressed by using appropriate settings of a browser of another application.

This provision shall not preclude storage or technical access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user”.

The text of Art. 5.3 of the ePrivacy Directive is worded as follows:

“Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

Consequently the Luxembourg legislator added:

1) “The methods used to provide this information et to offer the right to object should be as usage-friendly as possible.” This text has been copied from Recital 25 of the Directive.

2) “If technically possible and effective, the consent of the subscriber and of the user may be expressed by using appropriate settings of a browser of another application”.

**b.** The legislation does not differentiate between different forms of cookie.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

| Art. 4 e) states that “if technically possible and effective, the consent of the subscriber and of the user may be expressed by using appropriate settings of a browser of another application”.

In practice this means that the consent of the subscriber and the user can be implicitly deducted from the browser settings. |
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Art. 4 e) of the Law of 2005 states that the informed consent rule “ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d’une communication par la voie d’un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d’un service de la société de l’information expressément demandé par l’abonné ou l’utilisateur.”

English translation: “This provision shall not preclude storage or technical access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user”.

The legislator does, in other words, literally copy the text of Art. 5.3 of the ePrivacy Directive on this point.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

| Compliance of website owners with the new rules concerning the use of cookies in Luxembourg has not yet been systematically investigated. There are no statistics on compliance and we are not aware of any enforcement action against violations of the rules. |
| Navigating through websites in Luxembourg learns us that practices are very diverse. |
| The information given to the users is sometimes very extensive, and contains in some cases even an extensive list of all cookies (including the name, type, host, etc.) used on the website. See, for example: [http://luxembourg.angloinfo.com/](http://luxembourg.angloinfo.com/). To discover the information, however, one has to click on a link on the bottom of the home page referring to the cookie policy (in extremely small characters). |
| Most of the large international companies have adapted their websites similar to what they have done in the other Member States where they operate. New visitors of the website receive a banner worded as follows: “We use cookies to ensure that we give you the best experience on our site. Cookies are files stored in your browser and are used by most websites to help personalise your web experience. By continuing to use our website without changing the settings, you are agreeing to our use of cookies. More information...” (taken from the Telindus-Luxembourg website). |
| Many local Luxembourg companies apparently didn’t yet adapt their websites in order to be compliant with the rules introduced in 2011. We navigated through 25 websites of randomly selected companies and rarely (only in 3 cases) found explicit information on the use of cookies on these websites. |
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

| a. | The only guidance provided by the data protection commission (CNDP) in Luxembourg is the following paragraph: “The law of 28 July 2011 introduced an important innovation with respect to traces of connection to the Internet (usually called “cookies”) and reinforces the guarantees of transparency and fair use of these techniques that are used almost everywhere on the Internet. Online services (often not paid) use this method to customize as much as possible the navigation of the user and interact with him (including placing ads into account its interests). The requirement of fairness and transparency, and the ability to accept or reject the use of “cookies” includes both the placement of the cookies on the terminal of the user and the subsequent access to the information deducted from these cookies stored by the original or other partners or stored on other websites” |
| b. | There have been no court cases to date. |
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The amendment introduced in 2011 (introduction of the consent rule) has mainly led to an increased awareness about the use of cookies and to an improvement of the information given by website owners about the use of cookies and about the possibility to adapt the settings of the web browser.

b. The legislation in Luxembourg and the way it is implemented and enforced mainly demonstrates that improving the effectiveness of this legal framework is not a real objective.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Article 2(f) of the Law of 2005 contains the following definition: “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

This definition is identical to the one in Art. 2 b) of the ePrivacy Directive.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Article 5 of the Law of 2005 regulates the processing of traffic data and is formulated as follows:

“(a) For the purposes of the investigation, detection and prosecution of criminal offences leading to a criminal or correctional sanction of which the maximum is equal to or higher than one year of imprisonment, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing or generating traffic data in the framework of the provision of data services related to the traffic must retain such data for a period of 6 months starting from the date of the communication. The obligation to retain includes the saving of the data relating to unsuccessful telephone calls if these data are generated or processed and saved (as far as telephone data are concerned) of logged (as far as internet data are concerned) in the framework of the provision of the communication services concerned. The categories of traffic data capable of being used for the investigation, detection and prosecution of criminal offences shall be determined by Grand-Ducal regulation. This regulation can also establish the forms and modalities for making available the data to the judicial authorities.

(b) Upon the expiry of the retention period provided for in (a) above, the service provider or operator shall be required to erase or render anonymous traffic data relating to subscribers and users.

2. Service providers or operators processing traffic data concerning subscribers or users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph 1(a) above, in such a way as to make it impossible for anyone to access the data in question once they are no longer needed for the transmission of a communication or for processing pursuant to paragraphs 3 and 4, with the exception of access which is:

– ordered by authorities acting pursuant to Art. 67-1 of the Code of Criminal Procedure and by authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences; or

– requested by the competent bodies with a view to settling disputes, in particular interconnection or billing disputes.

3. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing shall be permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued, and may not in any event exceed a period of six months where the invoice has been paid and has not been disputed or challenged.

4. Traffic data may be processed for the purposes of marketing electronic communications services or providing value added services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or
the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his/her consent, notwithstanding his/her right to object to such processing at any time.

5. Processing of traffic data in the context of the activities referred to in paragraphs 1 to 4 shall be restricted to persons acting under the authority of the service provider or operator and handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. It must be restricted to what is necessary for the purposes of such activities.

6. Any person who contravenes the provisions of paragraphs 1 to 5 of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.”

3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Article 5 b) of the Law of 2005 states: “(b) Upon the expiry of the retention period provided for in (a) above, the service provider or operator shall be required to erase or render anonymous traffic data relating to subscribers and users.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| There have been no cases concerned specifically with traffic data under the ePrivacy Directive. |</p>
<table>
<thead>
<tr>
<th>5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application in practice of the duty for operators and service providers to delete traffic data after the retention period of six months or to render these data anonymous, is not monitored nor enforced.</td>
</tr>
</tbody>
</table>
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Art. 2 of the Law of 2005 contains the following definition: (g) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service”.

This is exactly the definition of Art. 2 c) of the ePrivacy Directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Article 59 of the Law of 2005 regulates the processing of location data other than traffic data and is formulated as follows:

“1.(a) For the purposes of the investigation, detection and prosecution of criminal offences leading to a criminal or correctional penalty of which the maximum is equal to or higher than one year of imprisonment, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing or generating location data other than traffic data in the framework of the provision of data services related to the localisation other than the traffic must retain such data for a period of 6 months starting from the date of the communication. The obligation to retain includes the saving of the data relating to unsuccessful telephone calls if these data are generated or processed and saved (as far as telephone data are concerned) or logged (as far as internet data are concerned) in the framework of the provision of the communication services concerned. For the application of this paragraph one localisation information is requested per communication or call. The categories of traffic data capable of being used for the investigation, detection and prosecution of criminal offences shall be determined by Grand-Ducal regulation. This regulation can also establish the forms and modalities for making available the data to the judicial authorities.

(b) Upon the expiry of the retention period provided for in (a) above, the service provider or operator shall be required to erase or render anonymous location data other than traffic data relating to subscribers and users.

2. Service providers or operators processing location data other than traffic data concerning subscribers or users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph 1(a) above, in such a way as to make it impossible for anyone to access the data in question once they are no longer needed for the transmission of a communication or for processing pursuant to paragraphs 3 and 4, with the exception of access which is:

– ordered by authorities acting pursuant to Art. 67-1 of the Code of Criminal Procedure and by authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences; or

– requested by the competent bodies with a view to settling disputes, in particular interconnection or billing disputes.

3. Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his/her consent thereto, to the extent and for the duration necessary for the supply of a value added service and subject to the provisions of paragraphs 2, 4 and 5.
4. Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time.

Where consent of the subscribers or users has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

5. Processing of location data other than traffic data in the case of the activities referred to in paragraphs 1 to 4 shall be restricted to persons acting under the authority of the service provider or operator or of the third party providing the value added service, and must be restricted to what is necessary for such activities.

6. Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.”
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

As already mentioned before, Art. 9 (3) of the Law of 2005 is formulated as follows: “(3) Tout fournisseur de services ou opérateur ne peut traiter des données de localisation autres que les données relatives au trafic et concernant les abonnés ou les utilisateurs que si celles-ci ont été rendues anonymes ou moyennant le consentement de l’abonné ou de l’utilisateur, dans la mesure et pour la durée n écessaires à la fourniture d’un service à valeur ajoutée et sous réserve des dispositions des paragraphes (2), (4) et (5)”

In other words: Unless the operator or service provider has the consent of the subscriber or user, or unless another exception is applicable (such as data retention for law enforcement purposes), location data can only be further processed in anonymous form.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. To data there have been no decisions, opinions or other forms of guidance on this aspect of the legislation.

b. To date there have been no court or tribunal decisions on this aspect of the legislation.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

In general there have been no issues concerning the application of the rules regarding location data in Luxembourg.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

“1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is permissible only in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

3. The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in paragraphs 1 and 2 shall be permissible only with the prior consent of the subscriber concerned.

4. The practice of sending of electronic mail for purposes of direct marketing disguising, concealing or misrepresenting the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, is prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons.

6. Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.”

Compared to Art. 13 of the ePrivacy Directive, formulated as follows:

“1. The use of automated calling and communication systems without human intervention
(automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers or users concerned or in respect of subscribers or users who do not wish to receive these communications, the choice between these options to be determined by national legislation, taking into account that both options must be free of charge for the subscriber or user.

4. In any event, the practice of sending electronic mail for the purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, which contravene Article 6 of Directive 2000/31/EC, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that Article shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

6. Without prejudice to any administrative remedy for which provision may be made, inter alia, under Article 15a(2), Member States shall ensure that any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.”
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Art. 11 (3) mentions: “3. The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in paragraphs 1 and 2 shall be permissible only with the prior consent of the subscriber concerned.”

3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Identically to the ePrivacy Directive, Art. 11 (2) states: “2. Notwithstanding paragraph 1, where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.”
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Luxembourg legislator literally transposed the provisions of the ePrivacy Directive on this point.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There are no additional documents or decisions issued by the CNDP on this item of the legislation.</td>
</tr>
<tr>
<td>b.</td>
<td>No court cases</td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions of the law in Luxembourg are in conformity with the provisions of the Directive but it is difficult to state that they have been effective in reducing the volume of spam messages.
COUNTRY REPORT

LATVIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Sarmis Spilbergs, LAWIN

Date: 18.08.2014
Contents

Part 1: Management summary ........................................................................................................ 3
Part 2: Answers to the questionnaire............................................................................................ 5
Part 1: Management summary

The transposition of the e-Privacy Directive into Latvian law can be summarized as follows:

- The provisions of the Directive 2002/58/EC have mostly been transposed by the Electronic Communications Law 2004. However, the provisions of the Directive 2002/58/EC regarding unsolicited communications, namely Article 2(h), Article 5(3) and Article 13 of the Directive have been implemented into Latvian law by the Law on Information Society Services 2004. The implementation process was not completely seamless, taking into consideration the fact that the implementation of the provisions regarding unsolicited communications took place later than prescribed by the Directive. The provisions of the Directive 2009/136/EC, which amended the Directive 2002/58/EC, have been successfully transposed into Latvian law by the amendments to the Electronic Communications Law and to the Law on Information Society Services.

- Article 5(2) of the Directive 2002/58/EC has been transposed into Latvian law in a general manner by Articles 19(1)(11) and 70(2) of the Electronic Communications Law. Other provisions in Latvian laws may also be considered to embody this article. However, due to the text of the article not being transposed directly its scope and effectiveness are of concern.

- Article 5(3) of the Directive on cookies has been transposed into Latvian law almost literally. So far no provisions further elaborating and explaining the said transpositions have been adopted. Therefore, the application of the transposing provision – Article 7.1 of the Law on Information Society Services is still rather unclear, especially due to the fact that so far no relevant court decisions or guidelines have been issued. Additionally, in practice it is also unclear which authority is responsible for ensuring and supervising compliance with the said provision.

- The provisions of the Directive 2002/58/EC regulating traffic data have been correctly implemented into the Electronic Communications Law. This does not expensis verbis provide for anonymisation or erasing of the traffic data when it is no longer needed for the purpose of the transmission of a communication. However, the Latvian law does provide that traffic data shall be processed in a time period, in which the user or subscriber may dispute the invoice and perform payments according to the procedures specified in regulatory enactments and that in individual cases, traffic data can be processed and stored while objections are being examined and resolved, as well as until the time when unpaid payments are recovered. This provision may entail that generally processing, inter alia – storing, of the traffic data is not permissible in all other cases and thus in those situations such data should be erased. Also, Latvian legislation does not stipulate for the service provider to inform the subscriber or user of the types of traffic data, which will be processed and of the duration of such processing as stipulated under Article 6(4) of the Directive.

- The provisions of the Directive 2002/58/EC regarding location data have been correctly transposed into Latvian Law. The Latvian law, contrary to the Directive, specifies what should be understood as geographic location for different types of networks, however, in our opinion this should not be viewed as a significant deviation from the provisions of the Directive. No case law or recommendations have been issued in respect to location data.
At the present moment, the authority responsible for supervising compliance with the rules provided in Article 9 of the Law on Information Society Services (unsolicited commercial communications) is the Data State Inspectorate. However, the Consumer Rights Protection Centre, based on its authority to supervise compliance with the rules on advertising, has also addressed rules regulating commercial communications, which later, in more detail have been reviewed in Administrative court. As regards application of Article 9 of the Law on Information Society Services, it is the provision regarding which the most recommendations have been issued and court decisions adopted, compared to other Articles implementing the provisions of Directive 2002/58/EC.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Latvia:
- Directive 2002/58/EC has been partly transposed into Latvian national legislation by the Electronic Communications Law of 28 October 2004 (hereinafter referred to as the Electronic Communications Law).
- As regards Article 13 of the Directive 2002/58/EC on unsolicited communications, it was transposed into Law of 4 November 2004 on Information Society Services (hereinafter – Law on Information Society Services) by the Amendments of 10 November 2005 to the Law on Information Society Services. The definition of the term “electronic mail” was also transposed by the same amendments. The abovementioned transposition of the Articles of the Directive 2002/58/EC was carried out later than prescribed by the Directive; it took place only after Latvia on 21 March 2005 received the letter from the Commission, where it was pointed out that Latvia had not yet fulfilled its obligations in respect of the implementation of the Directive 2002/58/EC.
- On the same date, i.e. 19 May 2011, the Law on Information Society Services was also amended in order to incorporate the requirements of Article 5(3) of the Directive 2002/58/EC.
- Additionally, in 2011 the Public Utilities Commission issued the General Permit Regulations of 24 August 2011. The Informative reference of the General Permit Regulations stipulates that the said Regulations contain provisions, which follow from the Directive 2009/136/EC.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
Art. 1(1)(1)

Art. 3 (Scope)  
This provision has been implemented into Latvian legislation in a general manner in Art. 14 and Art. 25(2) of the Electronic Communications Law.

Art. 5.1 (Confidentiality)  
Electronic Communications Law of 28 October 2004, Art. 19(1)(4) and Art. 68  
http://likumi.lv/doc.php?id=96611

Art. 5.2 (Business exception)  
Electronic Communications Law of 28 October 2004, Art. 19(1)(11) and Art. 70(2)  
http://likumi.lv/doc.php?id=96611

Art. 5.3 (Cookies)  
Law of 4 November 2004 on Information Society Services, Art. 7  
http://likumi.lv/doc.php?id=96619

Art. 6 (Traffic data)  
Electronic Communications Law of 28 October 2004, Art. 70  
http://likumi.lv/doc.php?id=96619

Art. 9 (Other location data)  
Electronic Communications Law of 28 October 2004, Art. 71  
http://likumi.lv/doc.php?id=96619

Art. 13 (Unsolicited communications)  
Law of 4 November 2004 on Information Society Services, Art. 9  
http://likumi.lv/doc.php?id=96619

2. Which enforcement authority (lies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)  
For each authority please provide in the table below:  
a. the full name in your national language  
b. the English translation of the short name  
c. the part or the provision(s) of the ePrivacy Directive it supervises  
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or the provision(s) of the Directive it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Summary

<table>
<thead>
<tr>
<th>Authority (Code)</th>
<th>Agency (Name)</th>
<th>Supervises</th>
<th>Authority Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sabiedrisko pakalpojumu regulēšanas komisija (PUC)</td>
<td>Public Utilities Commission</td>
<td>PUC is the authority responsible for supervising the compliance with the regulatory enactments in the electronic communications sector.</td>
<td><a href="http://www.sprk.gov.lv/">http://www.sprk.gov.lv/</a></td>
</tr>
</tbody>
</table>

### Explanation:

- The Ministry of Transport is a leading institution of state administration of transport and communication branches, which elaborates legal acts and policy planning documents regulating the branch. Thus, the Ministry of Transport is the authority which holds responsibility for implementing the provisions of the Directive 2002/58/EC into Latvian national law.

- The Public Utilities Commission, also known as the Regulator, is institutionally and functionally independent, an autonomous body governed by public law, which, among other things, carries out regulation of public services in electronic communications. The Regulator independently performs the functions transferred by law and within its competence independently adopts decisions and issues administrative acts, which are binding to specific providers and users of public services.

- The Data State Inspectorate is a state administration institution whose functions, rights and duties are determined by law. It carries out supervision of personal data protection. It operates independently, fulfilling the functions specified in regulatory enactments, taking the decisions and issuing administrative acts in accordance with the law.

- The Consumer Rights Protection Centre is an authority under surveillance of the Ministry of Economics, which enforces protection of consumer rights and interests.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Article 1 (11) of the Electronic Communications Law defines “electronic communications network” as “transmission systems, switching and routing equipment (including network elements which are not being used) and other resources, which irrespective of the type of transmitted information permits the transmission of signals by utilising wires, radio waves, optical or other electromagnetic means in the networks, including:

a) satellite networks, fixed networks (channel and packet switching networks, including internet) and mobile terrestrial electronic communications networks,

b) networks, which are utilised for radio and television signal distribution, and

c) cable television and cable radio networks, electricity cable systems to the extent they are used for the purposes of transmitting signals.”

The citation of the said Article clearly shows that Article 2(a) of the Directive 2002/21/EC, which provides a definition of the term “electronic communications network” has been correctly implemented into Latvian law.

Article 1(9) of the Electronic Communications Law holds a definition of electronic communications service: “a service that is usually ensured for remuneration and which entirely or mainly consists of the transmission of signals in electronic communications networks”.

By comparing the transposing provision cited above with Article 2(c) of the Directive 2002/21/EC, it may be concluded that Article 1(9) of the Electronic Communications Law has a more narrow scope than the respective provision of the Directive 2002/21/EC. However, Articles 3(2) and 3(3) of the Electronic Communications Law rectify this error by stipulating:

“(2) This Law shall also apply to the electronic communications networks that are necessary for the distribution of radio or television programmes. The Radio and Television Law shall determine the procedures for the establishment, registration, operation and supervision of broadcasting organisations within the jurisdiction of the Republic of Latvia.

(3) This Law shall not apply to the provision of information society services and the information content thereof, which are transmitted or received in electronic communications networks.”

Therefore, although Articles 3(2) and 3(3) of the Electronic Communications Law officially are not the provisions implementing Article 2(c) of the Directive 2002/21/EC, they still help to fulfil the obligation of correctly and fully transpose Article 2(c) of the Directive 2002/21/EC.

The Electronic Communications Law is mostly addressed towards an “electronic communications merchant”. Article 1(8) of the Electronic Communications Law contains the following definition:

“Electronic communications merchant – a merchant or a branch of a foreign merchant who is entitled to carry out commercial activity, to ensure a public electronic communications network or provide electronic communications services in accordance with the procedures specified in this Law.”

Article 1(10) of the Electronic Communications Law stipulates that an “electronic communications service provider” is “an electronic communications merchant who provides publicly accessible
electronic communications services, utilising the public electronic communications network;”

Therefore, Latvian law contains a distinction between “public” and “private” electronic communications network.

Article 1(33) of the Electronic Communications Law also provides the following definition: “operator – an electronic communications merchant who provides an electronic communications network or associated facilities”.

Therefore, as stated in Articles 1(10) and 1(33) of the Electronic Communications Law, “electronic communications merchant” may act as an “electronic communications service provider” and/or an “operator”.
| 4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)? |

Due to the ePrivacy Directive being implemented in both the Electronic Communications Law and the Law on Information Society Services, the applicability of the implementing legislation depends on whether such services fall within the scope of electronic communications services and information society services as accordingly defined under these laws.

Should any of these services fall under the scope of the electronic communications service definition, i.e., entirely or mainly consists of the transmission of signals in electronic communications networks and not be considered an information society service, the provisions of the ePrivacy directive implemented in the Electronic Communications Law would apply. While it is possible that VoIP would fulfil this requirement, it is, however, doubtful that webmail and location based services would do as well since they are likely to be content oriented and not sufficiently connected with the transmission of signals in electronic communications networks. Furthermore since the latter are typically information society services, as such they would also be excluded from the scope of application of the Electronic Communications Law and provisions of the ePrivacy Directive therewith implemented.

However, some of the provisions of the ePrivacy Directive as indicated above are applicable solely to the information society service providers. Under Article 1(1)(2) of the Law on Information Society Services an information society service is defined as a distance service which is usually a paid service provided using electronic means (electronic information processing and storage equipment, including digit compression equipment) and upon the individual request of a recipient of the service. Information society services include the electronic trade of goods and services, the sending of commercial communications, the possibilities offered for searching for information, access to this and the obtaining of information, services that ensure the transmission of information in an electronic communication network or access to an electronic communication network, and storage of information. Thus, as webmail and location services are likely to be considered to be information society services the relevant provisions of the Law on Information Society Services where the according provisions of the ePrivacy Directive has been transposed would be applicable. Applicability of these provisions to VoIP would depend on the according set up of such a service.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

As mentioned above, the provisions of the Directive 2002/58/EC mainly have been transposed by two Latvian laws – Law on Information Society Services and Electronic Communications Law. However, neither contains a provision where the territorial scope is clearly defined.

In general, the provisions of Electronic Communications Law apply to “electronic communications merchants”. The definition of “electronic communications merchant” is provided by Article 1(8) of the Electronic Communications Law “a merchant or a branch of a foreign merchant who has the right to perform commercial activity, to ensure a public electronic communications network or provide electronic communications services in accordance with the procedures specified in this Law”. According to Article 32(2) of the Electronic Communications Law a merchant may commence providing electronic communications or electronic communications services once a registration notification has been sent to the regulatory authority – Public Utilities Commission. Thus, both permission to provide electronic communications and electronic communications services and applicability of Electronic Communications Law are subject to a prior establishment of local presence in Latvia either by setting up a local company or a branch.

However, should any foreign operators or providers of electronic communications services provide electronic communications or electronic communications services in the Republic of Latvia without establishing a local presence in Latvia they would be in breach of Article 158.2 of the Latvian Administrative Violations Code (LAVC) which, inter alia, foresees responsibility for provision of public services without the necessary registration and breach of the general permit in the electronic communications sector. Breach of this provision may be sanctioned with a fine up to €700 for natural persons and up to €14 000 for legal persons.

Furthermore, it should be noted that both foreign electronic communication merchants operating in Latvia through a subsidiary and a branch still may be subject to the Personal Data Protection Law as personal data “controllers”. The scope of applicability of this law is defined in Article 3(1) which closely mirrors Article 4(1) of the Directive 95/46/EC. Thus, foreign entities may be subject to administrative liability under LAVC and coercive measures applicable to legal persons under the Criminal Law for breaches of personal data protection laws and regulations. E.g., according to Article 204.7 LAVC a penalty of up to €11 000 may be imposed on legal persons for illegal operation with personal data while according to Article 145 of the Criminal Law illegal actions with personal data, if substantial harm has been created.

The Law on Information Society Services is mainly addressed to providers of information society services, thus, its application depends on whether the subject can be considered a provider of an information society service. The Law on Information Society Services does not hold a specific definition of such a provider, however, the concept of an information society service has been thoroughly described under Article 1(1) Law on Information Society Services as cited in answer to Question A4 above. In comparison to the Electronic Communications Law there are no prerequisites
of local presence for operation in the territory of Latvia under the framework of Law on Information Society Services. Thus, the law is equally applicable to local and foreign entities providing information society services. Although, the scope of applicability is quite broad there are not so many infringement decisions issued by the responsible authority – Data State Inspectorate. E.g., in 2012 only one subject was punished for sending unsolicited communications, while in 2013 two such decisions had been issued by the authority. In regard to unsolicited communications, it must be mentioned that due to commercial communications being required (under Article 8 of the Law on Information Society Services) to be in compliance with the general provisions of the Advertising Law, the Consumer Rights Protection Centre quite often investigates infringements in regard to unsolicited communications which are qualified as provision of advertising contrary to the provisions of Advertising law. In general, violations of sending unsolicited communications are sanctioned under Article 204.\textsuperscript{16} LAVC with a fine up to €7000 for legal persons.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. National enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. National courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>None of the Latvian enforcement authorities mentioned in the Section A2 of this research has issued any guidelines or decisions in concrete case regarding the definitions described in section A3 of this research.</td>
</tr>
<tr>
<td>b.</td>
<td>We are not aware of any court cases in Latvia where further guidance on interpretation or scope of definitions stated in this section would have been provided.</td>
</tr>
</tbody>
</table>
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. In general, the provisions of Latvian Law described above are quite clear, logically consistent and appropriate for protecting privacy within Latvia. However, the scope of actions that may be taken by authorities in regard to foreign electronic communications providers acting illegally is somewhat limited. As described in further sections problems may arise due to the separation of provisions implementing the Directive 2002/58/EC either in Electronic Communication Law or Law on Information Society Services.

   b. It would be recommended to define territorial scope more clearly in the Electronic Communications Law, in order to avoid any uncertainty. Additional rights of the Regulator to combat the illicit provision of electronic communication services could also be reviewed.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

According to the information available on the website of Latvian legislator, the principle of confidentiality enclosed in Article 5(1) of the Directive 2002/58 has been implemented by Article 19(1)(4) of the Electronic Communications Law. The said Article broadly stipulates the obligation of the electronic communications merchant to “ensure the protection of user data including personal data in accordance with regulatory enactments”.

Further, Article 68 of the Electronic Communications Law in a more detailed manner implements Article 5(1) of the Directive 2002/58/EC:

“(1) An electronic communications merchant has a duty not to disclose information regarding users or subscribers without the permission of the user or subscriber, as well as information regarding the electronic communications services or value added services received by them, except in the cases if such information is necessary for the institutions referred to in Article 70, Paragraphs eight and nine of this Law, as well as for the performance of the functions specified in regulatory enactments by the institutions referred to in Article 711, Paragraph one of this Law and for the purposes referred to in Article 712.

(2) An electronic communications merchant is prohibited to disclose information, which he or she transmits or which is transmitted while providing electronic communications services to users or subscribers without the consent of the user or subscriber, except in the cases if such information is necessary for the performance of the functions specified in regulatory enactments of the institutions referred to in Article 711, Paragraph one of this Law and for the purposes referred to in Article 712.”

Additionally, the Public Utilities Commission, based on its authority granted by Article 34(1) of the Electronic Communications Law, has issued General Permit Regulations, which are binding to all electronic communications merchants. According to Article 10 of the General Permit Regulations “electronic communications merchant shall not, except in situations prescribed by law, disclose information on user without a written permission, as well as shall not disclose details on information transmitted or which is transmitted via electronic communications network, or which may be obtained by providing electronic communications services.”

As regards “communications”, the Latvian legislator has not utilized this exact term in the laws implementing the Directive 2002/58/EC in the context of confidentiality, and, consequently, Latvian legislation does not contain any definition of this term. As can be seen from the citation of the transposing provisions of law, the terms “information” or “user data” are employed instead. Article 144 of the Criminal Law employs the term “correspondence” when referring to data protection.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Based on the information provided on the official website of Latvian legislator, Article 5 of the Directive 2002/58/EC has been completely transposed by Article 68 of the Electronic Communications Law. This would entail a logical assumption that Article 5(2) of the Directive is correctly and fully implemented into Latvian law. However, Article 68 of the Electronic Communications Law (please see the full citation of the said Article in the Answer to the question B1 above) does not contain the exception enclosed in Article 5(2) of the Directive. Nevertheless, during the meeting with the responsible official of the Ministry of Transport it was explained that Article 5(2) of the Directive 2002/58/EC has been in a general manner transposed into the Latvian law by Articles 19(1)(11) and 70(2) of the Electronic Communications Law. Article 19(1)(11) generally stipulates that the electronic communications merchant is obliged to ensure the retention of the data to be retained for the period of 18 months. Further, pursuant to Article 70(2) of the Electronic Communications Law: “Traffic data shall be processed in a time period, in which the user or subscriber may dispute the bill and make payments according to the procedures specified in regulatory enactments. In individual cases, it is allowed to process and store the traffic data while objections are being examined and resolved, as well as until the outstanding payments are recovered.” However, considering the wording cited above it may be argued that the scope of the above-mentioned provisions of the Electronic Communications Law is narrower than that of Article 5(2) of the Directive 2002/58/EC.

Moreover, the Personal Data Protection Law contains Article 7(6), pursuant to which personal data processing is permitted when “the data processing is necessary in order to comply with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the controller or of such third person to whom the personal data have been disclosed to”. Thus, the business exception enclosed in Article 5(2) of the Directive 2002/58/EC might be interpreted as “lawful interests of the controller”.

Due to Article 5(2) of the Directive 2002/58/EC being transposed into Latvian law only in a general manner without any express wording close to the text of the article in the Directive its scope and effectiveness are disputable. In our opinion a direct transposition of this article would have granted businesses with more effective rights as envisaged by Article 5(2) of the Directive 2002/58/EC than the current means of transposition of this article.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Yes, the Electronic Communications Law contains several exceptions to the confidentiality principle.

Article 68 of the Electronic Communications Law, which implements the confidentiality principle, refers to Articles 71.¹ and 71.² as to provisions of law, where exceptions to the confidentiality principle are regulated.

Article 71.¹(1) of the Electronic Communications Law contains the following exception:
“Data to be retained shall be retained and transferred to pre-trial investigation institutions, authorities for investigation activities, State security institutions, the Office of the Public Prosecutor and the courts in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and trial of criminal cases.”

Article 71.²(1) of the Electronic Communications Law stipulates:
“An electronic communications merchant shall, upon request by the court, ensure the provision of the information regarding the given name, surname or designation and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the connection in order to ensure the protection of the rights and legal interests of the individual infringed in the electronic environment in the civil cases.”

However, as regards Article 71.¹ of the Electronic Communications Law, to which Article 68 of the Electronic Communications Law refers as an exception of the confidentiality principle, please be aware that in the nearest future it may be excluded from the Electronic Communications Law, or amended. This particular information has not been yet made public, but was provided by both the Data State Inspectorate and the Public Utilities Commission. The amendments are necessary due to the fact that Article 71.¹(1) of the Electronic Communications Law implements the provisions of the Directive 2006/24/EC, to which the reference is given in Article 15(1)(b) of the consolidated version of the Directive 2002/58/EC.

On 8 April 2014 the Court of Justice of the European Union passed a judgement in the joined cases C-293/12 and C-594/12, where the CJEU has ruled that the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, is invalid. In the judgement the CJEU, inter alia, stated that: “Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.”

Therefore, as a result of the abovementioned judgement, currently a legal basis upon which national legislation to contain rules on “data to be retained” is no longer valid.
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. Latvian laws do not contain any specific provisions regarding automated breaches without human intervention.

Latvian laws regarding the protection of the communications do not contain a distinction between the content of communications and other data relating to communications (i.e. traffic data).

b. Yes, in Latvia a provision dedicated to the protection of private electronic communications was introduced several years before the obligation to transpose the Directive 2002/58/EC had occurred, namely by Article 144 of the Criminal Law of 1 April 1999. The said Article consists of two paragraphs. The first paragraph of Article 144 stipulates:

“For a person who commits intentional violation of the confidentiality of personal correspondence or information in the form of transmissions over a telecommunications network, or commits intentional violation of the confidentiality of information and programs provided for use in connection with electronic data processing, the applicable sentence is deprivation of liberty for a term not exceeding two years or temporary deprivation of liberty, or community service, or a fine.”

Further, Article 144(2) contains a penalty for the same actions as listed in Article 144(1), if these actions were committed with the purpose of acquiring property. In such case the penalty is stricter – deprivation of liberty for a term not exceeding five years or community service or a fine.

Doctrinal commentary of the Criminal Law by professors U. Krastiņš, V. Liholaja and A. Niedre holds an explanation that Article 144 of the Criminal Law protects any transmissible information, regardless of whether it is written, oral or electronic personal correspondence, information transmissible via telecommunication networks or information and programs provided for use in connection with electronic data processing. This encompasses information, which a person receives or transmits via post, electronic mail, telephone, telegraph, fax, telex, pager or any other means of communication, as well as information inserted in the automatic data processing system.

Regarding Article 144 of the Criminal Law it is important to note that a victim of the criminal offense described in this Article may only be a natural person. Therefore, Article 144 of the Criminal Law does not extend its protection to legal persons.

As regards the person that commits the offense – it may be any natural person of a sound mind, who is at least 14 years old. The offense can be committed only intentionally, when offender is aware of the fact that he is accessing information without legitimate basis.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

   a. Article 7.1 of the Law on Information Society Services implements the requirements of the Article 5(3) of the Directive 2002/58/EC as follows:

   “(1) Storage of information in a terminal equipment of a subscriber or user, or access to the information stored in a terminal equipment shall be permitted, if the respective subscriber or user has given his or her consent after he or she has received clear and comprehensive information regarding the purpose of the aforementioned processing in accordance with the Personal Data Protection Law.

   (2) The consent referred to in Paragraph one of this Article shall not be necessary, if storage of the information in a terminal equipment or access to the information stored in a terminal equipment is required for the purposes of ensuring of circulation of the information in the electronic communications network or for intermediary service provider in order to provide a service requested by a subscriber or user.”

   b. The provision quoted above does not distinguish between types of cookies or between categories of end equipment.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

There are no specific rules in Latvian laws, where informed consent in context of rules on cookies and spyware would be elaborately explained. Article 7.1(1) of the Law on Information Society Services contains a reference that a person is entitled to receive “clear and comprehensive information regarding the purpose of the aforementioned processing in accordance with the Personal Data Protection Law”.

The Personal Data Protection Law, to which the Law on Information Society Services refers, contains general requirements and standards on the notion of “consent”, which are applicable not only in respect to rules on cookies, but also to rules on sending commercial communications, etc.

Article 2(2) of the Personal Data Protection Law contains the following definition: “Consent of a data subject – a freely, unambiguously expressed affirmation of the will of a data subject, by which the data subject allows his or her personal data to be processed in conformity with information provided by the system administrator in accordance with Article 8 of this Law.” Article 8 of the Personal Data Protection Law further lists the exact information system administrator is obliged to provide to a data subject.

Also, the Data State Inspectorate in its Recommendation on Sending Commercial Communications has provided a brief explanation as to exactly what is understood by the term “consent”. Although the Recommendation is mostly dedicated to explaining Article 9 of the Law on Information Society Services, which implements Article 13 of the Directive 2002/58/EC, it is still rather useful and relevant in order to gain a better understanding on what is “consent” in the context of the rules on cookies.

Additionally, the Article 29 Working Party in its “Opinion 04/2012 on Cookie Consent Exemption” and “Working Document 02/2013 providing guidance on obtaining consent for Cookies” provides an insight on how the informed consent rule should be understood, and Latvian authorities would most likely closely follow the opinion expressed in the said documents.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

| Article 7.1 (2) of the Law on Information Society Services implements the exceptions to the informed consent rule: “The consent referred to in Paragraph one of this Article shall not be necessary, if storage of the information in a terminal equipment or access to the information stored in a terminal equipment is required for the purposes of ensuring of circulation of the information in the electronic communications network or for intermediary service provider in order to provide a service requested by a subscriber or user.” |

Therefore, it may be concluded that the second sentence of the Article 5 (3) of the Directive 2002/58/EC is implemented into Latvian legislation correctly, and the Law on Information Society Services does not contain any additional exceptions to the informed consent rule.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

In practice we have observed that a number of Latvian websites provide information that a website contains cookies. However, the manner in which the relevant information on cookies is provided mostly tends to be rather brief and the consent necessary often cannot be considered to be validly obtained. The manner in which the information is provided and the consent is “obtained” is often far from conformity with the Article 29 Working Party “Working Document 02/2013 providing guidance on obtaining consent for cookies”. For example, as observed on several Latvian websites, it is not a common practice in Latvia to explicitly obtain the consent of a user (by providing a box to tick, etc.), mostly Latvian websites merely contain a disclaimer “The website contains cookies, which are necessary in order to identify a user” or a similar disclaimer. (See for example rule 3.11. in the following website: [http://www.juristavards.lv/redakcija.php?zina=5](http://www.juristavards.lv/redakcija.php?zina=5)).

Latvian websites usually do not contain tools such as splash screens, banners, model dialog boxes, etc., to obtain active consent of a user. Another aspect that must be highlighted is the fact that the information on cookies usually can be obtained by reading the terms of use of the specific website. These observations allow concluding that in Latvia it is common to only provide a notice stipulating that by using the website the user agrees to the cookies being set by the websites. However, such practice, where a website merely contains information that the website uses cookies, is not in line with the requirement set out in the Article 29 Working Party “Working Document 02/2013 providing guidance on obtaining consent for cookies” that in order for the consent of a user or subscriber to be considered as valid, the said consent must be given via active actions of a user or subscriber.

The abovementioned problems might exist due to fact that in practice it is unclear, which authority holds the responsibility for enforcing the rules on cookies. Moreover, the Law on Information Society Services does not clearly state the authority responsible for enforcing the rules on cookies.

To our knowledge there are no publicly available data, statistics or surveys on users’ views or on what percentage of users refuse or accept cookies.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>To our knowledge none of the enforcement authorities mentioned under section A of this document have ever issued any guideline or recommendation regarding cookies. The only relevant information found regarding this subject is Article 29 Working Party “Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential”, which is referred to on the website of the Data State Inspectorate. This indicates that Data State Inspectorate closely follows the activity of the Article 29 Working Party, yet so far the authority has not produced its own opinion or recommendation on this subject.</td>
</tr>
<tr>
<td>b.</td>
<td>We are not aware of any existing case law regarding enforcement of the Article 7.¹ of the Law on Information Society Services.</td>
</tr>
</tbody>
</table>
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

| a. In our opinion currently the rules on cookies are rather brief and vague. During our research it has transpired that in practice the application of Article 7.1 of the Law on Information Society Services has not been further detailed in any other Latvian laws, thus creating room for uncertainty regarding its application. Also, neither the Data State Inspectorate, nor any other responsible authority, has issued any guidance or recommendation regarding the application of the Article 7.1 of the Law on Information Society Services. This may be the one of the reasons why up to the present moment there has been no relevant case law in Latvia regarding application of the said Article. Furthermore, the Law on Information Society Services does not clearly state the authority responsible for ensuring and supervising the compliance with the said provision nor does it provide specific duties and rights to a specific authority in ensuring compliance with this provision. Two contradicting views were obtained regarding which authority in practice is responsible for supervising the compliance with the rules on cookies. The Data State Inspectorate claimed that this task is not within its field of competence, whereas the Ministry of Transport stated that it is the duty of the Data State Inspectorate to supervise the compliance with the rules on cookies. Thus, without continuous supervision of these provisions and specific guidelines these provisions lack efficiency which is demonstrated by the often non-compliant practice of website owners highlighted above.

b. Firstly, as regards possible improvements of the legal framework regulating cookies, our suggestion is to add a provision of the law which would clearly indicate the authority, which holds the responsibility for supervising and enforcing rules on cookies. Secondly, it would be advisable to include provisions which in a detailed manner would explain the action a provider must take in order to ensure informed consent from users. |
### C. Traffic data

<table>
<thead>
<tr>
<th><strong>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 1(1)(29) of the Electronic Communications Law defines traffic data in the following manner: “any information or data, which is processed in order to transmit information over an electronic communications network or to prepare bills and register payments, except the content of the transmitted information.”</td>
</tr>
</tbody>
</table>

By comparing the definition of “traffic data” provided by the Directive 2002/58/EC and Article 1(1)(29) of the Electronic Communications Law, it may be concluded that the wording of the Latvian law slightly differs from the wording used in the Directive, however, the meaning of these definitions remains identical. Nevertheless, Article 1(1)(29) of the Electronic Communications law contains an additional emphasis that content of the transmitted information is excluded from the scope of the definition of “traffic data”.”
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Please see below the citation of the Electronic Communications Law:

**Article 70. “Processing of Traffic Data”**

(1) [3 May 2007]

(2) Traffic data shall be processed in a time period, in which the user or subscriber may dispute the bill and make payments according to the procedures specified in regulatory enactments. In individual cases, it is allowed to process and store the traffic data while objections are being examined and resolved, as well as until the outstanding payments are recovered.

(3) An electronic communications merchant is entitled to process traffic data without making a previous agreement with the user or subscriber only for cost accounting regarding the electronic communications services provided, recovery of payments, examination of objections or provision of interconnections, except in the cases provided for in Paragraph seven, eight and nine of this Article and in Articles 68, 71¹ and 71² of this Law.

(4) Processing of traffic data shall be permitted for the distribution of electronic communications services and provision of value added services, if a user or subscriber to whom such data relates has given a consent before such processing of traffic data in accordance with an entered into electronic communications services contract. The user or subscriber has the right to revoke his or her consent to the processing of traffic data at any time.

(5) [3 May 2007]

(6) A user or subscriber does not have the right to access traffic data and to make corrections therein.

(7) The Regulator has the right to request and receive from electronic communications merchants traffic data for the purpose of examination of interconnection or fraud disputes or issues which is carried out, using the numeration, as well as traffic data that are necessary for examination of the respective application regarding the user who has filed an application with the Regulator.

(8) For the purposes of monitoring of the circulation of electronic communications services, personal data protection and information society services specified in regulatory enactments, the Data State Inspection has the right to request and electronic communications merchants has a duty to provide traffic data within 15 days.
(9) For the purposes of investigation of the violations of the regulatory enactments regarding the financial and capital market, the Financial and Capital Market Commission is entitled, on the basis of the decision by the judge, to request and to receive from the electronic communications merchant the traffic data which are specified in Clause 1 of the Annex No.1 to this Law and sub-clauses 1, 2, 3, 4, 5 and 6 of Clause 2, as well as data which are specified in Clauses 1, 2, 3, 4, 5, 6, 7 and 8 of the Annex No.2.

(10) An electronic communications merchant has no obligation to take additional measures for obtaining of information specified in Paragraph eight and nine of this Article if, while providing electronic communications services the technical equipment of the electronic communications merchant does not generate, process or register it.

(11) The Cabinet shall define the procedure for requesting and transferring of the traffic data to the institutions referred to in Paragraphs eight and nine of this Article.”

Latvian law is in line with the provisions of the Directive. A key difference is that the Latvian provisions do not stipulate for the service provider to inform the subscriber or user of the types of traffic data, which will be processed, and of the duration of such processing as stipulated under Article 6(4) of the Directive. Also the Electronic Communications Law does not expressis verbis provide for anonymisation or erasing of the traffic data when it is no longer needed for the purpose of the transmission of a communication. However, the Latvian law does provide that traffic data shall be processed in a time period, in which the user or subscriber may dispute the invoice and perform payments according to the procedures specified in regulatory enactments and that in individual cases, it is allowed to process and store the traffic data while objections are being examined and resolved, as well as until the time when unpaid payments are recovered. This provision may entail that generally processing, inter alia – storing, of the traffic data is not permissible in all other cases and thus in those situations such data should be erased. Still as of the moment of the writing of this report, there is no case-law or other sources of interpretation for this rule, the exact scope of this rule remains unclear.
### 3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

The Electronic Communications Law does not contain any explicit requirement to anonymise or delete traffic data.

Prior to the Amendments to Electronic Communications Law, which came in force on 7 June 2007, Article 70(1) used to contain the following requirement:

“Traffic data must be deleted or made anonymous as soon as the processing is not necessary any more for transmission of communication, recording of payments for electronic communications services provided, review of complaints, recovery of payments or for providing interconnection.

However, since the date when the abovementioned Amendments to the Electronic Communications Law became legally binding, Article 70(1) has been excluded from the Electronic Communications Law and thus, the requirement to delete or anonymise traffic data no longer exists in the Latvian legislation.

The Electronic Communications Law might have been amended, as described above, due to the fact that Personal Data Protection Law contains Article 10(1)(3) which stipulates that the data controller must ensure that “the personal data are stored so that the data subject is identifiable during a relevant period of time, which does not exceed the time period prescribed for the intended purpose of the data processing”.

<table>
<thead>
<tr>
<th>4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Latvian authority has not issued any guidelines in regard to traffic data. However, it pays close attention to documents issued by the Article 29 Data Protection Working Party, which has issued opinion on apps and smart devices, which inter alia concern also traffic data and location data.(<a href="http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf">http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf</a>)</td>
</tr>
</tbody>
</table>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The protection is not sufficient. Latvian rules do not stipulate for the service provider to inform the subscriber or user of the types of traffic data which will be processed and of the duration of such processing as stipulated under Article 6.4 of the Directive. Also the Electronic Communications Law does not expresiss verbis provide for anonymisation or erasing of the traffic data when it is no longer needed for the purpose of the transmission of a communication.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Article 1(1)(5) of the Electronic Communications Law provides the following definition: “Location data” – data, which is processed in an electronic communications network or processed by using electronic communications services and indicates the location of the terminal equipment of an electronic communications service user. For public mobile electronic communications networks, satellite networks and wireless networks, which are utilised for the distribution of radio or television signals, it shall be the geographic location (address) of the terminal equipment of an user of electronic communications services, whereas for public fixed networks, cable television and cable radio networks, and electricity cable systems to the extent they are utilised in order to transmit electronic communications signals – an address of the connection point.”

The Latvian law, contrary to the Directive, specifies what should be understood as geographic location for different types of networks, however, in our opinion this should not be viewed as a significant deviation from the provisions of the Directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

The Electronic Communications Law provides:

**Article 71.** Processing of Location Data  
(1) The processing of location data, subject to exceptions specified in this Article, shall be permitted only to ensure the provision of electronic communications services.

(2) The processing of location data for other purposes without the consent of a user or subscriber shall be permitted only in such cases, if it is not possible to identify the user or subscriber by using such location data.

(3) The processing of location data for other purposes with the consent of a user or subscriber shall be permitted in the time period, which is necessary to provide value added services.

(4) Prior to the receipt of a consent regarding the processing of location data for other purposes, an electronic communications merchant has an obligation to inform the user or subscriber regarding the type of data to be processed, the purpose and time periods of the processing, as well as regarding the fact of whether the location data will be transferred to third parties for the provision of value added services.

(5) A user or subscriber has the right to revoke his or her consent for the processing of location data for other purposes at any time, notifying the relevant electronic communications merchant of this revocation.

(6) A user or subscriber who has consented to the processing of location data for other purposes has the right to request free of charge that the processing of location data be suspended for a specific time, notifying the relevant electronic communications service provider of this suspension.

(7) An electronic communications merchant may process location data without the consent of the user or subscriber, if the processing of location data is necessary for the State Fire-Fighting and Rescue Service, the State Police, the Emergency Medical Service and the Gas emergency services, the Maritime Search and Rescue Service or the emergency number “112”, as well as the Information Centre of the Ministry of the Interior for the performance of the duties thereof and transferring of such data to the services referred to in this Paragraph of the Article.”

As regards the users’ rights to refuse the processing of location data, the Latvian law provides that this may be done temporarily, but does not specify that the refusal can be made for each connection to the network or for each transmission of a communication as the Directive does.

Concerning third parties, which harvest the data from users’ devices, the law stipulates that user’s consent is necessary before data is transferred to a third party for the purpose of providing the value added service. Other than that the law does not specifically address third party access to
location data. It should be noted that in accordance with the Electronic Communications Law, processing of location data can be done only by registered providers of electric communication services for the purpose of ensuring the provision of the electronic communication service. In all other cases a prior consent of the data subject is required or the data needs to be made anonymous.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Yes - Section 71 (2) of Electronic Communications Law provides that: “The processing of location data for other purposes without the consent of a user or subscriber shall be permitted only in situations where it is not possible to identify the user or subscriber by using such location data.”
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

- a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
- b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>a. The Latvian authority has not issued any guidelines in regard to location data. However, it pays close attention of documents issued by the Article 29 Data Protection Working Party, which has issued opinion on apps and smart devices, which inter alia concern also traffic data and location data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. To our best knowledge there is no case-law of Latvian courts on the interpretation and application on ‘location data rules’.</td>
</tr>
<tr>
<td>5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>In our opinion the Latvian law offers appropriate protection of location data.</td>
</tr>
</tbody>
</table>
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. As regards Article 13 of the Directive 2002/58/EC on unsolicited communications, it was transposed into Law on Information Society Services by the Amendments of 10 November 2005 to the Law on Information Society Services. The definition of the term “electronic mail” was also transposed by the same amendments.

   Article 9 of the Law on Information Society Services stipulates:

   “(1) It is prohibited to use automated calling systems (terminal equipment) that operate without human intervention (automatic calling machines), electronic mail or facsimile machines (fax) which allow an individual contact with a recipient of a service for sending of a commercial communication, if the recipient of a service has not given prior free and express consent.

   (2) A service provider who within the framework of his or her commercial transactions has obtained electronic mail addresses from recipients of a service may use them for other commercial communications, provided that:

   1) commercial communications are sent for similar products or services of the service provider;

   2) a recipient of a service has not initially objected to further use of electronic mail address;

   3) a recipient of a service explicitly has given free of charge opportunity to withdraw from further use of electronic mail address upon each further receipt of a commercial communication (filing an application or sending a notification electronically).

   (3) Other forms of communication, by using publicly available electronic communication services for sending of a commercial communication may occur, if the recipient of a service has given prior free and express consent, except for the cases referred to in Paragraph one and two of this Article.

   (4) It is prohibited to use electronic mail or other forms of communication, by using publicly available electronic communication services, for sending of a commercial communication, if invalid electronic mail address, invalid phone or fax number is used to which the recipient of a service may send a request to cease such communication or if refusal by the recipient of a service from further receipt of commercial communications is not taken into account.

   (5) Each sending of prohibited commercial communication constitute a separate breach.

   (6) Prohibitions and restrictions specified in Paragraph one, two and three of this Article shall apply to sending of the commercial communications to natural persons.”

   b. Please note that in the Law on Information Society Services term “commercial communications” is used instead of the term “unsolicited communications”, and, therefore, in the answers to the questions below term “commercial communications” will be used.

   Article 1(3) of the Law on Information Society Services defines commercial communications as “any form of communication in electronic form designed to promote, indirectly or directly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft
activity or exercising a regulated profession. Information allowing direct access to general information about the service provider and the activities thereof (domain name or electronic-mail address) shall not be regarded as a commercial communication”. The initial annotation to the Law on Information Society Services contains an explanation that the Law on Information Society Services contains provisions transposing the Directive 2000/31/EC. Therefore, the definition of the term “commercial communications” is the result of the implementation of Article 2(f) of the Directive 2000/31/EC into the Latvian law. Thus the term “unsolicited communications” has not been additionally transposed into Latvian law and the term “commercial communications” is employed instead.

Additionally, please also be aware that the rules on the “soft opt-in” have been implemented into Law on Information Society Services only recently (in 2009), and it took place later than it was prescribed by the Directive.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>Article 13(1) of the Directive 2002/58/EC has been transposed by Article 9(1) of the Law on Information Society Services as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“It is prohibited to use automated calling systems (terminal equipment) that operate without human intervention (automatic calling machines), electronic mail or facsimile machines (fax) which allow an individual contact with a recipient of a service for sending of a commercial communication, if the recipient of a service has not given prior free and express consent.”</td>
</tr>
<tr>
<td>By comparing the respective provisions of the Directive and the Law on Information Society Services, it may be concluded that Article 13(1) of the Directive 2002/58/EC has been fully implemented into Latvian legislation. However, it may also be concluded that the Law on Information Society Services does not contain any additional requirements and does not list any additional means of communication.</td>
</tr>
<tr>
<td><em>In addition it is important to note that pursuant to Article 8(1) of the Law on Information Society Services a commercial communication must be in compliance with the requirements set forth by the Advertising Law. Therefore, in Latvia it is not sufficient to send commercial communications only via lawful electronic means, the content of electronic communications must also be in line with the applicable legislation regarding advertising.</em></td>
</tr>
</tbody>
</table>
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

<table>
<thead>
<tr>
<th>Article 9(2) of the Law on Information Society Services contains an exception (three cumulative conditions) to the opt-in consent mechanism, which is in line with Article 13(2) of the Directive 2002/58/EC:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“A service provider who within the framework of his or her commercial transactions has obtained electronic mail addresses from recipients of a service may use them for other commercial communications, provided that:</td>
</tr>
<tr>
<td>1) commercial communications are sent for similar products or services of the service provider;</td>
</tr>
<tr>
<td>2) a recipient of a service has not initially objected to further use of electronic mail address;</td>
</tr>
<tr>
<td>3) a recipient of a service explicitly has given free of charge opportunity to withdraw from further use of electronic mail address upon each further receipt of a commercial communication (filing an application or sending a notification electronically).”</td>
</tr>
<tr>
<td>Data State Inspectorate in its Recommendation on “Sending Commercial Communications” emphasizes that upon evaluating, whether products or services are similar within the meaning of the Law on Information Society Services, the opinion and interests of the possible recipient must be estimated and not the interests of the sender of commercial communications.</td>
</tr>
<tr>
<td>Additionally, according to the Law on Information Society Services, different rules apply based on whether commercial communications are being sent to natural or legal persons. Stricter rules apply in regard to sending commercial communications to natural persons. This distinction between natural and legal persons was introduced by the Amendments of 12 June 2009 to the Law on Information Society Services, prior to these Amendments same rules applied in regard to both natural and legal persons.</td>
</tr>
<tr>
<td>Article 9(4) in conjunction with Article 9(6) of the Law on Information Society Services allows sending commercial communications to legal persons without obtaining prior consent, however, as in respect to natural persons, legal persons also must be provided with the opportunity to refuse the receipt of future commercial communications.</td>
</tr>
<tr>
<td>Therefore, in Latvian Law there are no any additional requirements or derogations from the provisions of the Directive 2002/58/EC on exceptions to the opt-in consent mechanism.</td>
</tr>
</tbody>
</table>
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Law on Information Society Services does not provide a distinction between certain communication channels.

Article 1(3) of the Law on Information Society Services lists “electronic form” as one of the constituting elements of the term “commercial communications”. An important issue is the fact that Latvian legislation does not contain a straightforward answer on which communication channels are encompassed by the term “electronic form”. As Date State Inspectorate elaborately explains in its Recommendation on “Sending Commercial Communications”, the meaning of this term may be revealed by analysing Articles of the Law on Information Society Services in conjunction with Articles of the Electronic Communications Law.

Thus, Data State Inspectorate has compiled an exemplary list as to which means of communication are commonly understood by the term “electronic form”:

1) automated calling systems (terminal equipment) without human intervention (automatic calling machines);
2) electronic mail;
3) facsimile machines (fax);
4) other publicly available electronic communication services;

The Electronic Communications Law contains a very wide list of electronic communication services and thus creates a false impression that a commercial communication may be any information that is distributed by using any publicly available electronic communications services. However, as the Data State Inspectorate emphasizes in its Recommendation, information transmitted via publicly available means of communication, such as television, radio or internet (where a person cannot choose a content of this information) shall not be regarded as constituting “electronic communication”.

During the research we managed to find a recent court case (the Judgement of 25 January 2013 of the Regional Administrative Court, case No. A420617510), which is rather controversial due to the fact that the court considered that the term “commercial communications” also covers situations where a banner is posted on a website. In this case the Regional Administrative Court established that, although the plaintiff argued that a banner on an internet website cannot be considered as an advertisement, since Latvian legislation does not provide a definition of the term “banner”, the determining factor is the content of the said banner (a link to the website of a plaintiff and information that the plaintiff provides consumer crediting services). Thus, the Court concluded that the banner in question was, in fact, an advertisement and, simultaneously, a commercial communication. However this judgement should be viewed under strict scrutiny. It could be argued that such a conclusion of the court is contrary to the understanding of what constitutes “commercial communication”. Furthermore in practice this would mean that in order to post a banner on a website, it would be necessary to obtain a consent from every person who visits the website where the banner is placed.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. In 2009 the Data State Inspectorate issued a Recommendation on “Sending commercial communications” (hereinafter – the Recommendation). This Recommendation generally outlines and explains the requirements and rules contained in Article 9 of the Law on Information Society Services. The objective of the Recommendation is to analyse the term “commercial communication”, as well as list all the requirements, which need to be complied with in order for commercial communications to be in line with the relevant legislation. Thus, the Recommendation is mainly directed towards undertakings, organizations or other persons that send out commercial communications with the aim to advertise and promote their products or services. The Data State Inspectorate has to a considerable extent based its Recommendation on the Preamble of the Directive 2002/58/EC, Directive 95/46/EC, as well as on the Opinion of the Article 29 Working Party.

b. In Latvia the case law on “commercial communications” is rather scarce. So far there have been only few cases dealing with the application of the Article 9 or Article 1(1)(3) of the Information Society Services.

Most case law of Latvian courts on commercial communication originates from appeals of the Consumer Rights Protection Centre decisions where the authority has analysed compliance of commercial communications with the notions under Advertising law. In these cases Latvian courts usually establish whether a specific communication may be considered as “commercial communication” pursuant to the Law on Information Society Services and afterwards review whether the content of the said commercial communication (which is simultaneously regarded as an advertisement) is in line with the provisions of the Advertising Law. See, e.g., the judgements in the following cases:


Another case of the Administrative court, which was resolved on the application of Article 9 of the Law on Information Society Services, can be highlighted (the Judgement of 1 February 2010 of the District Administrative Court, case No. 42556308). In this case the District Administrative Court dismissed the plaintiff’s argument claiming that they, as a legal person, should not be fined. The argument was based on a fact that commercial communication was sent outside the official office hours, i.e. on a weekend. The court dismissed this argument by observing that it was the plaintiff’s board member who sent the said commercial communication, and it was advertising the plaintiff’s commercial services. Thus, the District Administrative court established that the time when the commercial communication is sent may not be used as an excuse to avoid liability.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| In our opinion, in general, the rules on unsolicited commercial communications are clear, effective, logically consistent and appropriate to protect privacy in Latvia. Several Administrative court cases also indicate the same. However, as illustrated in the answer to Question E4 above, some interpretations of the concept of “commercial communications” by the Latvian courts are debatable and, thus, further clarity on this subject may be required. |  
|---|---|
| Additionally, currently there are on-going discussions, regarding which authority would be better suited for supervising the compliance with the provisions on commercial communications. At the moment the Data State Inspectorate is mandated to investigate non-compliance with the provisions on commercial communications, however, the responsible authority considers the Consumer Rights Protection Centre to be better placed to have the responsibility for supervising the compliance with the said provisions. |  |
COUNTRY REPORT
MALTA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Olga Finkel, WH Partners

Date: 09 September 2014
Contents

Part 1: Management summary for Malta ................................................................. 3
Part 2: Answers to the questionnaire ................................................................. 4
Part 1: Management summary for Malta

The transposition of the ePrivacy Directive into Maltese law can be summarized as follows:

- The provisions with regard to the scope of the Directive have been transposed in line with the Directive by the Processing of Personal Data (Electronic Communications Sector) Regulations. The Data Protection Commissioner is the sole regulator on data protection matters, however, certain specific aspects of ePrivacy Directive fall under the competence of Malta Communications Authority, the NRA in terms of the Electronic Communication Sector. While the range of persons responsible for compliance with the Regulations appears to extend, for some provisions (e.g., relating to cookies), to information service providers (and the current interpretation of the law seem to be consistent with this approach), the overall scope of the applicability of the Regulations appears to limit their reach by stating that they apply only when processing is done in connection with the provision of electronic communication service. The Data Protection Commissioner generally adopts Art.29 Working Party’s opinions and guidance.

- Confidentiality of communications are enshrined in Maltese law, both as a result of the transposition of e-Privacy Directive and independently from it. Art. 5.3 of the Directive (about “cookies” etc.) has been transposed into Maltese law more or less verbatim and, consequently, is lacking in details and not very useful for the purposes of practical application. Coupled with the low level of awareness and lack of effective means of enforcement, this provision has been largely ignored.

- With respect to traffic and location data, the rules, once again, have been implemented more or less literally as stated in ePrivacy Directive. While the application of these rules by the providers of certain electronic communications network and services (e.g., mobile operators) has been quite uniform (especially after the data retention rules have been established), the same cannot be said about other providers (e.g., mobile application providers). In particular with respect to location data other than traffic data, there is low level of awareness and the enforcement is practically non-existent.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications sent to non-customers via specified means (electronic mail, fax, automated calling machine) have been transposed with opt-in approach imposed in relation to both natural and legal persons. Sending of unsolicited communications via other means or to existing customers for promotion of other products or services is subject to opt-out rule.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English

- the short title of the law in English

- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Directive 2002/58/EC was initially transposed into Maltese legislation in 2003, when Malta was not yet a member of the European Union, but was in the process of aligning its legislation with the acquis communautaire, by

  o ‘Processing of Personal Data (Telecommunication Sector) Regulations’, (Legal Notice 16/2003 - subsidiary legislation), which was renamed in 2004 as ‘Processing of Personal Data (Electronic Communications Sector) Regulations’ (to be referred to as “PPD(ECS) Regulations”) issued under the Data Protection Act (“DPA” – primary legislation); and

  o ‘Telecommunications (Personal Data and Protection of Privacy) Regulations’, (Legal Notice 19/2003 - subsidiary legislation), which was later renamed as ‘Electronic Communications (Personal Data and Protection of Privacy) Regulations’ (to be referred to as “EC(DPP) Regulations”) issued under the Telecommunications (Regulation) Act (now – Electronic Communications (Regulation) Act) (Chapter 399 of the Laws of Malta).

  o More generic applicable definitions relevant to the scope of application (such as defining electronic communications networks and services) have been included in the Electronic Communications (Regulations) Act

- In 2008, PPD(ECS) Regulations were amended by Legal Notice 198 of 2008 and EC(DPP) were amended by Legal Notice 199 of 2008 to implement data retention provisions.

- As stated above, the initial transposition of Directive 2002/58/EC in 2003 was such that the provisions of the Directive 2002/58/EC were split into two legal notices: one under the Data Protection Act, and one under the Electronic Communications Act. The PPD(ECS) Regulations dealt with traffic data,
location data, directories of subscribers, unsolicited communications. EC(DPP) Regulations dealt with security of processing and obligation to inform about a situation that may lead to a security breach, itemised billing, presentation and restriction of calling and connected line identification. Moreover, the definitions contained in Directive 2002/58/EC were to a large extent duplicated in both legal notices (i.e. in PPD(ECS) and in EC(DPP)).

- As a result of the dual transposition under different primary legislative acts, the matters covered by Directive 2002/58/EC ended up being split under the competence of two different and separate competent regulatory bodies: matters covered under PPD(ECS) Regulations fell under the competence of the Data Protection Commissioner, while matters under EC(DPP) Regulations fell under the Malta Communications Authority – the authority supervising the electronic communications sector.

- In 2006, certain specific provisions relevant for this study have been included in the Electronic Commerce (General) Regulations (as amended).

- In 2011, the matters within the scope of this study, including the provisions of Directive 2009/136/EC, were transposed by Legal Notice 239 of 2011 and incorporated into PPD(ECS). Upon amendments introduced by Legal Notice 429 of 2013, the PPD(ECS) Regulations now explicitly state that the Regulations implement Directive 2002/58/EC, as amended by Directive 2009/136/EC and that the Regulations are to be read in conjunction with the requirements of the Commission Regulation (EU) 611/2013.

- Another change made in 2011 was that, by legal notice 273 of 2011, the matters previously regulated by EC(DPP) Regulations were incorporated into Electronic Communications Networks and Services (General) Regulations (to be referred to as “ECNS(G) Regulations”) under the Electronic Communications (Regulation) Act.

- The table below refers only to the substantive legislative instrument currently containing the relevant provision.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>
Art. 3 (Scope)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 3.  

Art. 5.1 (Confidentiality)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 4(1).  

Art. 5.2 (Business exception)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 4(2).  

Art. 5.3 (Cookies)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 5.  

Art. 6 (Traffic data)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 6.  

Art. 9 (Other location data)  
Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 273/2011, as amended), Reg. 57(2).  
Art. 13 (Unsolicited communications) Processing of Personal Data (Electronic Communications Sector) Regulations (L.N. 16/2003, as amended), Reg. 9., Reg. 11, Reg.16

Electronic Commerce (General) Regulations (L.N. 251/2006, as amended), Reg 6

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language

b. the English translation of the short name

c. the part or the provision(s) of the ePrivacy Directive it supervises

d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and Data Protection Commissioner</td>
<td>IDPC</td>
<td>All matters regulated under the Data Protection Act and subsidiary legislation issued thereunder, including under the Processing of Personal Data (Electronic Communications Sector) Regulations’ (“PPD(ECS) Regulations”). The matters regulated by the Malta Communications Authority (see</td>
<td><a href="http://idpc.gov.mt/">http://idpc.gov.mt/</a></td>
</tr>
</tbody>
</table>
Malta | MCA
---|---
Communications Authority | All matters regulated under the Electronic Communications Sector (Regulation) Act and subsidiary legislation issued thereunder, including under the Electronic Communications Networks and Services (General) Regulations (“ECNS(G) Regulations”). None of the matters which are the focus of this study are under MCA competence.

**Explanation:**

- The Malta’s Information and Data Protection Commissioner (idpc.gov.mt) is the supervisory body for all matters regulated under the Data Protection Act. This includes all matters under ePrivacy Directive except for those that fall under the remit of the Malta Communications Authority.

- The Malta Communications Authority is the national NRA for the supervision of the electronic communications sector and is a competent authority for matters under ePrivacy Directive which have been implemented under the Electronic Communications Sector (Regulation) Act. These are matters relating to security of processing, itemised billing, presentation and restriction of calling and connected line identification, automatic call forwarding, technical features and standards.

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

According to Reg 3 of PPD(ECS) Regulations, these Regulations apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, including networks supporting data collection and identification devices. It is the same as in Article 3 of the ePrivacy Directive.

Article 2 of the Electronic Communications (Regulation) Act (‘ECRA’) contains the following definitions:

“Public communications network” means electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points.

“Electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit-switched and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

Therefore, any network, including networks used for broadcasting, falls under the scope.

“Electronic communications service” means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in the Electronic Commerce Act, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

“Publicly available electronic communications service” means an electronic communications service available to the public.

The ECRA defines also an operator: “operator” means an undertaking providing or authorised to provide a public communications network or an associated facility; while “provision of an electronic communications network” means the establishment, operation, control or making available of such a network.

In addition, one can easily establish the reach of the ‘provision’ of a publicly available electronic
communication services’ with reference to the definition of said service.

4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

If the scope of the service in question falls within the definition of ‘electrical communications service’, i.e. if the service consists wholly or mainly in the conveyance of signals on electronic communications networks, then such service, be it VoIP, webmail, location based services or any other, will be within the scope of the implementing legislation. Conversely, if the service provided is more focused on content – it would be outside the scope.

5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

The PPD(ECS) Regulations apply to processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks ‘in Malta and in any other country’, which has been understood to apply at least throughout the European Union, even though there has not been any official pronouncement to this effect.

Presumably, the law applies to the providers of the said service, as the enforcement actions are envisaged against providers of such service if they are in breach. Therefore, it appears that as far as processing of personal data occurs in a network, non-Malta based operators, in particular when the equipment used for the processing of personal data is situated in Malta, even minimally, should be subject to the PPD(ECS) Regulations when they provide relevant services to persons in Malta. It must be noted that there is no case-law on this point.

On the other hand however, as a matter of general principle, laws are applied on the basis of the territorial principle and, therefore, within Malta only. This principle must be applied to the PPD(ECS) Regulations, especially due to the fact that to-date, the Minister responsible for freedom of information and data protection has not designated any countries, explicitly falling within the PPD(ECS) Regulations, whether within the European Union or otherwise. Accordingly, only operators who engage in processing of personal data in Malta or, operators whose main place of establishment is outside of Malta but who have equipment used for processing in Malta are
considered as ‘data controllers’ under the Data Protection Act and must be registered with the Data Protection Commissioner. In practice, not all providers of relevant services who are based outside of Malta are registered as data controllers and, therefore, in such case the Malta’s Data Protection Commissioner does not have jurisdiction over them.

The perceived ‘extraterritorial’ application of PPD(ECS) Regulations has been interpreted to apply in so far as (a) persons outside of Malta whose rights have been prejudiced by a breach of Malta-based provider have the right to complain against a Malta-based provider and bring action in Malta and (b) persons whose rights have been prejudiced by a breach of non-Malta-based provider may complain against a non-Malta operator in Malta and can expect the Data Protection Commissioner to direct them to a proper regulatory body in the country of the non-Malta provider to assist the individual.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

   a. There has been no guidance on these matters

   b. We are not aware of any case law in Malta dealing with these issues

7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

   a. (1) The fact that the competence over the privacy in the electronic communications services and networks is somewhat split between DPC and MCA leads to some confusion and make complaints more difficult, as an individual may not know to which authority to apply in relation to which issue. (2) The Malta Data Protection Commissioner does not have sufficient powers and competence to be effective with respect to non-Malta based providers.

   b. (1) The current framework should apply equally to information society service providers and electronic communications service providers. (2) There should be more uniform and
equitable provisions with respect to dealing with providers in breach due to cross-border activity. Currently, it appears that there is a lot of potential for loop-hole exploitation. (3) More effective rules to apply to non-EU providers processing personal data of EU data subjects should be established.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Reg. 4(1) of PPD(ECS) Regulations stipulates that no person other than the user shall listen, tap, store or undertake any other form of interception or surveillance of communications and of any related traffic data without the consent of the user concerned. ‘Communication’ is defined by PPD(ECS) Regulations as ‘any information exchanged or transmitted between a finite number of parties of a publicly available electronic communications service’, but excluding any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.

One can note that no intent of any kind is relevant or required to be proven here - the mere acts of interception or surveillance are prohibited.

Violation of the prohibition is an administrative offence punishable with an administrative fine not exceeding €23,293.73 for each violation and €2,329.37 for each day during which such violation persists.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

This exception has been transposed by Reg 4(2) of PPD(ECS), which states that legally authorised recording of communications and the related traffic data in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication is allowed. Data required for the billing and interconnection purposes may be process but only up to the end of the period during which the bill may be lawfully challenged or payment pursued (Reg. 6(2)) and the provider must inform the subscriber or user of the type of data being processed and of the period during which it is processed.

Furthermore, Reg. 18 of PPD(ECS) stipulates that a provider of publicly available electronic communications services or of a public communications network shall retain certain types of data pursuant to Directive 2006/24/EC, which includes data generated or processed in the process of supplying the communications services concerned for one year (for communications data relating
to fixed, mobile and internet telephony) or for six months (for communications data relating to internet access and emails).

The above exceptions to the rule of prohibition of interception and surveillance do not extend to the content of communication and, in terms of Reg. 18(3) of PPD(ECS), no data revealing the content of any communication may be retained.

3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The principle of confidentiality of communications enshrined in Art 5(1) of the ePrivacy Directive and implemented by Reg 4(1) of DDR(ECS) Regulations, is restricted not only by Reg 4(2) of PPD(ECS).

Confidentiality of communications does not apply when (in terms of Reg 10 of DDR(ECS) Regulations) any law specifically stipulates the provision of information as a necessary measure in the interest of:

a. National security;

b. Defence;

c. Public security;

d. The prevention, investigation, detection and prosecution of criminal or administrative offense, or of breaches of ethics for regulated professions;

e. An important economic or financial interest including monetary, budgetary and taxation matters;

f. A monitoring inspection or regulatory function connected, even occasionally, with the exercise of official authority referred to in paragraphs (c), (d) and (e); or

g. The protection of the subscriber or user of the rights and freedoms of others.

Storing of related traffic data is allowed for the purposes of checking the security and proper functioning of the networks.

Furthermore, interception, including of the content of communications, is deemed legal and allowed if authorised under the Security Services Act by the Security Service, under a relevant warrant. Moreover, the Malta Communications Authority is authorised to devise technical and operational requirements (which it did) for operators to enable legal interception by competent authorities. In practice, the Security Services have set up a system with every network provider,
which allows it to tap into communications directly without the knowledge or involvement of the network in each case.

4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. (1) The Maltese legislation does not explicitly address ‘automated breaches of confidentiality without human intervention. In principle such breaches of confidentiality will be considered as a sub-type of a generic breach of Reg 4(1) of DDR(ECS) Regulations, provided it does not fall under any exemptions. In this respect, the type of network is irrelevant.

(2) The prohibition of interception of the content of a communication is stronger than the prohibition related to traffic data and has fewer exceptions to it. As such only the competent authorities under a warrant are authorised to intercept content of a communication without consent.

b. (1) Malta’s Criminal Code provides for an offence consisting of an unauthorised access to information by any technical means, interception by technical means of a non-public transmission of data.

(2) The Security Service Act makes interception of or interference with communications in the course of their transmission by post or my means of a radio-communications or telecommunications system or by any other means unlawful, unless such interception or interference is authorised by a warrant.

(3) The Postal Services Act makes in an offence to malicious open or cause to open any postal article.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Reg 5(1) of PPD(ECS) Regulations provides that the storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his consent, having been provided by the controller with clear and comprehensive information in terms of Article 19 of the Act. Article 19 of the Data Protection Act requires the data controller to provide at least the following information:

   (1) the identity and habitual residence or principal place of business of the controller and of any other person authorised by him in that behalf, if any;

   (2) the purposes of the processing for which the data are intended; and

   (3) any further information relating to matters such as:

      (i) the recipients or categories of the recipients of data;

      (ii) whether the reply to any questions made to the data subject is obligatory or voluntary, as well as the possible consequence of failure to reply; and

      (iii) the existence of the right to access, the right to rectify, and, where applicable, the right to erase the data concerning him, and, insofar as such further information is necessary, having regard to the specific circumstances in which the data is collected, to guarantee fair processing in respect of the data subject.

Accordingly, if the data controller has not provided all information stated above in (1), (2), (3) – the user’s consent would not be considered as given.

Reg 5(2) of PPD(ECS) Regulations limits the scope of application of Reg 5(1), by stating that Reg 5(1) shall not prevent the technical storage of access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network or as may be strictly necessary in order for the service provider to provide an information society service explicitly requested by the subscriber or user to provide the service.
b. Maltese law does not distinguish between various types of cookies and/or various types of devices.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

The law does not explicitly address any of these questions. The Malta’s Data Protection Commissioner has not issued guidance on the subject. Instead, the Art 29 Working Party’s Guidance 02/2013 WP 208 has been accepted as applicable.

7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent (i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

The law does not explicitly address any of these questions. The Malta’s Data Protection Commissioner has not issued guidance on the subject. Instead, the Art 29 Working Party’s Guidance 02/2012 WP 194 has been accepted as applicable.

8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

There has been no local guidance on any issue relating to cookies, so the general guidance used in Malta is that provided by the Art 29 Working Party. There are no statistics on compliance and there have been no complaints or satisfaction surveys locally either.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

   a. The guidance documents by the Art 29 Working Party with respect to cookies (as all other guidance documents provided by the Working Party) have been adopted by the Data Protection Commissioner. There is no other guidance issued.

   b. There is no case law on this topic.

10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

   a. The guidance provided by Art 29 Working Party is not easily applicable by businesses, since it is vague and subject to interpretation itself, and in some respects may be too restrictive. The result is that, in my view, the obligation with respect to obtaining consent for cookies has been largely ignored; and there has been no enforcement.

   b. (1) I believe that, even though it appears that the rules should apply also to information society service providers, strictly speaking, the overall scope of e-Privacy Directive is to apply to providers of electronic communications networks and services and, therefore, at least in some cases the intended effect is not achieved. The rights of users would be better protected if the obligation is imposed also to information society service providers directly. In other words, the scope should be clearly and unambiguously widened. (2) The rules must be simplified and simple practical examples of implementation should be provided via guidance documents. (3) The scope of information to be provided to a user should be reduced to something that is actually possible to include in a simple one-time banner or message, including on a mobile device.

C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

‘Traffic data’ is defined in Reg 2 of PPD(ECS) Regulations as ‘any data processed for the purposes of the conveyance of a communication on an electronic communications network or for the billing
thereof’.

This Regulation also defines ‘value added service’ as ‘any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

The above definitions are the same as in the ePrivacy Directive.

2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

In terms of Reg (6)(1) of PPD(ECS) Regulations, traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by a undertaking which provides publicly available electronic communications services or by an undertaking which provides a public communications network shall be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. This provision is without prejudice to the following:

1. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed provided that such processing shall only be permissible up to the end of the period during which the bill may lawfully be challenged or payment pursued.

2. For the purpose of marketing its own electronic communications services or for the provision of value added services to the subscriber, the undertaking which provides publicly available electronic communications services may process the data referred to in Reg (6)(1) to the extent and for the duration necessary for such services, provided the subscriber has given his consent.

3. The undertaking which provides publicly available electronic communications services shall inform the subscriber or user of the types of traffic data that are processed and of the duration of such processing for the purposes mentioned in point 1 above and, prior to obtaining consent, for the purposes mentioned point 2 above.

Processing of traffic data under Reg (6)(1) and under any of the above three points shall be restricted to persons acting under the authority of undertakings which provide publicly available electronic communications and of undertakings which provide a public communications network handling billing or traffic management, customer enquiries, fraud detection, marketing the electronic communications services of the provider or providing a value added service, and shall be restricted to what is necessary for the purposes of such activities.

"Consent" means any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed.
Nothing stated above shall preclude the furnishing of traffic data to any competent authority for the purposes of any law relating to the settling of disputes, in particular interconnection and billing disputes.

One difference between the above-stated provisions of PPD (ECS) Regulations and Article 6 of the ePrivacy Directive is that the last sentence of Article 6.3 (‘Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time’) has been omitted. However, this requirement to allow for withdrawal of consent at any time is generally provided for, with respect to processing of any personal data and therefore including traffic data, with the limitation that such withdrawal is not possible to the extent that processing of traffic data is necessary (for conveyance of communication and billing purposes).

3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Subject to the 3 points stated in the previous question when traffic data can be kept longer, Reg (6)(1) of PPD(ECS) Regulations requires traffic data of a subscriber or user to be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

Early on, prior to data retention periods being established in the law, mobile operators lobbied to allow traffic data processed for the purposes of billing to be deleted sooner rather than later. The basis for this claim was the costs involved in keeping massive volumes of data, especially in view of frequent upgrades and changes of their billing and other systems, which necessitated placing old data in archiving mode and keeping systems available to restore it when requested. At that period of time, the Malta police was placing demands on mobile operators to provide high volumes of data covering long time (e.g. 3 years or longer) periods in relation to investigation of offences (which demands, as was ruled by the court in one of these cases, were excessive). The matter was settled by the introduction of definite retention periods for traffic data.

5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The rules are logical and clear, in my view.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

‘Location data’ is defined in Reg 2 of PPD(ECS) Regulations as ‘any data processed in an electronic communications network or by an electronic communications service, indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service.’

The above definition is the same as in the ePrivacy Directive.

2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Under Reg 7 of PPD(ECS) Regulations, where location data other than traffic data relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

For processing with the consent of subscriber or user to take place lawfully, prior to obtaining the consent, the undertaking which provides publicly available electronic communications services shall inform them of the following:

(1) the type of location data other than traffic data, which shall be processed;
(2) the purposes and duration of the processing; and
(3) whether the data shall be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers may withdraw their consent for the processing of location data other than traffic data at any time.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber shall continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

The law also stipulates that the processing of location data other than traffic data in accordance with the above shall be restricted to persons acting under the authority of the undertaking which
provides publicly available electronic communications services or of the undertaking which provides a public communications network or of the third party providing the value added service, and shall be restricted to what is necessary for the purposes of providing the value added service.

The definition and the rules are the same as in the ePrivacy Directive.

The law does not explicitly restrict the applicability of the above provisions to providers of electronic communications networks and services only and the respective penalties apply to ‘any person who contravenes’, so the rules cover even third parties who harvest location data. However, one would need to examine whether such third parties fall within the definition of a provider of an electronic communications services and, therefore, within the overall scope of the Regulations.

Location data is also dealt with by ECNS(G) Regulations, in so far that these Regulations allow operators to process location data irrespective of the user’s or subscriber’s denial of consent for such processing, on a per line basis, for calls made to emergency access numbers for the purposes of responding to such calls; as well as to pass this data to competent authorities in charge of emergency services.

3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Since the Regulations state that location data other than traffic data can only be processed with user or subscriber consent or in an anonymised form, one can conclude that such data must be anonymised as soon as the user’s or subscriber’s consent is withdrawn. A derogation from this rule would be processing of location data in case of calls to emergency services or in relation to responding to emergency services calls.

4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. Malta’s Data Protection Commissioner generally adopts all opinions and guidance provided by Art. 29 Working Party. This includes opinion WP 115 on location data.
b. We are not aware of such decisions

5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

(1) While in some cases the rules are quite clear (for example, when processing is required for emergency services), the growing usage of mobile apps providing location-optimised services require further clarity. Such clarity needs to be established, first and foremost, as to who should comply with the legal obligations to process location-other-than-traffic data only on the basis of consent and as long as such consent is not withdrawn. I believe that, even though it appears that the rules should apply also to information society service providers, strictly speaking, the overall scope of e-Privacy Directive is such as to apply to providers of electronic communications networks and services and, therefore, at least in some cases the intended effect is not achieved. The rights of users would be better protected if the obligation is imposed also to information society service providers directly. In other words, the scope should be clearly and unambiguously widened.

(2) For a small country like Malta, most offenders come from outside of the country and this makes national enforcement almost impossible. Therefore, the rules for cooperation and regulatory action cross-border must be greatly improved to be effective. In this regard, it may be opportune to explore the possibility of extending the scope of the regulatory provisions also to app platforms (such as AppStore or GooglePlay) so that if users have justified complaints, such platforms are forced to remove them from their distribution platform or be subject to regulatory action.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

a.

In terms of Reg (9)(1) of PPD(ECS) Regulations, a person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited communication for the purpose of direct marketing by means of an automatic calling machine; or a facsimile machine; or electronic mail to a subscriber or user, irrespective of whether such subscriber or user is a natural person or legal person, unless the subscriber or user has given his prior consent in writing to the receipt of such a communication.

"Consent" means any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed.

“Electronic mail” is defined as any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient. Therefore any message, test, SMS, MMS, etc, is an ‘electronic mail’.

Reg (9)(2): Notwithstanding Regulation (9)(1), where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the applicable provisions of the Data protection Act, that same person may use such details for direct marketing of its own similar products or services, provided that customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use.

Reg (9)(3): A person who uses or causes to be used any other means of communication other than those stated in Reg (9)(1) and Reg (9)(2) for the purpose of direct marketing shall, at no charge to the subscriber or user, ensure that any such communications to a subscriber or user are not sent if the subscriber or user requests that such communications cease.
In all cases the practice of sending electronic mail for the purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, which contravene the provisions of regulation 6 of the Electronic Commerce (General) Regulations (which prescribes the minimum information to be provided to the recipient of a communication, including clear identification that the communication is a promotional one), or which do not have a valid address to which the recipient may send a request that such communications cease, or which encourage recipients to visit websites that contravene such regulation, shall be prohibited.

b.

From the point of view of the recipient of unsolicited communication, Reg (9)(1) is wider than the minimum required by Article 13(5) of e-Privacy Directive, as Reg (9)(1) applies to both natural and legal persons.

From the point of view of the type of contact, Reg (9)(1) is in line with Article 13(1).

For contacts made by means other than automatic calling machine; or a facsimile machine; or electronic mail (by voice/telephone, for example), the Maltese law adopted opt-out approach, with respect to both natural and legal persons.

In addition to PPD(ECS) Regulations, telemarketing is regulated by Distance Selling Regulations, covering any form or means of consumer solicitation. Under these Regulations, a trader who, in soliciting custom, uses a facsimile machine or an automated calling unit without having first obtained the consent of the consumer is liable for compensation to the consumer for any inconvenience caused and resultant damages suffered.

2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

1. For sending of unsolicited communications via electronic mail (and this includes an SMS or MMS), fax or automated calling machine, prior consent of a subscriber or user must be obtained in case where such subscriber or user is not a customer of the sender (i.e., opt-in principle). Any such communication must also clearly identify the person on whose behalf the communication is made, clearly state, in each communication, that it is a promotional message and conditions for any promotional offer, and clearly state how the subscriber or user can ask that such communications cease. This applies to unsolicited communications to both legal and natural persons.

2. For other means of contact (for example, by telephone call where such call is not
automated), unsolicited communication can be made on the basis of opt-out principle (not opt-in), provided that the customer has been informed about this possibility at the point of electronic contact collection and in every communication.

3. In case where unsolicited communications are sent to a subscriber or user who is already a customer of the person on whose behalf the communication is sent, the rules are the same except that no prior consent (opt-in) is required, but the way to opt-out should still be clearly identified in every communication.

Breach of the above rules is an administrative offence. In addition, a person affected by the breach has the right to compensation for the damages suffered.

3. **Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?**

Reg (9) of PPD(ECS) Regulations provides for the following exceptions to the opt-in consent principle:

1. In cases where all of the below conditions are satisfied:
   a. contact details for electronic mail were obtained by a person (provider) from its customer (whether legal or natural person) in relation to the sale of a product or a service, and
   b. such electronic contact was obtained in accordance with the applicable provisions of the Data protection Act, and
   c. such electronic contact is used by the same person (provider) for direct marketing of its own similar products or services, and
   d. the customer is given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details:
      i. at the time of their collection, and
      ii. on the occasion of each message where the customer has not initially refused such use.

2. In cases where the unsolicited communication is sent to a user or subscriber (natural or legal person) by means other than by electronic email, facsimile or automatic calling machines, provided that
   a. The subscriber or user has not previously requested that such communication ceases; and
   b. The right to request such communication to cease should be provided to the subscriber or user at no charge.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The distinction arises due to the definition “electronic mail”, which is defined as ‘any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient’ – in line with the definition contained in ePrivacy Directive.

Therefore any message, test, SMS, MMS, voice mail, instant message, newsfeed message, Twitter message or any other message fitting into the definition will be treated as an ‘electronic mail’, regardless of the means of sending or channel or network type. Conversely, a call made by a human being over a telephone will not be within the scope of ‘electronic mail’.

5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. In 2004, the National Information Society Council (NISCO) put the issue for discussion on the agenda and subsequently published a consultation document entitled ‘Addressing Spam Together’. The Maltese Data Protection Commissioner generally adopts the guidance issued by Article 29 Working Party, and this includes the Opinion 5/2004 of the Working Party WP 90 on unsolicited communications for marketing purposes. The IDPC has a tool on its website to post users’ experiences with unsolicited communications and to lodge a complaint. While there is a short article on the IDPC website relating to unsolicited communication, it does not really provide any guidance or interpretation of the legal provisions.

b. We are not aware of court case containing interpretation of unsolicited direct marketing
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

From the annual reports of the Maltese IDPC, it transpires that the number of complaints relating to unsolicited communications is not high. In my view, this does not represent the current state of affairs at all. In practice, it is a known fact that the amount of spam is enormous, it is just that complaining to the IDPC is not generally regarded as an effective course of action. To be fair, though, the vast majority of spam emails generally come to Maltese residents from entities established abroad which are, therefore, out of reach of the local authorities altogether.

One type of complaint that the IDPC does deal with in relatively high numbers are complaints relating to spam coming from political parties, normally at the time of general election campaigns. These emails often do not relate to fund raising, etc (and therefore, fall outside of scope of ‘direct marketing’ in terms of the guidance of Art 29 Working Party), but, nevertheless cause great nuisance and raise issues of proper – or otherwise – use of accumulated data by political parties. Naturally, the normal rules on the use of data in accordance with the general principles of data protection can still be enforced, but these rules are less stringent compared to the rules applicable to processing in the electronic communications sector. This raises an interesting question as to whether the interpretation of the scope of ‘direct marketing’ should be widened, or, alternatively, whether the prohibition of unsolicited communication without opt-in should be widened to cover situations where the communication is for a purpose other than direct marketing.
COUNTRY REPORT

The Netherlands

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: mr. dr. Bart W. Schermer, Partner Considerati, Assistant Professor Leiden University

Date: 22 August 2014
Contents

Part 1: Management summary ........................................................................................................... 3
Part 2: Answers to the questionnaire ................................................................................................4
Management Summary for The Netherlands
The transposition of the ePrivacy Directive into Dutch law can be summarized as follows:

- The provisions of the Directive have been transposed into the Dutch Telecommunications Act. This Act forms the general telecommunications framework in the Netherlands. Since some provisions prescribe rules regarding the processing of data (in line with Directive 95/46/EC) the Dutch Data Protection Act is also applicable. Consequently, the NRA (Authority for Consumers and Markets - ACM) and the DPA (College Bescherming Persoonsgegevens – Cbp) are designated to supervise the provisions. Finally, the Radio Communications Agency (Agentschap Telecom) is also competent to enforce some of the provisions, for instance those in the area of confidentiality of traffic and content data.

- The scope of the transposed provisions is largely defined by the definitions mentioned in article 1 of the Telecommunications Act. Almost all provisions are addressed to the ‘provider of a public electronic communications network’. The exact scope of this term is not entirely clear since there haven’t been any judgements or guidance from the NRA. Some provisions have a different scope, for instance article 11.7a of the Telecommunications Act (article 5(3) of the ePrivacy Directive) which is applicable to everyone that wishes to access data stored in the terminal equipment of users.

- Article 5(3) of the Directive has been transposed in article 11.7a of the Telecommunications Act. The Dutch provision contains stricter rules than the provision in the Directive. For marketing purposes the only legal ground according to the DPA is the unambiguous consent of the data subject, a more strict form of consent than the ‘general consent’ of article 5(3) of the Directive.

- The provisions concerning traffic data can be found in article 11.1 – 11.5 of the Telecommunications Act and are formulated in line with the provisions in the Directive. The provisions concerning location data are also laid down in 11.1 – 11.5 of the Telecommunications Act and are formulated in line with the provisions in the Directive.

- The Dutch legislator transposed the provisions concerning unsolicited direct marketing communications into article 11.7 of the Telecommunications Act. The substance and scope of the provision is comparable with the provision in the Directive. The use of terminology is slightly different than the Directive. For example: in the Directive the term ‘direct marketing’ is used, while in the transposed provision the term ‘unsolicited communication for commercial, ideal or charitable goals’ is used. With the aforementioned terminology the Dutch provision seems to be somewhat more precise than the Directive.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Netherlands:
- The provisions in the ePrivacy directive were transposed in the Dutch Telecommunications Act on May 19 2004 (hereinafter: “Telecommunications Act” or “Tw”) via ‘de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002’ (Implementation Act of the European Regulatory Framework for the Electronic Communication Sector).
- Following the 2009 amendment of the European Regulatory Framework for Electronic Communication, the Dutch legislator amended the legal framework. A revision of article 5(3) is pending and currently tabled for discussion in Parliament.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article</td>
<td>Description</td>
<td>Reference</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Art. 3</td>
<td>(Scope)</td>
<td>Not directly transposed into national legislation</td>
</tr>
<tr>
<td>Art. 5.2</td>
<td>(Business exception)</td>
<td>Article 11.5 lid 2 Telecommunications Act</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

- the full name in your national language
- the English translation of the short name
- the part or the provision(s) of the ePrivacy Directive it supervises
- URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoriteit Consumenten Markt (ACM)</td>
<td>Authority for Consumers and Markets (ACM)</td>
<td>Mainly 5(1), 5(2), 5(3) and 13</td>
<td><a href="https://www.acm.nl/en/">https://www.acm.nl/en/</a></td>
</tr>
<tr>
<td>College bescherming persoonsgegevens (Cbp)</td>
<td>Data Protection Authority (Cbp or DPA)</td>
<td>Provisions regarding the processing of personal data (primarily article 5(1), 5(2), 5(3), 6, 9 and 13)</td>
<td><a href="http://www.dutchdpa.nl/Pages/home.aspx">http://www.dutchdpa.nl/Pages/home.aspx</a></td>
</tr>
<tr>
<td>Agentschap Telecommunicatie</td>
<td>Radiocommunications Agency</td>
<td>Article 5(1), 6, 9</td>
<td><a href="http://www.agentschaptelecom.nl/radiocommunications-agency">http://www.agentschaptelecom.nl/radiocommunications-agency</a></td>
</tr>
</tbody>
</table>

Explanation:
- The Netherlands Consumer Authority, the Netherlands Competition Authority (NMa) and the Netherlands Independent Post and Telecommunications Authority (OPTA) joined forces on April 1st 2013, creating a new regulator: the Netherlands Authority for Consumers and Markets (ACM). The ACM is a national supervisory body for the electronic communications sector and responsible for enforcing compliance with the provision of the ePrivacy Directive as implemented in the Dutch Telecommunications Act, in particular article 5(3) and article 13 of the Directive.
- As electronic communications may also entail the processing of personal data, the ACM and Cbp have a cooperation protocol on the manner of cooperation with regards to these cases. [http://www.cbpweb.nl/downloads_samenwerking/samenwerking_opta.pdf](http://www.cbpweb.nl/downloads_samenwerking/samenwerking_opta.pdf) (in Dutch). In case of overlapping competences, the protocol sets as a general rule that the ACM uses its competences primary when the main focus is on the Telecommunications Act, while the Cbp uses its competences when it concerns the application of the Dutch Data Protection Act.

- Article 11.7a Tw (the implementation of article 5.3 of Directive 2009/136/EC) may also be enforced by the Cbp. Article 11.7 Tw (implementation of article 13 of Directive 2009/136/EC) may be enforced by the Cbp if it concerns the processing of electronic contact information for electronic messages.

- Consumers can address signals regarding data protection and privacy related issues to the Cbp. These signals do not lead to an individual treatment of the complaint, but are used by the Cbp to decide their research areas. If there are many complaints on a specific issue, this may trigger an ex officio investigation.

- Complaints with regards to telemarketing and electronic communications have to be addressed to ConsuWijzer, the consumer office from the ACM ([https://www.consuwijzer.nl](https://www.consuwijzer.nl)). These signals do not lead to an individual treatment of the complaint, but are used by ACM to decide their research areas. If there are many complaints on a specific issue, this may trigger an ex officio investigation.

- Complaints with regards to unsolicited messages can also be addressed to Spamklacht, an office related to ACM ([https://www.spamklacht.nl](https://www.spamklacht.nl)).

- the Dutch Radiocommunications agency is responsible for enforcing the requirements in the area of the confidentiality of content, traffic and location data. It also has a cooperation protocol with the data protection authority: [http://www.agentschaptelecom.nl/sites/default/files/samenwerkingsovereenkomst-at-cbp.pdf](http://www.agentschaptelecom.nl/sites/default/files/samenwerkingsovereenkomst-at-cbp.pdf) (in Dutch).
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Article 1.1 under e of the Telecommunications Act defines electronic communication networks as ‘transmission systems, including switching or routing equipment, network elements, inactive network elements and other instruments that allow signals to be transmitted through cables, radio waves, optic or other electromagnetic resources, including satellite networks, fixed and mobile terrestrial networks, electricity nets, to the extent that signals are used for transfer of signals and networks for radio and television broadcast and cable television networks, regardless of the information transmitted’. Additionally, article 1.1 under h, a public electronic communications network is defined as “an electronic communication network that is partly or mainly used to offer public communications services, including a network, destined for distributing programs to the extent that this is offered to the public”.

Article 1.1 under f, defines an electronic communications service as ‘a service, usually offered in return for compensation, which partly or mainly consists of transferring signals through electronic communication networks, including telecommunication services and transmission services on networks used for broadcasting, yet not the service which uses electronic communication networks and services to deliver the transferred contents or does editorial checks.’ Article 1.1, under g, defines public electronic communications services as an ‘electronic communication service available to the public’.

Article 1.1 of the Telecommunications Act does not contain a definition for the provider of an electronic communications service. However, offering a network is defined in article 1.1 under i as: ‘building, exploiting, managing or making available an electronic communication network.’

Since the definitions in the Telecommunications Act are literally implemented from the Framework Directive, there aren’t any differences in the scope.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

The answer to this question depends on whether or not these services are transferring signals through electronic communication networks, including telecommunication services and transmission services on networks used for broadcasting, yet not the service which uses electronic networks and services to deliver the transferred contents or does editorial checks (article 1.1 under f). In general, the question to be answered is whether these services transfer signals through electronic communication networks. With regard to VoIP services they cannot be regarded as a (public) electronic communication service if they only offer the possibility to communicate via a closed protocol (p2p).

This point of material scope raises many questions in practice. This also links in with the Data Retention Directive (2006/24/EC), since a broad interpretation of the material scope also triggers the applicability of the Data Retention Directive. Although the Directive has been declared invalid by a decision of the ECJ, the national implementation of the Data Retention Directive has not yet been repealed.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

In the Dutch Telecommunication Act the territorial scope has not been defined in a separate provision, however the provisions are applicable on activities on the Dutch territory (this can be derived from the documents of the parliamentary process for the Telecommunications Act and the formulation of the definitions). For Bonaire, Sint Eustatius and Saba there is a separate law ‘Wet telecommunicatievoorzieningen BES’. In principle the provisions in the Dutch Telecommunication Act are applicable to providers of a public electronic communications network, providers of a public electronic communication service and to the parties that offer or install the accompanying facilities. They are under the obligation to notify their activities to the ACM. Because of the territorial scope of the provisions it could be possible that national law is applicable to foreign entities, because they have activities on Dutch territory.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

<table>
<thead>
<tr>
<th>a. The ACM has published guidance on the territorial scope of for instance article 11.7 Tw (unsolicited commercial emails) and article 5(3) (cookies) in its FAQs. These can be found via:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.acm.nl/nl/publicaties/publicatie/12768/Veelgestelde-vragen-over-de-cookiebepaling/">https://www.acm.nl/nl/publicaties/publicatie/12768/Veelgestelde-vragen-over-de-cookiebepaling/</a></td>
</tr>
<tr>
<td>(in Dutch)</td>
</tr>
<tr>
<td>b. We are not aware of any case law regarding the scope of the definitions.</td>
</tr>
</tbody>
</table>
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

| a. The distinction between ePrivacy (2002/58/EC, 2009/136/EC) and data protection (95/46/EC) does not make sense anymore. Because of the artificial distinction between ePrivacy and data protection there is an overlap of rules and (depending on national implementation) of enforcement. This leads to problems when it comes to 1) determining the applicability of the rules, 2) the interpretation of the rules and 3) the enforcement of the rules. |
| Ad1 Due to the rapid technological developments in the field of telecommunications the material scope of the Directive has become unclear. In many cases, it is difficult to determine whether an organisation meets the criterion of being an 'electronic communications service'. This issue may lead to an unlevel playing field, given the fact that public communications networks and communication services must follow the rules of the ePrivacy Directive, whereas they may not apply to information society services that perform similar functions, but possibly cannot be characterised as an electronic communications service (e.g. SMS versus online instant messaging). While the definition of an 'electronic communications service' has room for extensive interpretation and could include VOIP, messaging and other services, there is a reluctance to include these in the Netherlands, as this interpretation may also trigger the applicability of data retention rules. |
| Ad2 A lack of uniformity and harmonisation in an international context leads to different interpretations of definitions such as consent. Given the fact that, at a European level both NRAs and DPAs may be competent when it comes to enforcement (depending on the Member State) and there is less coordination between NRAs and DPAs than there is between just DPAs or NRAs, interpretations may vary. |
| Ad 3 In the Netherlands, ACM and Cbp are both competent in most cases. This leads to an unnecessary overlap when it comes to enforcing the rules. For instance, in the case of NPO (Dutch National Public Broadcasting Organisation on first party cookie consent), both the ACM and the Cbp issued their own findings. While there is coordination, the overlap leads to double work. The effectiveness of the rules in cross-border cases seems limited. In particular because of questions regarding the competence of supervisory authorities and limited coordination in the field |
of ePrivacy, the effectiveness of cross border enforcement is limited.

b. Merge the rules for ePrivacy and data protection, focussing on the latter. Given the fact that in most cases the data processed in the context of the ePrivacy Directive is personal data, the distinction between ePrivacy and data protection is artificial. Because (most) of the ePrivacy requirements only apply to public communications networks and communication services, there is no longer a level playing field between information society services that provide functionalities similar to communication services, but cannot be qualified as such.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

| Article 11.2 Telecommunications Act sets the general rule with regards to the confidentiality of electronic communications. The provisions state that providers of electronic communications networks and services shall take care of the protection of data and the privacy of their subscribers and users. This provision functions alongside the other obligations laid down in chapter 11 of the Telecommunications Act and the provisions regarding the confidentiality of communications in the Data Protection Act (article 13 Wbp).

| Article 11.2a of the Telecommunications Act prescribes rules with regards to the principle of confidentiality of communications and the related traffic data.

| Pursuant to 11.2a, first paragraph the provider of a public electronic communications network and the provider of a public electronic communication service are responsible for safeguarding the confidentiality the communication and the related data transferred via their services, notwithstanding the Dutch Penal Code and any other obligations under this law.

| The second paragraph ascertains that the provider of a public electronic communications network and the provider of a public electronic communications network will abstain from tapping or any other interception or checking the information via a public electronic communications network or public electronic communications service and the related data, unless and insofar:

| a. the concerned subscriber has given explicit consent for these actions;
| b. these actions are necessary to guarantee the integrity and security of services of the concerned provider;
| c. these actions are necessary for the transfer of information via networks and services of the concerned provider, or
| d. these actions are necessary to accomplish with a legal provision or legal order.

| Article 11.2a, paragraph 3 states that prior to obtaining consent as mentioned above, the provider provides the subscriber to following information:

| a. the category of data that is being tapped, intercepted or checked;
| b. the purposes of the data that is being tapped, intercepted or checked and;
| c. the duration of the tapping, intercepting and checking the data.

| The subscriber can withdraw his consent at any moment (article 11.2a Telecommunications Act)
Furthermore, a definition of ‘communications’ can be found in article 11.1, under e of the Telecommunications Act:

‘Communications: information that is transferred or shared between a finite number or parties through a public electronic communication service; this doesn’t contain the information that is transferred via a broadcasting service over an electronic communications network, except when that information can be related to the identifiable subscriber or the users that receives the information.’
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

This provision has been transposed in article 11.5(2) Telecommunications Act. It follows from this provision that a provider can process data that are necessary for invoicing, including invoices for subscribers or the person that is legally related to the provider, or for the purpose of a payment regarding granted access. Traffic data can be processed until the term of the invoice ends or if payment can be legally forced. This ‘business’ exception has a broad scope, besides covering the sending of invoices it also contains the payment of interconnection and the registration of credit by prepaid-users.

Article 11(4) states that the provider informs the subscribers or users of the categories of traffic data that is processed, as well as the duration of the processing. Furthermore, the processing of traffic data can only be exercised by those who are under the authority of the provider of the invoices.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Article 11.5 of the Telecommunications Act contains exceptions to the confidentiality of communication. Besides the aforementioned business exception (article 11.5(2)), data could be used – with permission of the user or subscriber – for market research or selling activities regarding electronic communication services. The market research and selling activities do not have to be directly related to the provider’s service, but it is required that the provider processes the data and keeps the control over the data. Furthermore, article 11.13 of the Dutch Telecommunications Act provides an exception to articles 11.5, 11.5 and 11.9(1) of the Dutch Telecommunications Act. The exception is applicable if the provider meets with one of the conditions, namely:

- National security
- Prevention, investigation and persecution of criminal offences.

Pursuant to the Dutch Code of Criminal Procedure (Wetboek van Strafvordering, or “Sv”) powers are given to the Dutch public prosecutor to request information from communications providers (Book 1, Title IVA, seventh Section of the Sv - Special Powers of Investigation), which regards, amongst others, the tapping of information (article 126m Sv), traffic data (126n Sv), personal data (126na Sv) and location data (126nb Sv).
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. Dutch legislation doesn't explicitly address “automated breaches of confidentiality without human intervention”. The legislation doesn’t distinguish between automatic and non-automated breaches. In principle such breaches of confidentiality will be considered an infringement of the confidentiality requirements set forth in the Telecommunications Act.

Moreover, such acts would very likely also be considered an infringement of data protection legislation. See for instance the Dutch Google Streetview case investigated by the DPA. The DPA laid down an order for penalty payments. According to the investigation of the DPA, Google gathered the unique MAC address of over 3,6 million wifi-routers without the knowledge of the data subjects. They gathered the addresses through the cars that are used for Google Streetview. The DPA stated that these addresses combined with a calculated location can be considered as personal data, since the data can provide information about the holder of the wifi router.

Google Streetview case by the DPA: [http://www.cbweb.nl/Pages/pb_20110419_google.aspx](http://www.cbweb.nl/Pages/pb_20110419_google.aspx) (In Dutch).

The distinction between traffic data and personal data (or content data) exists, but traffic data is mostly associated with identifiers such as IP-addresses and MAC-addresses, rendering it personal data.

b. Article 139c of the Dutch Penal Code (Wetboek van Strafrecht) prohibits the interception of (confidential) information via telecommunications and/or automated means, unless this information is broadcasted (e.g. a radio show). This covers all the above-mentioned examples.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Provisions regarding cookies and spyware are laid down in article 11.7a Telecommunications Act. Anyone who wishes to access data stored in the side/terminal equipment of users, or wishes to store information on the equipment of a user needs to: (article 11.7a (1) Telecommunications Act)

- provide the users with clear and complete information, in compliance with the Data Protection Act, with regards to the access or storage goals, and (article 11.7a (1) Telecommunications Act)

- get prior permission from the user to do so, unless the cookies are strictly necessary for the technical operation of the service, or necessary for a service specifically requested by the use. (article 11.7a (1) Telecommunications Act)

The Dutch legislator moreover has 'goldplated' the national implementation of article 5(3) by adding the following rule:

- In those cases where the cookie is able to gather information concerning different information society services (i.e. tracking cookies), the cookie is presumed to cover personal data. (article 11.7a Telecommunications Act)

This addition thus triggers the applicability of the Data Protection Act, meaning that a legitimate goal for processing the data is necessary. For marketing purposes the only possible legal ground according to the DPA is the unambiguous consent of the data subject, a more strict form of consent than the general consent in article 5(3). For analytics purposes a new legal exception is currently contemplated. Apart from the legitimate basis, cookie droppers also need to comply with all the other provisions of the DPA, for instance entering into processing agreements with parties such as Google/Doubleclick.

The burden of proof for this presumption lies with the cookie dropper.

The provisions apply to ‘anyone’, in practice this means that anyone who stores or scans data that is stored on terminal equipment has to comply with the provisions, irrespective of the country of establishment. The provision aims to protect Dutch citizens, therefore the information and consent demands apply equally to Dutch and foreign based websites that target Dutch users. This can be determined on the basis for the offered information, the possibility to deliver products in the Netherlands or that the website is offered in the Dutch language. The Dutch NRA provided guidance on this topic via http://www.consuwijzer.nl/telecom-post/internet/privacy/uitleg-cookies &
Although it is called the ‘cookie provision’, the provision also applies to other systems, including the use of Javascripts, flash cookies, HTML5-local storage and other technologies that store or scan data.

b. Yes, in general they are called functional or technical cookies and they are exempted from the provision. One speaks of such a cookie when 1. It is specifically necessary for the technical operation the service 2. When strictly necessary to deliver a by the user requested service, for example cookies that allow users to set language preferences on a website. Because these cookies are exempted from the provision, no information messages or consent-boxes are necessary. The law does apply to all forms of end-user equipment (computers, smartphones, tablets, smart-TVs etc).

6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

Article 11.7a demands that the user is informed and gives prior consent to the storage of cookies, however there is a lot of discussion on how this informed consent should be obtained. Consent is defined in article 1 of the Dutch Data Protection Act and thus matches the definition of consent in directive 95/46/EC:

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

The legislator left it to the websites to decide how they would design this informed consent provision. The same rules apply to all devices. If the cookie doesn’t fall within the scope of an exempted cookie, prior informed consent must be obtained.

Please note that due to the goldplating of article 5(3), in those cases where tracking cookies (analytics, marketing) are used, actually two consent requirements apply:

1) Prior consent for the processing of cookies

2) Unambiguous consent for the processing of personal data.

In practice, these two forms of consent can be given at the same time.

ACM and Cbp are both competent to enforce these rules. The focus of the Cbp is on the provisions in the Data Protection Act. In practice they have a strong cooperation in cases that overlap in competences.

There already have been several cases in which the Cbp has enforced the rules based on the presumption personal data is processed, namely: NPO (first party cookie consent), TPVision (cookie consent in the context of smart-tvs) and YD (cookie consent for a display advertising network). In all these cases it was held that the data controllers had not properly informed the data subject and had not obtained a valid unambiguous consent. Recently, ACM (in cooperation with Cbp) published an official report on the enforcement of the provision with regard to the website of the public broadcaster (NPO: www.npo.nl). ACM ruled that the NPO doesn’t comply with article 11.7a, because they didn’t sufficiently inform their users and don’t provide the possibility to give informed consent, which constitutes a breach of the informed consent rule. Furthermore, ACM states in their publication regarding the research that they started with the enforcement on government-related
website because of the role the government has in setting the right example. (https://www.acm.nl/nl/publicaties/publicatie/13170/Publieke-omroep-overtreedt-regels-voor-plaatsen-cookies/)

NPO case:  http://www.cbpweb.nl/Pages/pb_20140708_npo-cookies-publieke-omroep.aspx  (In Dutch)

TPVision case:  http://www.cbpweb.nl/Pages/pb_20130822-persoonsgegevens-smart-tv.aspx  (In Dutch)

YD case:  http://www.cbpweb.nl/Pages/pb_20140513_yd-cookies-privacy.aspx  (In Dutch)

In order to inform websites on the rules with regards to cookies, ACM published a FAQ on its website which can be found here: https://www.acm.nl/nl/publicaties/publicatie/12768/Veelgestelde-vragen-over-de-cookiebepaling/ (in Dutch).
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Under Dutch law, there are two exceptions to the informed consent rule (article 11.7a under 3(a+b) Telecommunications Act):

- When a cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or
- when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. (Functional or technical cookie). For example cookies that allow users to set language preferences on a website. Because these cookies are exempted from the provision, no information messages or consent-boxes are necessary. The law does apply to all end-user’s equipment.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

In practice, websites obtain (informed) consent by displaying either a 'cookie wall' that requires a specific opt-in, or by using headers/footers informing users about the use of cookies and that clicking through on the website implies their unambiguous consent.

At this moment there aren’t any official statistics on the compliance, however ACM and Cbp have started enforcement against violations of the rules. See above for relevant cases.

The Dutch Consumer Association took a survey asking consumers about their experiences with cookie notifications. Main outcomes (http://www.consumenbond.nl/test/elektronica-communicatie/veilig-online/privacy-op-internet/extra/cookiewet-heeft-weinig-opgeleverd/):

- 50% always clicks ‘OK’/’Agree’, 25% depends their choice on the type of website and only 3% never accepts cookies.
- 71% wants to stop tracking cookies
- 30% thinks that the cookie provision has improved their privacy
- 73% reads sometimes or always the information on website with regards to the types and goals of the cookies

Furthermore, the Dutch newspaper NRC Handelsblad reported on the use of tracking cookies, publishing that a third of the Dutch websites stores cookies before anyone has given informed consent (http://www.nrc.nl/nieuws/2014/03/17/nederlandse-websites-schenden-massaal-de-privacywet/?_ga=1.131854927.1359042041.1407847143).
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

| a.       | The Dutch DPA gives extensive guidance and information on its website: [http://www.cbpweb.nl/Pages/th_cookies_start.aspx](http://www.cbpweb.nl/Pages/th_cookies_start.aspx). Furthermore, ACM deals with the practical side of cookies. They also provide a lot of guidance and information aimed at both consumers and companies on their website: [https://www.acm.nl/nl/zoekresultaat/?query=cookies](https://www.acm.nl/nl/zoekresultaat/?query=cookies) and [https://www.acm.nl/nl/publicaties/zoeken-in-publicaties/?zff[]=qu%3Acokies](https://www.acm.nl/nl/publicaties/zoeken-in-publicaties/?zff[]=qu%3Acokies). |
| b.       | Not available. |
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

| a. No. I feel the rules are unnecessarily complicated, regulating the means rather than the goal, and contribute little to none to real privacy protection for citizens. In addition, due to the goldplating of article 5(3), organisations incur huge legal costs for privacy compliance which could have better been spent on improving general privacy compliance. Worse still, users are conditioned to except all cookies and routinely click away consent dialogue buttons. Not only does this not change anything for their privacy, it creates additional risks because users can give away more of their privacy based on consent. Finally, cookie consent boxes are viewed as a nuisance both by consumers and businesses. All in all the Dutch implementation and generally the changes to article 5(3) in 2009/136/EC are an utter failure from a privacy perspective. |
| b. For my personal opinion on improving the legal framework please read my article The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection. Available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418). This article, published in the journal Ethics and Information Technology, deals specifically with this issue and gives recommendations for improving the legal framework. It has been attached to this country report. Abstract: “In this article we examine the effectiveness of consent in data protection legislation. We argue that the current legal framework for consent, which has its basis in the idea of autonomous authorization, does not work in practice. In practice the legal requirements for consent lead to ‘consent desensitization’, undermining privacy protection and trust in data processing. In particular we argue that stricter legal requirements for giving and obtaining consent (explicit consent) as proposed in the European Data Protection Regulation will further weaken the effectiveness of the consent mechanism. Building on Miller & Wertheimer’s ‘Fair Transaction’ model of consent we will examine alternatives to explicit consent.” [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418). |

In practice 'implied consent' solutions whereby users signal consent by clicking through on the website seem to be most user friendly. In general, I would advice education to make users more tech-savvy and allow them to delete cookies via their browser.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The definition of traffic data can be found in article 11.1(b) of the Telecommunications Act, it is defined as: ‘data processed for the transmission of communications over an electronic communications network or for the invoicing of such communications’.</td>
</tr>
<tr>
<td>Moreover, article 11.1(c) of the Telecommunications Act defines the processing of traffic data as processing by the means of the provisions in the Data Protection Act (article 1).</td>
</tr>
<tr>
<td>The provisions concerning traffic data can be found in article 11.5 of the Telecommunications Act. The definitions are in line with the definitions in the ePrivacy directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

The legal framework regarding the process of traffic data is laid down in article 11.5 of the Telecommunications Act. According to this provision, traffic data needs to be deleted or anonymised when the data is no longer necessary for the transmission of communications. Anonymising means that the concerned data is completely and irreversible removed from any personal identification characteristics. Besides the earlier discussed invoice/business exception that can be found in article 11.5(2) Telecommunications Act, there are several other exceptions.

Following this provision, a provider can process data that is necessary for invoicing, including invoices for subscribers or the person that is legally related to the provider, or for the purpose of a payment regarding granted access. Traffic data can be processed until the term of the invoice ends or if payment can be legally forced. This ‘business’ exception has a broad scope, besides sending invoices it also contains they payment of interconnection and the registration of credit by prepaid-users.

Article 11(4) states that the provider informs the subscribers or users of the categories of traffic data that is processed, as well as the duration of the processing. Furthermore, the processing of traffic data can only be exercised by those who are under the authority of the provider of the invoices.

Article 11.5 of the Telecommunications Act contains exceptions to the confidentiality of communication. Besides the aforementioned business exception (article 11.5(2)) data could be used – with permission of the user or subscriber – for market research or selling activities regarding electronic communication services. The market research and selling activities do not have to be directly related to the provider’s service, but it is required that the provider processes the data and keeps the say over the data.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The legal framework regarding the anonymising or deletion of traffic data is laid down in article 11.5 of the Telecommunications Act. According to this provision, traffic data needs to be deleted or anonymised when the data is no longer necessary for the transmission of communications. Anonymising means that the concerned data is completely and irreversible ridded from any personal identification characteristics.</td>
</tr>
</tbody>
</table>
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

| Last year, the Dutch DPA did an investigation into the analysis of data traffic (packet inspection) on the mobile network by the mobile operators KPN, Tele2, T-Mobile and Vodafone. The Dutch DPA found that all four operators had violated the Dutch Data Protection Act and the Telecommunications Act. The companies were found to have stored data, in breach with the law, on a detailed level about visited websites and used app. According to the law, data must be deleted as soon as possible or irreversibly anonymised. The investigation showed that customers weren’t correctly or not informed about the fact that telecom operators collected this information and what they do with it. According to the DPA, this led to a lack of transparency, which is also a breach of the law. The DPA didn’t lay down measures, but will verify if the violations are ongoing and decide whether it will take enforcement measures. |
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| The provisions lead to an unlevel playing field between traditional telecommunications services and new online communications services in practice, because their scope is limited to electronic communications services and public telecommunications networks. The processing of traffic data by other information society services is only protected via the general data protection legislation. While 'communication services' could be interpreted more broadly, this may lead to unwanted consequences such as trigger data retention requirements for broader categories of data controllers. |
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
</table>

The term location data is defined in article 11.1(d) Telecommunications Act as follows: ‘data processed in a public electronic communication network or an electronic communication service that indicates the geographical position of the user’s terminal equipment of a public electronic communication service.’

This definition is in line with the definition in article 2(c) of the ePrivacy Directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Article 11.5a of the Telecommunications Act transposes the provisions of the ePrivacy Directive with regard to location data. For the greater part, the rules correspond with the rules regarding traffic data. Location data can only be processed in a non-anonymised way if that is necessary for the delivery of value added services. Furthermore, users and subscribers must have the option to restrain the process of location data in a simple and free manner.

The definition in the Telecommunications Act corresponds with the definition in the ePrivacy Directive.

The provision is also applicable to third parties which harvest the data from users’ devices: the processing of location data, not being traffic data, concerning subscribers or users of public electronic communication networks or public electronic communication services is allowed only, if:

- a. the data is anonymised, or
- b. the concerned subscriber or user has given consent to process the data for the purpose of the delivery of the value added service.

Before obtaining consent, the user or subscriber must be provided with the following information:

- a. the type of location data
- b. the goals of the processing
- c. the duration
- d. if the data will be given to third parties for the purpose of delivering a value added service.

Processing the data for the purpose of a value added service is only allowed if this is necessary for the delivery of the value added service.
<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 11.5a of the Telecommunications Act sets requirements regarding the anonymisation and deletion of location data. The processing of location data is allowed when this data is anonymised or when the concerned subscriber or user has given permission for the processing of the data.</td>
</tr>
</tbody>
</table>
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>Country</th>
<th>Details</th>
</tr>
</thead>
</table>

b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The provisions lead to an unlevel playing field between traditional telecommunications services and new online communications services in practice, because their scope is limited to electronic communications services and public telecommunications networks. The processing of location data by other information society services is only protected via the general data protection legislation. While 'communication services' could be interpreted more broadly, this may lead to unwanted consequences such as triggering data retention requirements for broader categories of data controllers. This issue has become more pressing as a result of the use of smartphones and apps that enable geolocation.</td>
</tr>
</tbody>
</table>

### E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

   a. the scope and substance of your national implementation

   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. The Dutch legislator transposed article 13 of the ePrivacy Directive into article 11.7 Telecommunications Act. The substance and scope of the provision is comparable with the provision in the ePrivacy Directive.

   b. The national provision is in line with the Directive, although the use of terminology is not exactly the same. For example: in the Directive the term ‘direct marketing’ is used, in the transposed provision the term ‘unsolicited communication for commercial, ideal of charitable goals’ is used. With the aforementioned terminology the Dutch provision seems to be somewhat more precise than the Directive.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

In the transposed provision there is an opt-in regime for unsolicited messages via electronic mail or other means. For these forms of communication the sender has to obtain consent of the targeted users. The definition of a user is not limited to natural persons, therefore legal entities also fall within the scope of the provision (b2b spam).

The B2b spam-regime applies to unsolicited marketing via electronic messages, such as e-mail and sms. Sending electronic messages does not require permission if electronic contact details are specifically used for such communication (e.g. acquisition@company.com).
<table>
<thead>
<tr>
<th>3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?</th>
</tr>
</thead>
</table>

When electronic contact details are collected in the context of a sale, the information may be used to offer similar services or products (soft opt-in). The receiver must have the possibility to easily opt-out without any costs involved.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The provisions distinguishes *automatic call systems without human intervention*, fax and electronic messaging. The definition of electronic messaging does cover e-mail, but also SMS/text messages/MMS, this is in line with the definition in the ePrivacy Directive.

However, due to the link with public communications networks and electronic communications services, Bluetooth and similar technologies probably fall outside the scope of the regulations.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b. On June 5 2014 the Administrative Court on Trade and Industry (College van Beroep voor het Bedrijfsleven/CBb) has given more clarity on the application of the opt-out regime in article 11.7 Telecommunications Act. In its judgment the CBb states that the definition of a commercial message is: messages with the goal of direct marketing, or so to say messages with a recruiting character, that aim to set up or maintain a direct relationship between provider/operator and customer (<a href="http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:CBB:2014:206">http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:CBB:2014:206</a>).</td>
<td></td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The Dutch anti-spam rules are quite effective, in large part due to effective enforcement by the ACM and the self-regulation within the sector (such as the Dutch Email Code). New types of spam such as those via IM-services or wireless technologies do raise questions, but haven’t led to big issues in practice.
COUNTRY REPORT

POLAND

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Dr. hab. Dariusz Adamski, University of Wroclaw

Date: 14 August 2014
Contents

Part 1: Management summary ............................................................................................................. 3
Part 2: Answers to the questionnaire .................................................................................................. 4
Part 1: Management summary

Management Summary for Poland

The transposition of the ePrivacy Directive into Polish law can be summarized as follows:

- Providers and networks covered by Polish provisions implementing the ePrivacy Directive are more granularly defined than what Art. 3 e-Privacy Directive provides for. The rationale for these differences is essentially to adjust the obligations to specific types of providers/networks and hence to make sure they are unambiguous. The only serious legal uncertainty in this respect is whether content (information society services) providers are covered by provisions of the Polish Telecommunications Law implementing the obligation of communications confidentiality (Art. 5 e-Privacy Directive). A positive answer to this question may be given only on the basis of the duty to interpret national law in conformity with EU law.

- Two exceptions to the obligation of confidentiality of communications provided by Polish law are seemingly broader than what is allowed by Art. 15(1) ePrivacy Directive. In practice, however, one of them (Art. 159(2)(4) TL) is interpreted in an extremely narrow manner by supervisory authorities, which – rather than rendering the exception too broad, comparing to the EU standard, in practice eliminates certain exceptions to the obligation of confidentiality of communications, even when they would otherwise be justified by national provisions implementing Art. 7 Directive 95/46. Additional qualifications required by the systemic interpretation align the other (Art. 159(4) TL) with Art. 15(1) ePrivacy Directive, even if - so far - the access to retention data by law enforcement agencies has not been defined satisfactorily by specific legal acts determining their mandate.

- Rules on cookies have been properly transposed into the Polish legal system and compliance with the consent obligation is high. It is more dubious, however, whether in practice the consent is informed. There are no statistics on compliance, nor have there been any enforcement actions or statistics on users’ approaches to the rules. The issue has not attracted attention of the public authorities nor the general public, probably because no provider has attempted to use cookies in any other way than to enhance website functionality.

- The wording of Polish provisions implementing Art. 6 ePrivacy Directive (on traffic data) does not comply with the EU standard. Only when advance interpretative tools are used may the congruity be achieved. On the other hand, Polish rules on location data follow the ePrivacy Directive very closely.

- Polish law arguably recognises only the opt-in system in respect to unsolicited direct marketing communications by a natural or legal person, even when Art. 13(2) ePrivacy Directive requires an opt-out system. What is more important in practice, Art. 13 profoundly overlaps with general data protection rules. Hence, in practice, cases involving unsolicited direct marketing communications have been decided by the Polish Data Protection Authority on the basis of general data protection rules, rather than these implementing the ePrivacy Directive. Furthermore, irrespective of such isolated instances of legal actions targeted at spammers, it is highly questionable whether it is possible to substantially reduce spamming practices through legal norms, essentially because incremental nuisance of it, felt by users, are miniscule and because the practice is largely international in its nature.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Poland:
- Provisions on unsolicited communications are implemented by the Act of 18 July 2002 on providing services by electronic means (Pol. ustawa o świadczeniu usług drogą elektroniczną, hereafter “AES”)

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed in Polish law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 2 (Definitions)</td>
<td>user: Art. 2(49) TL; traffic data: Art. 159(1)(3) TL; location data: Art. 159(1)(4) TL; communication: Art. 2(17) TL; consent: Art. 174 TL; value-added service: Art. 2(47) TL; electronic mail: Art. 2(1) AES; personal data breach: Art. 174a(2) TL</td>
<td><a href="http://en.uke.gov.pl/files/?id_plik=41">http://en.uke.gov.pl/files/?id_plik=41</a> (TL); <a href="http://www.giodo.gov.pl/data/filemanager_en/51.pdf">http://www.giodo.gov.pl/data/filemanager_en/51.pdf</a> (AES, original version, the referred provisions have not been amended)</td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
<td>Art. 1 TL and Art. 1 AES</td>
<td><a href="http://en.uke.gov.pl/files/?id_plik=41">http://en.uke.gov.pl/files/?id_plik=41</a> (TL); <a href="http://www.giodo.gov.pl/data/filemanager_en/51.pdf">http://www.giodo.gov.pl/data/filemanager_en/51.pdf</a> (AES, original version, the referred provisions have not been amended)</td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Art. 173(1)-(3) TL</td>
<td><a href="http://en.uke.gov.pl/files/?id_plik=41">http://en.uke.gov.pl/files/?id_plik=41</a></td>
</tr>
<tr>
<td>Art. 9 (Other location data)</td>
<td>Art. 166 TL</td>
<td><a href="http://en.uke.gov.pl/files/?id_plik=41">http://en.uke.gov.pl/files/?id_plik=41</a></td>
</tr>
<tr>
<td>(Unsolicited communications)</td>
<td>AES</td>
<td><a href="http://www.giodo.gov.pl/data/filemanager_en/51.pdf">http://www.giodo.gov.pl/data/filemanager_en/51.pdf</a> (AES, original version, the referred provisions have not been amended)</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
a. the full name in your national language
b. the English translation of the short name
c. the part or the provision(s) of the ePrivacy Directive it supervises
d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it is supervising</th>
<th>the URL linking to its website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generalny Inspektor Ochrony Danych Osobowych - Inspector General for Personal Data Protection (GIODO)</td>
<td>IGPDP, known more widely as GIODO.</td>
<td>All provisions having an impact on privacy or data protection (i.e. essentially the whole body of the rules implementing the ePrivacy Directive)</td>
<td><a href="http://www.giodo.gov.pl">http://www.giodo.gov.pl</a></td>
</tr>
</tbody>
</table>

Explanation:
- The Office of Electronic Communications is the NRA for the electronic communications sector in Poland and thus a default supervisory authority for the provisions transposing the ePrivacy Directive, as inserted into TL.
- The Inspector General for Personal Data Protection is a supervisory authority in respect to the provisions transposing EU directives on privacy and personal data protection. As the provisions covered by this report generally fall in this category, GIODO may be considered as a supervisory authority in respect to all of them (least clearly in respect to unsolicited communications).
- The provisions with regard to unsolicited communications may also be supervised by the Office of Competition and Consumer Protection, as long as they infringe on collective interests of consumers (local consumer protection authorities are in charge when the interests infringed are individual, not collective).
The implementing legislation defines the networks, services and providers which fall within its scope. Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Specific provisions of the TL define the providers covered by privacy related obligations in various manners. While the broadest obligation of confidentiality refers to any entity participating in the performance of telecommunications activities within public networks and entities cooperating with it (Art. 160(1) TL), the majority of specific e-privacy provisions impose obligations on providers of publicly available telecommunications services. Telecommunications activities are defined as “provision of telecommunications services, the provision of telecommunications networks or associated facilities” (the latter is explicitly associated with broadcasting aspects of electronic communications, as dealt with by the EU legislative package on electronic communications) (Art. 1(1)(1) TL), while a publicly available telecommunications service is a “service consisting mainly of the transmission of signals via a telecommunications network (i.e. a transmission system and switching or routing equipment as well as other resources, including non-active network elements, which enable the emission, reception or transmission of signals by wire, radio, optical or other electromagnetic means, irrespective of their type), available to the general public” (Art. 2(31), (35) and (48)).

To sum it up: the scope of the providers and networks covered is more granularly defined in the Polish legal system than is the case of Art. 3 e-Privacy Directive. The differences, however, are essentially introduced to improve the accuracy of the relevant obligations, by referring them to specific types of providers/networks and types of services in respect to which individual obligations are most pertinent. In other words, while the Polish legislation is more nuanced, it does not depart from the scope of the e-Privacy Directive.

The only quandary this leads to regards content providers. This category is tantamount to providers of services provided by electronic means in the Polish legislation, and hence are covered by AES. (Services by electronic means are defined (Art. 2(4) AES) as provided without a simultaneous presence of both parties (remotely), via a transfer of data upon an individual request of a service recipient, transferred and received by electronic means, including electronic compression and data storage, which is in entirety relayed, received or transmitted by a telecommunications network as defined in TL).

It is problematic whether such content providers “participate in the performance of telecommunications activities” (as they participate in the provision of content services, for which telecommunications services are only instrumental and ancillary). By the same token it is not obvious that they are covered by the abovementioned obligation of confidentiality, established in TL and implementing Art. 5 ePrivacy Directive. One argument supporting the thesis that they do (i.e. that these providers are covered by the obligation of confidentiality established by TL) might be based on the duty to interpret national law in conformity with EU law. As Art. 3 ePrivacy Directive refers to a broad category of providers (processing personal data “in connection” with the provision of publically available electronic communications services), arguably the term “participation in the
performance of telecommunications activities” should be interpreted accordingly. Under such an interpretation the scopes of the EU instrument and the Polish implementation is aligned.

Whether content providers are covered by the national implementation of Art. 3 ePrivacy Directive is of less practical significance than it may seem at first glance, though. First, violations of confidentiality of private communications are subject to Penal Code sanctions regardless of special provisions of TL (see Section B.4.b). Second, one should also keep in mind that the data or activities addressed by the ePrivacy Directive involve processing of personal data governed by general data protection law (Act of August 29, 1997 on the Protection of Personal Data). The latter also protects confidentiality of communication even if TL does not govern the issue (e.g. if it is accepted that processing of personal data by content providers is not covered by the confidentiality obligation established by TL).
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

VoIP and location-based services should be qualified as telecommunications services as far as they comprise services consisting mainly in the transmission of signals via a transmission system and switching or routing equipment. Only the providers actually carrying out the transmission are therefore considered as providers of telecommunications services, thus fully falling within the scope of the implementing legislation. Application providers are excluded as long as they are not involved in actually transmitting signals. The only obligation potentially covering them (even if this is not entirely obvious) is the obligation of telecommunications confidentiality, discussed further in Section B.

Privacy related obligations of content providers, e.g. webmail providers, are essentially defined by AES (and therefore this report does not address them). Extending the confidentiality obligation implemented by TL so that it covers this category as well may only be achieved by the interpretation invoking the duty to interpret national law in conformity with EU law (see Section A.3).
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

In principle, telecommunications activities in Poland are regulated and should be undertaken only by entities signed up to the register of telecommunications undertakings. Also telecommunications activities conducted by a telecommunications undertaking from another EU or EEA member state providing services in Poland temporarily should be subject to the entry (Art. 10 TL). In practice, however, certain providers of communications services (e.g. VoiP) do not apply for registration. In theory a failure to sign up to the register may trigger an administrative financial sanction (Art. 209 TL), imposed both on the entity providing services and its management. Enforcement obstacles in respect to entities from other countries are insurmountable in practice, however, when the provider is not physically present in Poland. Nor does the matter attract attention of enforcing authorities, as long, at least, as the provision of services is not fraudulent.

In respect to providers of unsolicited communications, AES makes an exception to the general rule that the law of the country of origin of service providers established in the EEA should apply (Art. 3a AES). In other words, those providers should be covered by prohibitions on unsolicited communications established by the Polish legislation (see Section E), of course as long as they target recipients on the territory of Poland. This rule, though, does not deal with providers from third countries, in respect to which not only jurisdictional issues are hardly possible to disentangle, but – more fundamentally – enforcement faces practically insurmountable obstacles.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. There are no guidance documents on the interpretation and/or application on the definitions mentioned in this section, issued by national enforcement authorities.

b. One court decision worth noting here was handed down by the Appellate Court in Warsaw (of 13 December 2012, Case No. VI ACa 1215/11, available at http://orzeczenia.waw.sa.gov.pl/content/$N/1545000000003003_VI_ACa_001215_2011_Uz_2012-12-13_001). The Court ruled that the status of a telecommunications undertaking does not depend on actual pursuance of the activities defined in Art. 2(27) TL (business activities consisting in the provision of telecommunications networks, associated facilities or in the provision of telecommunications services), but on signing up to the register of telecommunications undertakings held by the national NRA. In other words, unregistered undertakings providing telecommunications services are not covered by the obligations established by TL, except for those – like the obligation to safeguard the confidentiality of communications – that may be addressed to a category broader than only providers of telecommunications networks and/or services.
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>In strictly formal terms, the distinction between publicly available telecommunications services and content providers is problematic, particularly in the context of how Art. 5 ePrivacy Directive has been implemented in Poland. As mentioned earlier, however (see Section A.3) this formal incongruence does not have particularly important practical consequences. Other definitional rules may raise issues only in relation to specific obligations, discussed further in this report. They do not ensue any self-standing problems in respect to their effectiveness.</td>
</tr>
<tr>
<td>b.</td>
<td>It is highly problematic if any improvements of enforcement in respect to third country service providers are practically feasible (because enforcing powers of Polish authorities are limited to the territory of this country), while this is precisely the main shortcoming of the current provisions on the scope of relevant legislation, Art. 3 e-Privacy Directive in particular.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

According to the obligation of confidentiality of communications in telecommunications (hereinafter also referred to as confidentiality of communications or telecommunications confidentiality), established in TL (its Art. 159):

“1. The communications confidentiality within telecommunications networks, hereinafter called the “telecommunications confidentiality”, shall encompass:
   1) data concerning the user;
   2) content of individual communications;
   3) transmission data understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or within the framework of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services;
   4) location data, understood as location data beyond the data necessary for message transmission or billing;
   5) data relating to call attempts between specific telecommunications networks termination points, including data relating to unsuccessful call attempts meaning calls between telecommunications terminal equipment or network termination points which have been set up and not answered by an end user or aborted.”

Furthermore:

“3. With the exception of cases specified in the Act, the disclosure or processing of content or data subject to telecommunications confidentiality shall violate the obligation to keep the telecommunications confidentiality.
4. The provisions of paragraphs 2 and 3 shall not apply to messages and data public by their nature, data for a public purpose or disclosed by a ruling of a court in criminal procedure, a prosecutor’s ruling or under separate regulations.”

In addition, according to Art. 160 TL:

“1. An entity participating in the performance of telecommunications activities within public networks and entities cooperating with it shall keep the telecommunications confidentiality.
2. Entities referred to in paragraph 1 shall maintain due diligence, within the scope justified by technical or economic reasons, while securing telecommunications equipment, telecommunications networks and data collections from disclosing the telecommunications confidentiality.
3. A person coming into possession of a message not meant to be read by him/her when using radio or terminal equipment shall keep the telecommunications confidentiality. (...)
4. The recording of a message acquired in a manner described in paragraph 3 by a body executing control of telecommunications activities in order to document a violation of a provision of the Act, shall not be a violation of the telecommunications confidentiality.”

It may be argued that content providers, while they do not perform telecommunications activities within public networks themselves, in fact participate (passively) in such a performance, which
arguably should extend the abovementioned obligation to content providers (see Section A.3). This interpretation, however, has not been confirmed by an authoritative source, e.g. a court.

Violations of confidentiality of private communications are also subject to Penal Code sanctions (see Section B.4).

The term “communications”, to which Art. 159(1)(2) refers, is defined as “any information exchanged or transmitted between specific users by means of publicly available telecommunications services; this does not include information transmitted as part of radio or television transmissions broadcast by a telecommunications network, excluding information related to an identifiable subscriber or to the user receiving the information” (Art. 2(17) TL).
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

Art. 159(2) (3) TL provides that: “Knowledge, record, storage, transfer or another use of contents or data subject to telecommunications confidentiality by individuals other than the message sender and receiver shall be forbidden, unless performing this action is essential to record messages and associated transmission data applied within legal business practice for the purpose of ensuring evidence for commercial transactions or for the purpose of communications in commercial activities”.

This provision closely follows the exception established in Art. 5(2) ePrivacy Directive (while the last part of Art. 159(2) (3) TL – reading “or for the purpose of communications in commercial activities” - implements Art. 5(3) ePrivacy Directive).
### 3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The Polish law defines exceptions to the confidentiality principle differently than Art. 15(1) ePrivacy Directive. On the one hand it provides for an obvious exception necessary for the national NRA to fulfil its mandate properly. Namely, according to Art. 160(4) TL: “The recording of a message acquired (...) by a body executing control of telecommunications activities in order to document a violation of a provision of the Act, shall not be a violation of the telecommunications confidentiality”.

On the other hand, it contains a broad exception (Art. 159(2)(4) TL), according to which: “Knowledge, record, storage, transfer or another use of contents or data subject to telecommunications confidentiality by individuals other than the message sender and receiver shall be forbidden, unless this is necessary for other reasons provided for in the Act or separate regulations.” The obligation of the confidentiality of communication is lifted also in respect to “data for a public purpose or disclosed by a ruling of a court in criminal procedure, a prosecutor’s ruling or under separate regulations” (Art. 159(4) TL).

Both Art. 159(2)(4) TL and Art. 159(4) TL are clearly more general than Art. 15(1) ePrivacy Directive, and hence arguably broader. In practice, however, the first of them has been interpreted as of hardly any legal significance (see Section B.9), while additional qualifications of the second — aligning it with Art. 15(1) ePrivacy Directive — are required by systemic interpretation. More specifically, every statutory exception “under separate regulations” would violate Art. 8 ECHR (European Convention of Human Rights), as well as provisions of the Polish constitution defining the right to privacy (Art. 47 Polish Constitution) as a constitutionally protected individual right, unless it complies with the qualifications established in Art. 15(1) ePrivacy Directive.

All in all, therefore, any specific national statutory provision establishing an exception to the confidentiality principle to protect national, public security or crime detection and investigation (the latter understood broadly, as covering also various aspects of crime detection and investigation) would be unconstitutional and would violate the right to privacy as protected by the European Convention, unless it complies with Art. 15(1) ePrivacy Directive (which also indicates that — legally speaking — the latter may be considered as a redundant norm, otherwise flowing from the right to privacy as part of the ECHR and thus from general principles of EU law). Nonetheless, so far the access to retention data by law enforcement agencies has not been defined satisfactory from this perspective by specific legal acts determining their mandate.

Also problematically, the extremely narrow interpretation of Art. 159(2)(4) TL eliminates certain exceptions to the obligation of confidentiality of communications, even when such an exception would otherwise be justified by national provisions implementing Art. 7 Directive 95/46 (see also Section B.9).
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Polish legislation does not explicitly address “automated breaches of confidentiality without human involvement”. As mentioned earlier, Art. 160(1) TL imposes the obligation of confidentiality of communications on any entity participating in the performance of telecommunications activities within public networks and on entities cooperating with it. By the same token, those entities are obliged to prevent any breaches of confidentiality (including the automated ones). Their failure to do so is tantamount to a violation of this obligation, if preventing such a breach may be expected on the basis of “due diligence, within the scope justified by technical or economic reasons”, as required by Art. 160(2) TL.

b. The Polish Constitution enshrines the right to the confidentiality of communication (Art. 49). This right is primarily protected by provisions of the Criminal Code incriminating interception of the content of private communications and telecommunications (among other offenses against the protection of information: Chapter XXXIII of the Polish Penal Code of 1997, Arts. 265-277). The most pertinent to the privacy of electronic communications is Art. 267 Penal Code:

   “§ 1. Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a telecommunications network, or by breaching or avoiding electronic, magnetic, IT or other special protection thereof shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.
   § 2. The same punishment shall be imposed on anyone, who acquires, without an authorisation, an access to the whole IT system or a part thereof.
   § 3. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other special equipment or software.
   § 4. The same punishment shall be imposed on anyone, who discloses to another person the information obtained in the manner specified in § 1 - 3.
   § 5. The prosecution of the offence specified in § 1 – 4 shall occur on a motion of the injured person.”
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. There are two sets of rules of TL relevant in this context, both stemming from Art. 173. The first is a general one. It concerns storing or accessing (by any party) any information (e.g. cookies) in the telecommunications terminal equipment of a subscriber or a user. The second is a lex specialis dealing only with software (e.g. spyware) installed on a subscriber’s or an end user’s terminal equipment by entities providing telecommunications services or services by electronic means, as long as the software is intended for using these services or this software.

The first situation is governed by Art 173 (1 - 3) TL. Accordingly:

“1. The storing of information or the gaining of access to information already stored in the telecommunications terminal equipment of a subscriber or a user is only allowed on the condition that:
   1) the subscriber or the end user is directly informed in advance in an unambiguous, easy and understandable manner with regard to:
      a) the purpose of storing and the manner of gaining access to this information,
      b) the possibility to define the conditions of the storing or the gaining of access to this information by using settings of the software installed on its telecommunications terminal equipment or service configuration;
   2) the subscriber or end user, having obtained information referred to in point 1), gives its consent;
   3) the stored information or the gaining of access to this information do not cause changes in the configuration of the subscriber’s or end user’s telecommunications terminal equipment and in the software installed on this equipment.

2. The subscriber or end user may give its consent referred to in paragraph 1 (2) using settings of the software installed on its telecommunications terminal equipment or service configuration.
3. The conditions referred to in paragraph 1 shall not apply, if the storing of or the gaining of access to information referred to in paragraph 1 is necessary to:
   1) transmit communication over a public telecommunications network;
   2) provide a telecommunications service or services by electronic means, requested by the subscriber or an end user.”

The second situation is legitimate, pursuant to Art. 173 (4) TL, when a subscriber or an end user:

“1) is directly informed, before the installation of the software, in an unambiguous, easy and understandable manner, about the purpose of installing this software, and about the manner in which the service provider uses this software;
2) is directly informed, in an unambiguous, easy and understandable manner, about the manner in which the software may be removed from the end-user’s or subscriber’s terminal equipment;
3) gives its consent for the installation and use of the software prior to its installation.”

b. The provisions quoted above do not distinguish between types of cookies or between categories of end equipment.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

As a general principle, where provisions of TL require a consent of a subscriber or an end user, this consent, according to Art. 174:

1) may not be presumed or implied by a declaration of will of a different content;
2) may be expressed by electronic means provided that it is recorded and confirmed by the user;
3) may be withdrawn at any time, in a simple manner and free of charge.“

As an exception to this general rule, for the first of the two situations mentioned in Section B.5 (storing or accessing - by any party - any information - i.e. cookies, but not spyware - stored in the telecommunications terminal equipment of a subscriber or a user) Art. 173(2) TL provides that: “The subscriber or end user may give its consent (...) using settings of the software installed on its telecommunications terminal equipment or service configuration”.

Consent bars suffice as a method of obtaining consent pursuant to Art. 173(2) TL (cookies). The scope of information to be provided to the user in this situation is determined by Art. 173(1)(1) TL. Thus the information should be given in advance (before the consent is expressed) “in an unambiguous, easy and understandable manner with regard to:
a) the purpose of storing and the manner of gaining access to this information,
b) the possibility to define the conditions of the storing or the gaining of access to this information by using settings of the software installed on its telecommunications terminal equipment or service configuration.”

The rules on consent and information to be provided do not distinguish between various types of equipment, hence they apply to mobile devices and fixed devices alike.
No cookie types have been distinguished as subject to different rules.
The law does not allow to set up cookies before individuals have provided consent (as the consent may not be implied).
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

i) Art. 159(2) (3) in fine TL provides that: “Knowledge, record, storage, transfer or another use of contents or data subject to telecommunications confidentiality by individuals other than the message sender and receiver shall be forbidden, unless performing this action is essential to record messages and associated transmission data applied within legal business practice for the purpose of communications in commercial activities”.

This rule may be considered as broader than the exception “for the sole purpose of carrying out the transmission of a communication over an electronic communications network”, for it speaks of – more broadly – commercial activities, rather than, more strictly, only transmission of a communication. But the words “within legal business practice” indicate that other data protection rules define the scope of the commercial activities for the purposes of which the exception may apply. On the one hand this indicates that the provision may not be considered as an exception to e.g. the prohibitions to process personal data as established by the Act of August 29, 1997 on the Protection of Personal Data (which transposes Directive 95/46/EC). On the other, it suggests that exceptions to the confidentiality rule must stem from another legal provision to be applicable. Thus the significance of Art. 159(2) (3) in fine TL is uncertain, for it does not seem to constitute a self-standing exception.

ii) According to Art. 159(2) (1-2) TL: “Knowledge, record, storage, transfer or another use of contents or data subject to telecommunications confidentiality by individuals other than the message sender and receiver shall be forbidden, unless:
1) this constitutes the subject of a service or is required to perform it;
2) this is agreed by a sender or a receiver whom such data concerns”

This provision implements the exception “when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

While rules established in Art. 159(2) (1-2) do not use the phrase “strictly necessary”, this may be inferred from the very fact that the provision constitutes an exception to a general rule, to be interpreted restrictively according to general principles of legal interpretation.

In the application of the exceptions, no distinction is made between different types of cookies. The author does not believe that any of the categories mentioned under this question could cause any classification problems from this perspective.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

According to anecdotal evidence, compliance with the basic rule on cookies requiring a user’s consent to apply them is high in Poland. Providers universally use consent bars to obtain users’ consents. The wording of the consent requests differs from one website to another, from more developed ones, e.g.: “To provide you the highest level of services, our website uses cookie files. If you continue using the website, you agree for cookies to perform their function. To learn more about cookie files and to change their settings, please click “more information”” (http://www.volvocars.com) to the generic “this website uses cookies. Click OK. More information here” (http://www.malacukierenka.pl/jablka-pod-kruszona.html).

An issue more problematic in practice is the effectiveness of Art. 5(3) ePrivacy Directive, which requires that the user be “provided with clear and comprehensive information”. This obligation is developed in Poland by the requirement to give a user “the possibility to define the conditions of the storing or the gaining of access to this information by using settings of the software installed on its telecommunications terminal equipment or service configuration” according to Polish law (Art. 173(1)(1)(b) TL). Its implementation varies heavily, however, and the NRA primarily in charge (UKE) has not been particularly active in the field of guidance/supervision as to what the legal requirements mean in practice (the same has been the case of the rules on spyware).

There are no statistics on compliance with the rules on cookies, yet – as abovementioned – it is undoubtedly high in respect to the consent obligation. There have been no enforcement actions, either, or statistics on users’ approaches to the rules. The issue has not attracted attention either of public authorities or the general public, probably because no significant provider has attempted to use cookies in any other way than to enhance website functionalities.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

a. GIODO has dealt with the obligation of telecommunications confidentiality (Art. 159 TL and Art. 161 TL in particular) quite extensively, by consistently interpreting possible exceptions to it in a very narrow manner (e.g. decision DOLiS/DEC-1061/11, DOLiS/DEC-82.12, DOLiS/DEC-82.12, DOLiS/DEC-200/12, DOLiS/DEC-837/11, DOLiS/DEC-180/13/10093, 10096, 10100). More specifically, it has found that the national provision implementing Art. 7(f) Directive 95/46 does not qualify as a legal basis justifying an exception to the obligation of confidentiality, as the obligation, first, provides for more far-reaching protection of privacy and thus should be applicable according to the wording of Art. 5 of the Polish Act on the Protection of Personal Data (“Should the provisions of any separate laws on the processing of data provide for more effective protection of the data than the provisions hereof, the provisions of those laws shall apply”) and, second, is lex specialis comparing to the national provision implementing Art. 7(f) Directive 95/46.

In June 2014 UKE published its position on the interpretation of the obligation of telecommunications confidentiality (and, in particular, exceptions thereto), available at [http://www.uke.gov.pl/files/?id_plik=16700](http://www.uke.gov.pl/files/?id_plik=16700) (please copy paste the link to open it). The Authority was induced to do so by interventions of telecommunications operators uncertain whether they may disclose personal data of their clients pursuant to requests by civil courts and debt collectors to disclose the data on the basis of certain general civil procedure provisions. The question therefore dealt with the scope of Art. 159(2)(4) TL (quoted in Section B.3). UKE essentially took a very similar stance to the abovementioned position of GIODO, in functional terms aligning the meaning of Art. 159(2)(4) TL with this of Art. 159(4) TL (the latter essentially implements Art. 15(1) ePrivacy Directive – see also Section B.3). In other words, it considered that the obligation of confidentiality may not be overcome by a general disclosure obligation provided by the Code of Civil Procedure.

b. Not available.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<table>
<thead>
<tr>
<th>a.</th>
<th>There are two main points to make here, one on the implementation of Art. 5 in conj. with Art. 15(1) ePrivacy Directive and the other on Art. 13 ePrivacy Directive.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>First, while the wording of the provisions dealing with the obligation of telecommunications confidentiality is not entirely compliant with Art. 5 and Art. 15(1) ePrivacy Directive, it may be aligned with them on the basis of the systemic interpretation. Because, however, Art. 5 and Art. 15(1) ePrivacy Directive are more restrictive in the prohibition of processing personal data than is Art. 7 Directive 95/46 (Art. 15(1) refers to Art. 13(1) Directive 95/46, which provides only for a facultative legislative authorisation, rather than to the unequivocal Art. 7 Directive 95/46), the telecommunications confidentiality may exclude the application of certain fundamental provisions, e.g. Art. 7(f) Directive 95/46 (authorising processing of personal data when it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject). This may in practice – and GIODO decisions confirm this interpretation - lead to the situation when a person defamed online may find it impossible to obtain personal data (IP address) of the infringer, because the latter is subject to the confidentiality of communications. The point is all the more important considering that at least once a court (decision of the Regional Administrative Court of 17 June 2013, Case No. II SA/Wa 152/13 - available at <a href="http://orzeczenia.nsa.gov.pl/doc/15F2E1971D">http://orzeczenia.nsa.gov.pl/doc/15F2E1971D</a> - appeal pending) has decided that content providers are obliged to disclose IP addresses of their clients for the purposes of suing for defamation, but it did so without addressing the obligation of telecommunications confidentiality, as the latter was not raised in this particular case.</td>
</tr>
<tr>
<td></td>
<td>Second, the requirement to obtain separate consent to use cookies may be congruent with the general principle that a data subject’s consent may not be inferred from her non-conclusive actions (e.g. entering a website that uses cookies). On the other hand, though, as long as cookies are used merely to improve the functionality of a website, the requirement of separate consent to use them is of very limited practical value. It is because users entering a website may legitimately expect that it be as functional as possible (for which cookies are almost indispensable), while the consent to be given on this occasion never covers any more problematic uses – e.g. disclosing the history of entries to a third party. This may – at least partly – explain why UKE has not been particularly active in the field of enforcing the rules on cookies.</td>
</tr>
<tr>
<td></td>
<td>b. It may be recommended to consider a closer alignment of Art. 15(1) ePrivacy Directive with the grounds for legitimate processing of personal data on other grounds than a data subject’s consent (Art. 7 Directive 95/46), so that the latter is more properly envisaged in the scope of the former and thus is not deprived of its <em>effet utile</em>.</td>
</tr>
</tbody>
</table>
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic data – or transmission data, as it is termed in the Polish law – is “data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data (…)” (Art. 159(1)(3) TL). The definition follows closely the one established by ePrivacy Directive, by referring to a conveyance of a communication and to billing purposes.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Legal requirements for processing traffic data are established in Art. 165 (2-5) TL, which states that: “2. The processing of transmission data necessary for charging subscriber fees and interoperator settlements shall be permissible:

1) having informed a subscriber or an end user on the type of transmission data that is to be processed by a provider of publicly available telecommunications services, and on the period of this processing;

2) only until the end of the period referred to in Article 164 (note of the author of this report: i.e. during the period within which an agreement remains in force, and after its termination during the period of vindication of claims or the performance of other tasks provided for in the Act or separate regulations).

3. A provider of publicly available telecommunications services shall inform a subscriber or an end user with regard to the type of transmission data which is to be processed, as well as with regard to the period of this processing for the purpose of marketing telecommunications services or providing value added services.

4. A provider of publicly available telecommunications services may process the transmission data referred to in paragraph 3 within the scope and period necessary for marketing telecommunications services or providing value added services.

5. Entities acting on behalf of public telecommunications network operators and providers of publicly available telecommunications services dealing with charging, traffic management in telecommunications networks, customer care, financial abuse detection systems, telecommunications services marketing or the provision of value added services, shall be entitled to process the transmission data under paragraphs 2-4. These entities may process transmission data only where this is necessary for the performance of the aforementioned activities.”

Furthermore, according to Art. 163 TL “A provider of publicly available telecommunications services shall inform a subscriber with whom an agreement for the provision of telecommunications services is concluded, as well as the remaining end users, of the scope and purpose of processing transmission data and other data concerning the subscriber or end users, as well as of the possibility of influencing the scope of this processing”.

The wording of these provisions does not include certain aspects emphasised in Art. 6 ePrivacy Directive. Firstly, it does not require that the consent for processing of personal data for marketing purposes or to provide value added services be expressed a priori, as required by Art. 6(3) ePrivacy Directive, or be revocable at any time. Secondly, it does not require that in such a situation a subscriber/user should be informed about the types of traffic data to be processed and about the duration of such processing before the consent is given, contrary to Art. 6(4) ePrivacy Directive. Thirdly, Art. 165 TL does not transpose 6(1) ePrivacy Directive. Fourthly, Art. 165 TL does not transpose Art. 6(6) ePrivacy Directive.

In principle, however, each of the lacking provisions may be inferred from other norms of TL (for the third aspect see next Section). First, the additional requirements as to the moment and revocability of consent stem from Art. 174 (TL), as discussed in Section B.6 (the consent may not be implied, is revocable at any moment). Second, Art. 165(3) TL requires that the subscriber/user be informed about the types of data that will be processed. This implies that the act of informing the user must take place before the actual processing starts. Third, as Art. 6(6) ePrivacy Directive is a
specific manifestation of Art. 5(2) ePrivacy Directive (the two deal with the same situation from two opposite perspectives: while the former concerns “the possibility for competent bodies to be informed of traffic data”, the latter deals with “the purpose of providing evidence of a commercial transaction”; the latter makes no practical sense unless the former is its integral part), the provision implementing the latter (see Section B.2) may be considered as consuming the former.

The only aspect problematic in this context is that – as it is discussed in Section D – provisions of the ePrivacy Directive on location data have not been transposed with similar loopholes. Hence it may be argued a contrario that the legislator intended to exclude the words missing in the text of TL if a twin ePrivacy provision on location data has been transposed in entirety.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

A service provider will violate Art. 165 TL and its more general rules on the confidentiality of communications (which, as mentioned in Section B.1, cover traffic data as well) and even Penal Code provisions on the violation on requirements of professional confidentiality, if it processes personal data beyond time limits established in this provision. In other words, even without an explicit legal requirement to anonymise or delete the data, one of the two must happen in consequence of an expiry of the time period for legitimate processing of personal data. This interpretation implies that a compliance with Art. 6(1) ePrivacy Directive is an inevitable corollary of complying with the remainder thereof (time limits of processing). It also leaves it up to the data controller to choose the method of complying with the requirement to end the processing of personal data.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

As in other countries, the scope of legitimate restrictions to the protection of telecommunications confidentiality in respect to traffic data for law enforcement purposes (broadly speaking data retention issues) has raised serious legal problems which has led to a Constitutional Court decision. But this question refers to the implementation of the Data Retention Directive first and foremost, not the ePrivacy Directive. Hence it remains outside the scope of this report.
### 5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

All the rules on traffic data provided by Art. 6 ePrivacy Directive confirm and clarify general data protection requirements established by Directive 95/46. The latter makes it clear that processing is legitimate if it is necessary for the performance of a contract to which the data subject is a party (which is the case in respect to traffic data processed by electronic communications providers) and that processing in case no other legitimising factor applies (e.g. added value services, marketing purposes) requires a separate data subject’s consent. It also determines rules on the concept of consent and related informational requirements. Finally, it allows for processing of personal data without the data subject’s consent when it is necessary for the purposes of legitimate interests pursued by the controller (the situation of a dispute settlement) and defines legal consequences of involving a third party (processor) in the process on behalf of the controller.

The fact that the rules are congruent with the general data protection system, and that they are intuitively obvious, improves their effectiveness and allows for interpreting them in a consistent manner, even if it also leaves a certain impression of legal redundancy involved. By the same token the fact that law enforcement authorities are not covered by Directive 95/46 hits back on the effectiveness of the rules established by ePrivacy Directive in respect to processing of traffic data.
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The term “location data” is defined in Art. 159(1)(3) TL as “any data processed in a telecommunications network or within the framework of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services”. It is congruent with the definition provided by Art. 2(c) ePrivacy Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Pursuant to Art. 166 TL:

“1. In order to use location data, a provider of publicly available telecommunications services shall:
1) obtain the consent of a subscriber or an end user to process location data concerning this subscriber or end user, which may be withdrawn for a specific period or in relation to a specific call, subject to Article 174, or
2) perform the anonymisation of these data.
2. A provider of publicly available telecommunications services shall inform a subscriber or an end user, prior to receiving its consent, with regard to the type of location data which is to be processed, with regard to the purpose and time of its processing, and whether these data are to be passed on to another entity in order to provide a value added service.
3. The following entities shall be entitled to process the data referred to in paragraph 1:
1) those authorised by a public telecommunications network operator;
2) those authorised by a provider of publicly available telecommunications services;
3) those providing a value added service.
4. Location data may be processed only where this is necessary to provide value added services.”

The quoted provisions are entirely compliant with the requirements set by Art. 9 ePrivacy Directive.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

| Polish law provides for no specific legal requirements concerning anonymisation. |
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. There has been no such guidance on the interpretation and/or application of location data rules by national enforcement authorities in Poland.
   b. I am not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.). In cases when employees’ location data have been used by an employer - the legality of which was subsequently questioned by the employee before GIODO (cases DOLiS/DEC-180/13 and DOLiS/DEC-847.13) – the latter has based its decisions on the general data protection rules only. This result was inevitable, however, because Art. 9 ePrivacy Directive concerns the relationship between a service provider and a user, not between an employer and an employee.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

Specific provisions of the ePrivacy Directive on location data essentially confirm what could otherwise be inferred from national provisions implementing Directive 95/46. In this sense they may be deemed redundant. On the other hand, Art. 9 ePrivacy Directive may be considered as a useful clarification of how the general rules should more specifically apply to processing of location data by providers of electronic communications services.

The aspect most important from the practical perspective is the use of location data by law enforcement agencies in Poland. This aspect, which remains outside the scope of this report, is still far from being settled satisfactorily in Poland.
**E. Unsolicited commercial communications**

<table>
<thead>
<tr>
<th>1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. the scope and substance of your national implementation</td>
</tr>
<tr>
<td>b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.</td>
</tr>
</tbody>
</table>

a. Art. 13 ePrivacy Directive was implemented in the Polish legal system by means of Art. 172 TL and Art. 9-10, 24-25 AES.

Art. 172 TL provides:

1. The use of automated calling systems for direct marketing shall be forbidden, unless a subscriber or an end user has given prior consent to do so.
2. The provision of paragraph 1 shall be without prejudice to the bans and limitations concerning the transfer of unsolicited commercial information resulting from separate acts.”

According to Art. 9 AES:

1. Commercial information shall be clearly separated and marked in a manner not raising doubts that it is the commercial information.
2. Commercial information comprises:
   1) description of an entity on order of which the information is disseminated, and its electronic addresses,
   2) clear description of promoting activities, in particular discounts, free benefits in currency or in kind and other benefits related to promoted goods, service or image, and also unequivocal specification of conditions necessary for obtaining such benefits if they are a component that offer,
   3) any other information, which may influence determination of a range of liability of the parties, in particular warnings and reservations.
3. The provisions of paragraph 1 and paragraph 2 are without prejudice to the provisions of the following acts:
   1) of 16 April 1993 on Fighting Unfair Competition (...)
   and
   2) of 19 November 2009 on Gambling (...).”

Pursuant to Art. 10 AES:

1. Sending unsolicited commercial information addressed to a specified natural person by electronic communications means, in particular electronic mail, is prohibited.
2. Commercial information shall be considered solicited if the recipient has expressed his/her consent to receive such information, in particular he/she has made available for the purpose of such receipt an electronic address that identifies him/her.
3. The activity, referred herein to paragraph 1, shall be regarded as unfair competition practice within the meaning of provisions of the Act referred to in art. 9, paragraph 3, point 1.”

Art. 24 AES states:

“1. The one, who transmits by electronic communications means unsolicited commercial information, shall be liable to fine.
2. Prosecution of the offence mentioned in paragraph 1 is proceeded on the request of the harmed party."

And Art. 25 AES determines that:
“Judgement on deeds referred to in art. 23 and 24 shall be proceeded in accordance with the provisions applicable to prosecution of offences.”

Finally, according to Art. 209(1)(25) TL whoever does not comply with the obligation to obtain a consent of a user or subscriber may be subject to a financial administrative fine imposed by the NRA. Pursuant to Art. 209(2) a fine may be imposed also on members of its management board.

b. In certain aspects the Polish implementation differs from Art. 13 ePrivacy Directive. First, national provisions do not explicitly preclude unsolicited communications by fax machines. Second, the general Act on the Protection of Personal Data provides that a data controller may process personal data for direct marketing of it’s own services or products without separate consent of the data subject, because processing of personal data in such a situation is necessary for the purposes of the legitimate interests pursued by the controller (Art. 23(4)(1) Act of 29 August 1997 on the protection of personal data). This right, however, should arguably be disabled – both in respect to automated calling systems and unsolicited e-mails – by Art. 172 TL and Art. 10(1-2) AES, respectively, which are lex specialis in comparison to the more general Act on the protection of personal data. In other words, also for marketing of own products or services of the data controller a separate consent to receive the information seems necessary. In consequence, while Art. 13(2) ePrivacy Directive establishes a compulsory opt-out system for direct marketing of own products, in Poland the opt-in system ought to govern this situation. Such a conclusion is further corroborated by the wording of Art. 161(3) TL, according to which “a provider of publicly available telecommunications services may, with the consent of a user who is a natural person, process other data from this user in relation to the provided service, in particular a bank account number or a payment card number, as well as an electronic mail address and contact telephone numbers”. This provision does not make any exceptions in relation to marketing of own products or services by providers of telecommunications services, so it is hard to conceive how a different rule could apply to other suppliers for marketing of their own products/services.

It should be added in this context, however, that so far cases involving unsolicited communications have been decided by GIODO on the basis of general data protection rules only (see Section E.5) and hence a potential conflict between Art. 23(4)(1) Act of 29 August 1997 on the protection of personal data and the abovementioned provisions of TL and AES has not surfaced.

In situations other than direct marketing of own products the general opt-in system is compliant with the first of the two possible options allowed by Art. 13(3) ePrivacy Directive. Legitimate interests of subscribers other than natural persons with regard to unsolicited communications are protected only by means of Art. 172 TL, as the prohibition established in Art. 10 AES covers natural persons only (also natural persons performing an economic activity).
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

As abovementioned, the opt-in mechanism is unequivocal in the Polish system and there are no exceptions to it. While facsimile machines (fax) are not verbally included in the prohibition established by Art. 172 TL, it can be argued that they, too, should be covered by the expression “automated calling systems for direct marketing”, of course as long as long as they are operated automatically.
### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

<table>
<thead>
<tr>
<th>There are no exceptions to the opt-in mechanism in Poland (not even when Art. 13(2) ePrivacy Directive requires replacing it with the opt-out mechanism).</th>
</tr>
</thead>
</table>
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

No such distinctions apply.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. During the interview with GIODO I was informed that the authority is now working on a communication on spam, to be published soon on its website. Furthermore, in 2002 GIODO signed an agreement with the Polish Association of Direct Marketing (Stowarzyszenie Marketingu Bezpośredniego) establishing a Code of Conduct in Direct Marketing. The Agreement is available at: http://www.giodo.gov.pl/data/filemanager_pl/wsp_krajowa/SMB.pdf (in Polish only).

b. A very pertinent example of an administrative case involving unsolicited direct marketing communications is a case decided by GIODO (No. DOLiŚ/DEC – 585/13), on a complaint of a subscriber (a natural person) of a telecommunications service against a telecommunications operator providing him telecommunications services and sending direct marketing communications despite the subscriber objected this explicitly when signing his contract with the operator. While GIODO supported the complaint, emphasising in particular subsequent objections of the subscriber to having his personal data processed for marketing purposes by the operator, its decision was based on general data protection rules only.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| Filing a complaint to GIODO is the only – even if vaguely feasible - remedy to unsolicited commercial communications. First, however, as the case mentioned in Section E.5, makes it clear, GIODO decides such cases on the basis of general data protection rules, rather than those implementing the ePrivacy Directive. This is not problematic in functional terms, as the two systems lead to the same normative conclusions, posing the question of whether Art. 13 ePrivacy Directive is necessary. Second, GIODO should not be expected to act effectively in respect to third country infringers. 

Theoretically, subjects of personal data may – alternatively to complaining to GIODO – file a case before a civil court (when unsolicited commercial communication ensues a damage or a violation of personal rights) or before a criminal court (according to Art. 24 AES). In practice this does not happen. One reason for this situation may be related to a generally miniscule individual incremental damage/harm caused by spamming, smaller than the costs of efforts necessary to pursue a court case. The second one is related to the fact that a big share of unsolicited commercial e-mails is sent from other jurisdictions, primarily from outside the EU. Those limitations apply in a similar manner to penal provisions of Art. 24-25 AES (see Section E.1). In practice, therefore, anti-spam software is a more practical solution to the problem than legal provisions.

Of course, none of these problems may be eliminated by enhancing the harshness of potential sanctions, nor by improving the uncompromisingness of the prohibitions. On the other hand, the existing prohibitions and sanctions may exert a discouraging effect on at least some of the service providers who would otherwise have no scruples to spam Internet users.

It should also be mentioned that the discrepancy between Polish rules on unsolicited communications and Art. 15(2) ePrivacy Directive is not particularly problematic in practice, as providers of goods or services routinely insert consent clauses regarding processing of personal data for marketing purposes in contracts with their clients. This, however, does not inhibit the conclusion that the discrepancy is problematic in purely legal terms referring to transposition obligations. |
COUNTRY REPORT
PORTUGAL

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Luís Neto Galvão, SRS Advogados

Date: 14 August 2014
Content

Part 1: Management summary ................................................................................................. 3
Part 2: Answers to the questionnaire .......................................................................................... 4
Part 1: Management summary

Management Summary for Portugal

The transposition of the ePrivacy Directive into Portuguese law can be summarized as follows:

- The ePrivacy Directive has in general been carefully transposed and there are no material negative variations with regard to the provisions of the implementing piece of legislation, Law 41/2004, of 18 August.
- The Portuguese Data Protection Authority or “Comissão Nacional de Protecção de Dados” (www.cnpd.pt), is in charge of implementing and supervising the application of the (bulk of) provisions of Law 41/2004, of 18 August (it is arguable whether or not the CNPD can adequately implement such rules, due to scarce human and financial resources).
- Law 41/2004, of 18 August, does not specifically regulate its territorial scope, which is why we apply to that effect the general criteria contained under the Data Protection Law.
- The rules on the material scope of Law 41/2004, of 18 August, are effective and protect the privacy of clients of publicly available electronic communications networks and services.
- However, Law 41/2004, of 18 August does not directly address its territorial scope and, from a legal clarity standpoint, it would be beneficial that a provision specifically addressing this issue be inserted in the same law (as is the case with article 4 of Law 67/98, of 26 October, the Data Protection Law). The users of services that, in order to be provided, use publicly available electronic communications networks and services are not covered by specific rules on privacy (namely, information society services such as webmail, social media, location services, etc.). The users are only protected by the general rules of the Portuguese Data Protection Law and could benefit from a more specific set of rules.
- With regard to cookies, the rules of the Data Protection Law on prior information are generic and take no account of the specific circumstances in which the information is stored and accessed in terminal.
- Because of the evolving traits of cookies and of the importance of simplicity and effectiveness when obtaining online consent, guidance is absolutely necessary in order to create awareness and confidence in operators, followed by enforcement.
- The rules on the lawful processing of traffic and location data contained in 41/2004 have so far been effective, but the interaction of these rules with the rules on retention of data which implement Directive 2006/24/EC in Portugal (Law 32/2008, of 17 July), and with the rules of Law 109/2009, of 15 September, which transposed Framework Decision 2005/222/JAI, of the Council, has been problematic.
- The rules on the processing of location data adequately protect the privacy of individuals who are subscribers or users of electronic communications services or networks, but do not cover location services provided by information society services, which is an area solely regulated by the legislation implementing the Data Protection Directive. A specific protection of location data collected by such services could be adopted.
- The rules on unsolicited direct marketing communications are clear enough but the effectiveness of implementation has been extremely low.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Portugal:
- Directive 2009/136/EC has been transposed into Portuguese law by Law 46/2012, of 29 August;
- The provision on unsolicited communications was initially integrated in Decree Law 7/2004, of 7 January (“Electronic Commerce Law”), implementing the Electronic Commerce Directive but it was subsequently revoked by Law 46/2012, of 29 August, and integrated into Law 41/2004 – the regulation of spam is nowadays part of the diploma which transposed the ePrivacy Directive.

<table>
<thead>
<tr>
<th>Concordance table</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePrivacy Directive</td>
</tr>
<tr>
<td>Art. 2 (Definitions)</td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
</tr>
<tr>
<td>Art. 6 (Traffic data)</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:
- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comissão Nacional de Protecção de Dados / Portuguese Data Protection Commission</td>
<td>CNPD / NDPC (the CNPD does not use an English translation of short name; therefore, CNPD would be more appropriate, even in English)</td>
<td>All matters within its competence, inter alia the provisions that transposed articles 5.2, 5.3, 6, 9, and 13 of the ePrivacy Directive</td>
<td><a href="http://www.cnpd.pt/index.asp">http://www.cnpd.pt/index.asp</a></td>
</tr>
<tr>
<td>Autoridade Nacional de Comunicações / Portuguese Electronic Authority</td>
<td>ANACOM / PECA (ANACOM does not use an English translation of short name; therefore, ANACOM would be more appropriate, even in English)</td>
<td>All matters within its competence, namely the provisions that transposed article 5.1. of the ePrivacy Directive</td>
<td><a href="http://www.anacom.pt/">http://www.anacom.pt/</a></td>
</tr>
</tbody>
</table>

Explanation:

- The Portuguese Data Protection Authority or “Comissão Nacional de Protecção de Dados” (www.cnpd.pt) is the Data Protection Authority in Portugal. The CNPD is in charge of implementing and supervising the application of the national provisions transposing the ePrivacy Directive in Portugal (Law 41/2004), including (with relevance for this study) articles 5.2, 5.3, 6, 9, and 13 of the ePrivacy Directive.

- The Portuguese Electronic Communications Authority (ANACOM, www.anacom.pt) is the national regulatory authority (NRA) in Portugal for the electronic communications sector and the entity responsible for the management of the radio-electric spectrum.
- With regard to the matters covered by the ePrivacy Directive, ANACOM intervenes in all matters in connection with its sphere of competence, including the provisions that transposed article 5.1. (Confidentiality) of the ePrivacy Directive.

- The CNPD instructs all infringement procedures with regard to matters such as those covered by articles 5.2. (recording of communications), 5.3 (cookies), 6 (traffic data), 9 (location data), and 13 (spam) of the ePrivacy Directive.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Portugal:

Pursuant to Article 2, paragraph 3, of Law 41/2004, unless such law contains itself a specific definition, the defined terms used in Law 41/2004 are to be interpreted in accordance with the definitions used in Law 67/98, of 26 October, which transposed Directive 95/46/EC into Portuguese law (the “Data Protection Law”) and in Law 5/2004, of 10 February, as amended, which transposed the European Framework for Electronic Communications into Portuguese law (the “Electronic Communications Law”).

With regard to the term “networks”, the corresponding definition contained in the Electronic Communications Law applies. According to Article 3, point cc), of the Electronic Communications Law, electronic communication network is defined as “transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed”.


The Law defines “public” and “non-public” networks. The following is regarded as a “public” network: “an electronic communication network used wholly or mainly for the provision of electronic communications services available to the public” (Article 3, point dd), of the Electronic Communications Law).

In addition, Article 3, point ee), defines “electronic communication service”, as: “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, without prejudice to the exclusion referred to in points a) and b) of paragraph 1 of article 2”.

The services excluded in the final part of the definition of electronic communication service (referred to in points a) and b) of paragraph 1 of article 2), are “information society services, as defined in Decree-Law number 58/2000 of 18 April, which do not wholly or mainly consist of the conveyance of signals over electronic communications networks” and “services which provide or which exercise editorial control over content transmitted over electronic communications networks and services, including television and radio programme services and audio-text and value-added message-based services” (Article 2, paragraph 1, points a) and b), of the Electronic Communications Law).

Finally, electronic communications networks means “transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic
means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed” (Article 3, point cc), of the Electronic Communications Law).

With regard to the concept of “provider”, both Law 41/2004 and the ePrivacy Directive that it transposes, refer to “providers of publicly available electronic communication services” and “provider of a public communications network”, but do not specifically define “provider”. The same applies to the Electronic Communications Law, which defines electronic communications services and networks, as previously mentioned.

Finally, the scope of Law 41/2004 also comprises the natural or legal persons that use automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing (unsolicited communications).

The scope of the ePrivacy Directive is similar to that of Law 41/2004. Law 41/2004 applies to the processing of personal data in connection “with the provision of publicly available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices, specifying and complementing the provisions of Law No 67/98 of 26 October (Law on Protection of Personal Data)” (Article 1, paragraph 2, of Law 41/2004).

Similarly, the ePrivacy Directive applies to “the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community”, and the provisions of the ePrivacy Directive “particularise and complement Directive 95/46/EC” (Article 1, paragraph 2, and Article 3, paragraph 1, of the ePrivacy Directive).
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

Portugal:

Both the ePrivacy Directive and Law 41/2004 apply to the processing of data in connection with the provision of publicly available electronic communications services in public communications networks.

As previously analysed, for the purposes of Law 41/2004 an “electronic communication service” is a “a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (...)” (Article 3, point ee), of the Electronic Communications Law).

VoIP services are considered electronic communications services if they are provided in order to allow “wholly or mainly in the conveyance of signals on electronic communications networks”.

For instance, Voice over IP (“VoIP”) services using numbering resources will be considered equivalent to voice services based in publicly switched telephone networks, which are clearly electronic communications services. The ongoing deployment of fibre networks shows a trend to all IP based networks, which means that the fixed voice services have a tendency to become fully VoIP.

In this regard, please note that according to the Framework Directive, in its paragraph (5), the framework introduced by the directive “does not therefore cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services”.

In its Public Consultation on the regulatory approach to voice services supported in IP technology (VoIP), of 13.01.2006 (http://www.anacom.pt/render.jsp?contentId=1092219&languageId=1), ANACOM excluded some types of VoIP services from the notion of electronic communications services, namely the transport of voice in IP packets in public Internet (e.g. Skype) or voice services which are used in a private environment, which is not a commercial service offer (not publicly available).

However, VoIP services such as the use of VoIP in the IP backbone to support the voice communications of an international operator or a public communications network operator which only uses VoIP technologies internally within its own network (IP backbone), will be considered electronic communications services, as well as VoIP services that allow calls to be received and made from and to numbers part of the national numbering plan (NNP).

Other services as webmail or location based services, to the extent that they are based in other electronic communications services, such as the Internet access provision do not fall under the scope of Law 41/2004.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

### Portugal:

Law 41/2004 applies to the processing of personal data in the context of publicly available electronic communications networks and services, specifying and complementing the provisions of Law 67/98, of 26 October (the Data Protection Law).

Law 41/2004 does not specifically regulate its territorial scope, which is why we apply the general criteria contained under the Data Protection Law.

Article 4 of Law 67/98, of 26 October (the “Data Protection Law”) is titled “Scope of Application” and regulates the territorial scope of its application, namely:

(i) The first relevant criteria is that the Data Protection Law (and also Law 41/2004), applies to the processing of personal data undertaken in the context of the activities of an establishment of the data controller in the Portuguese territory.

    In order to understand if a data controller has an establishment in Portugal, it is required that such establishment carries out a direct and effective activity in the country.

    In this regard, paragraph (19) of the Data Protection Directive (Directive 95/46/EC), which was implemented in Portugal by the Data Protection Law, mentions that “establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements” and that “the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect”.

    Therefore, in order for Portuguese law to apply the controller must have some form of local representation in the country (see also the Google Case, Case C-131/12 Google:C:2014).

(ii) The second criteria is that the Portuguese Data Protection Law applies outside of the Portuguese territory, but in a place, such as an Embassy, where Portuguese law applies by virtue of international public law, and;

(iii) The third criteria relates to the activities of a controller who is not established in the European Union territory and who makes use of equipment, automated or otherwise, situated on Portuguese territory for purposes of processing personal data, unless such equipment is used only for purposes of transit through the territory of the European Union.
Under this criterion, the existence of physical means such as servers in the Portuguese territory will determine the applicability of the law.

Therefore, in the absence of an establishment of a controller in Portugal or of servers or other equipment in connection with the processing of data of an entity in a third country, Portuguese Data Protection Law (as well as Law 41/2004), does not apply to the processing of data (in this regard, see also Article 29 Working Party Opinion 8/2010 on applicable law, WP29 179).
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

**Portugal:**

a. ANACOM provides guidance in relation to the scope of the notions of electronic communications networks and services in a form that companies must file in order to initiate the provision of electronic communications networks and services under the general authorisation regime.

A link to such a form, which describes in an indicative manner the different types of networks and services covered by the abovementioned concepts can be found at:


b. We are not aware of any court cases in Portugal with regard to the interpretation of the term “operator” in the context of the Electronic Communications Law or of Law 41/2004.
7. What is your individual view of:
a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
b. possible improvements of the effectiveness of this legal framework.

**Portugal:**

a. The rules on the material scope of Law 41/2004, implementing the ePrivacy Directive are effective and protect the privacy of clients of publicly available electronic communications networks and services. However, Law 41/2004 does not directly address its territorial scope and it would be beneficial, from a legal clarity standpoint, that a provision specifically addressing this issue be inserted in the same law (as is the case with article 4 of the Data Protection Law).

b. The specific rules on privacy protect users of publicly available electronic communications networks and services. However, they do not protect “users of services that in order to be provided use publicly available electronic communications networks and services”. This means that the users of electronic communications services provided by BT, COLT or O2 are protected, but the users of Youtube, Amazon or eBay are not (the latter are not electronic communications services but information society services). The users are only protected by the general rules of the Portuguese Data Protection Law and could benefit from a more specific set of rules.
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Portugal:

The principle of confidentiality of communications is included in the list of rights, freedoms and guarantees part of the Portuguese Constitution. Pursuant to Article 34, paragraph 1, of the Portuguese Constitution, the secrecy of correspondence and other means of private communications are inviolable.

In addition, the Criminal Procedure Code extensively regulates the interception of communications, making phone tapping and the access to traffic and location data subject to a judicial order (Articles 187 to 190).

In the electronic communications sector, the “security of public networks against unauthorised access according to legislation governing personal data and privacy protection in respect of electronic communications”, is one of the conditions/obligations that providers of electronic communications networks and services can be subject to under the general authorisation regime (Article 27, paragraph 1, f), of the Electronic Communications Law).

In addition, providers may also be subject to a condition/obligation related to “personal data and privacy protection with specific respect to electronic communications, in accordance with legislation governing personal data and privacy protection” (Article 27, paragraph 1, h), of the Electronic Communications Law).

More specifically, Law 41/2004 provides for the inviolability of communications. In its Article 2, point d), “communication” is defined as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service”. This definition partly reproduces the ePrivacy Directive (Article 2, paragraph d)).

The regime of the inviolability of communications is regulated in Article 4 of Law 41/2004 in the following manner:

“1 – Undertakings providing electronic communications networks and/or services shall ensure the inviolability of communications and the related traffic data by means of a public communications networks and publicly available electronic communications services.

2 - Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users is prohibited, without the prior and explicit consent of the users concerned, except for cases provided for in the law.

3 – The provision in the present article shall not affect any legally authorized recording of
communications and the related traffic data, when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction, nor of any other communication made in the scope of a business relationship, provided that the data subject has been informed thereof and given his consent thereto.

4 - Recordings of communications by and for public services intended to provide for emergency situations of any nature shall be authorized.”

In Article 4, the Portuguese legislator deliberately uses the term “inviolability” instead of “confidentiality” in order to enhance the relevance of the obligation in question. In paragraph 1 of Article 4, the legislator made the obligation to ensure the inviolability of communications and respective traffic data incumbent upon “undertakings providing electronic communications networks and/or services”.

In paragraph 2 of Article 4, the Portuguese legislator requires the “prior and explicit consent of users concerned” for interception or surveillance of communications. Such requirement reinforces the wording used in Article 5, paragraph 1, of the ePrivacy Directive, which only refers to the need to obtain the “consent” of the users concerned. This is an obligation that derives from the Data Protection Law, but the legislator decided to establish the need for a prior and explicit consent expressly in Law 41/2004.

With regard to the matter of legally authorised recordings of communications, the legislator imposes in Article 4, paragraph 2, that such recording be effected on the basis of the informed consent of the data subject, a requirement that was not contained in the ePrivacy Directive.

Finally, in paragraph 4 of Article 4, the legislator authorises recordings in order to respond to emergency situations, a matter that is not dealt with by the ePrivacy Directive.

The breach of paragraphs 1 to 3 of Article 4 is an administrative infringement punishable with a penalty between 5,000€ and 5,000,000€ (Article 14, paragraph 1, point d), of Law 41/2004).

The CNPD is competent for instructing the infringement procedure in relation to the breach of the obligation in Article 4, paragraph 3. With regard to the breach of Article 4, paragraphs 1 and 2, ANACOM will be the entity in charge of instructing the penalty procedures.
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

Portugal:

This provision has been transposed in Article 4 of Law 41/2004.

Article 4, paragraph 3, of Law 41/2004 provides that the inviolability of communications does not prevent “any legally authorized recording of communications and the related traffic data” from taking place “when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction”, as well as “any other communication made in the scope of a business relationship”. In order for such recordings to be effected, the data subject must have “been informed thereof and given his consent thereto”.

In September 2010, the CNPD adopted a resolution containing a very substantial guidance on the principles applicable to the recording of communications (Resolution 629/2010).

The CNPD established that the processing of data in connection with the recordings must be notified to the CNPD and subject to an authorization.

With regard to the companies undertaking recordings of the communications with their clients, the workers must be informed that the recordings will take place. The clients must have been informed and given their consent for the recording, which must take place in the context of a lawful business practice for the purpose of “providing evidence of a commercial transaction” or “in the scope of a business relationship”.

Such recordings cannot be used in order to control the individual performance of workers.

However, the CNPD allows that the recording of calls takes place in order to control the generic quality of the performance of the workers in a call centre, provided a number of requirements are complied with, namely:

(i) the recordings must take place randomly and never comprising systematically the same worker;

(ii) only 5% of the total calls can be recorded;

(iii) the right of information must be complied with;

(iv) the express and unambiguous consent of all the intervening parties (worker and clients) be obtained;

(v) the recordings cannot be used to control the performance of the worker.

Finally, the CNPD sets as a rule a period of retention of the recordings that cannot exceed 90 days – a very short period - in relation to recordings undertaken for proof of a commercial transaction.
or in the context of a business relationship, and a period of 30 days for recordings undertaken for the purpose of quality control of the performance of a call centre.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

**Portugal:**

As previously analysed in B1., other than the exceptions to the inviolability of communications contained in article 4 of Law 41/2004, the Criminal Procedure Code extensively regulates the interception of communications and allows phone tapping and the access to traffic and location data, provided that such access is subject to a judicial order (Articles 187 to 190). Therefore, a Public Prosecutor cannot access traffic or location without it being previously authorised by a judge.

In addition, please note that article 4 includes an exception not contained in the ePrivacy Directive, whereby the recordings of communications are authorized if undertaken “by and for public services” and if such recordings are “intended to provide for emergency situations of any nature” (Article 4, paragraph 4).

Finally, the CNPD considers to be covered by the exception of Article 4, paragraph 3, the recording of calls with the purpose of monitoring the generic quality of the performance of the workers in a call centre. However, it introduces a number of requirements, all explained in the answer to Question B.2.
4. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

Portugal:

a. Portuguese law does not address specifically “automated breaches of confidentiality without human involvement”. Such breaches will be considered an infringement of article 4 of Law 41/2004, unless they fall under the scope of the exceptions contained in the same article.

Breach of article 4 of Law 41/2004 is an administrative infringement punishable with a fine between €5,000 and €5,000,000, when committed by a legal person (the fine will be between €1,500 and €25,000, when the infringement was committed by an individual).

In addition, the breach of confidentiality without human involvement (a concept that is perhaps a misnomer, given that it would always require some form of human intervention causing the automated breach), could also constitute a crime.

Article 194 of the Portuguese Criminal Code relates to the crime of breach of correspondence or telecommunications. Pursuant to its paragraph 1, “the person who, without consent, opens a parcel, letter or any other piece of writing which is closed and that is not addressed to him or her or who becomes aware, by technical methods, of its contents, or who prevents, by any means, that it is received by the addressee, shall be punished with up to 1 year in prison or with a fine of up to 240 days” - each day is around €100.

Paragraph 2 of the same Article 194 provides that the same penalties applicable under paragraph 1 shall apply to the person who, without consent, interferes with the content of telecommunications or becomes aware of it.

Finally, under paragraph 3, the person who, without consent, shares the contents of letters, parcels, closed written documents or telecommunications in the manner mentioned in paragraphs 1 and 2 shall be punished with up to 1 year in prison or a fine of up to 240 days.

Portuguese law protects in an equivalent manner the content of communications and other data such as traffic and location data. Namely, the regime of the legal interception of communications covering phone tapping and access to traffic and location data requires prior authorization by a judge, thus making no distinction between content and other data.

b. Other than the legislation already mentioned in this report, we should also mention Law 109/2009, of 15 September (the “Cyber Crime Law”), which implements the Framework Decision
number 2005/222/JHA, relating to attacks against information systems.

In Article 18, the Cyber Crime Law regulates the interception of communications with regard to investigations in connection with the crimes contained in that same law, such as illegal access to information systems or illegal interception of system data transfers.

Pursuant to paragraph 1 of the same article, the interception of communications is admissible when the authorities investigate crimes contained in the same law or who are committed using a computer system or in relation to which the evidence must be collected in electronic form and they are contained in article 187 of the Criminal Procedure Code (such as drug trafficking or smuggling).

The interception can involve content data or the collection and registry of data relating to traffic, and the judicial order authorising it must specify the scope of investigation in accordance with the concrete needs of investigation.

Portuguese law protects in an equivalent manner the content of communications and other data such as traffic and location data. Namely, the regime of the legal interception of communications covering phone tapping and access to traffic and location data requires prior authorization by a judge, thus making no distinction between content and other data.

b. There is no important legislation in Portugal with regard to the protection of private electronic communications other than that described above.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

**Portugal:**

a. The rules on cookies are contained in Article 5 of Law 41/2004 and are identical to those included in article 5.3 of the ePrivacy Directive.

Pursuant to article 5 of Law 41/2004, titled “Storage and access to information”:

“1 - The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [Law 67/98, of 26 October, the Data Protection Law], inter alia, about the purposes of the processing.

2 - Nothing in this article and in the preceding article shall prevent any technical storage or access:

a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;

b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

b. Article 5 of Law 41/2004 makes no distinction between types of cookies or between the types of device used.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

**Portugal:**

There is still no guidance on the practical implementation of article 5 of law 41/2004, namely regarding the informed consent rule. There is no guidance about the use of pop-up screens or consent bars, although they are a generalised practice in the market.

There are no specific rules/practices on which information needs to be provided. However, Article 5 has a direct reference to the applicability of the Data Protection Law (Law 67/98, of 26 October), which requires that the data subject be provided with information on:

1. the identity of the controller;
2. the purposes of the processing;
3. other information, such as, the recipients or categories of recipients, the existence and conditions of the right of access and the right to rectify.

Because the data are being collected on the Internet, the Portuguese Data Protection Law requires that the data subject be informed “except where he is already aware of it, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties”.

The rules of the Data Protection Law on prior information are generic and take no account of the specific circumstances in which the information is stored and accessed in terminal equipment, as such rules have been drafted for situations – in the case of online collection - where the data subject provides directly the information, namely by filling in an online form.

Therefore, it would be useful if some guidance was issued in this regard, although the inexistence so far of any infringement procedure or complaint on the matter may have contributed to such absence of guidance. The CNPD feels that “the law is clear”, but the official did not exclude the possibility of issuing some guidance on cookies still in the course of 2014.

Finally, the law does not allow the setting up of cookies before individuals have provided consent. In fact, the law explicitly requires that “prior consent” be given before any storage of information in the terminal equipment and access to such information takes place.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The exceptions to the informed consent, contained in Article 5, paragraph 2, of Law 41/2004, have been transposed with no variation in relation to the text of the ePrivacy Directive.</td>
</tr>
<tr>
<td>Article 5 of Law 41/2004, titled “Storage and access to information”, provides:</td>
</tr>
<tr>
<td>“1 - The storage of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the Law on Protection of Personal Data, inter alia, about the purposes of the processing.</td>
</tr>
<tr>
<td>2 - Nothing in this article and in the preceding article shall prevent any technical storage or access:</td>
</tr>
<tr>
<td>a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;</td>
</tr>
<tr>
<td>b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.</td>
</tr>
<tr>
<td>No guidance has been adapted to date on the treatment granted to different types of cookies. Such guidance may be adopted in the course of 2014.</td>
</tr>
</tbody>
</table>
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

Portugal:

There are clearly different approaches in the market to the obligations on cookies, from mere non-compliance to the use of pop-ups for providing consent, or references to the fact that the use of the site presupposes the (implied) consent to the use of cookies. The absence of guidance from the CNPD is likely to be part of the reason for this situation.

There are no official statistics on compliance. However, at the end of 2012 KPMG prepared a study on compliance with legal rules on cookies that showed that 80% of the Portuguese sites analysed were in breach of the law. KPMG analysed sites from public bodies and from companies in the sectors of energy, communications, insurance, banking distribution and transport.

A press release from KPMG regarding this study can be found at:


As previously mentioned, it is likely that the CNPD will prepare a guidance document and release it to the market still in 2014.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. With regard to guidance, it is possible that the CNPD will take some initiative in this regard still in 2014.</td>
</tr>
<tr>
<td>b. The CNPD is not aware of any complaints regarding cookies, which explains the reason why no proceedings were adopted to date on this matter (the CNPD usually acts upon complaint). This also explains the reason why there is no case law on the matter.</td>
</tr>
<tr>
<td>b. Not available.</td>
</tr>
<tr>
<td>10. What is your individual view of:</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?</td>
</tr>
<tr>
<td>b. possible improvements of the effectiveness of this legal framework.</td>
</tr>
<tr>
<td>a.</td>
</tr>
<tr>
<td>b.</td>
</tr>
</tbody>
</table>

**Portugal:**

a. The rules on cookies are not very effective given that they follow the wording of the ePrivacy Directive (which is not sufficiently prescriptive). Because of the evolving traits of cookies and of the importance of simplicity and effectiveness when obtaining online consent, my personal opinion is that guidance is absolutely necessary in order to create awareness and confidence in operators.

However, after the guidance is adopted, the only manner to measure and ensure the effectiveness of the rules is to monitor its compliance. For instance, such monitoring would allow control over compliance with information requirements (it is likely that notices do not adequately inform on the types of cookies used).

b. The effectiveness of the legal framework would greatly improve with guidance (preceded by a public consultation), and with monitoring of compliance and repressing the infringement of the rules by sites.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Portugal:

Traffic data is defined in Law 41/2004 in a manner identical to that provided in the ePrivacy Directive. Pursuant to Article 2, paragraph 1, of Law 41/2004, traffic data “means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof”.


Pursuant to Article 2, point c), of Law 109/2009, "Traffic data" shall mean any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service”.

One question relevant to the definition of traffic data that was resolved by jurisprudence was whether or not the IP number, in a given date and hour, can be accessed by the Public Prosecutor without an order of a judge.

The general regime of access to traffic data set in the Criminal Procedure Code makes access to traffic data subject to a judicial order. Recent jurisprudence of higher Courts has concluded that such regime is not applicable to the provision of the IP number of a given user at a particular date and time and that no judicial order is required to that effect.

However, when the request comprises the use of IP addresses in a given period of time or on multiple communications effected by a suspect, then the generated traffic is subject to the general regime of access to traffic data and a judicial order is required.

The Public Prosecutor’s Office (Ministério Público), issued in 2013 a note summarizing recent jurisprudence on this matter:

http://cibercrime.pgr.pt/index.html

In addition, we include a link to a very recent decision of the Court of Appeal of Lisbon on this matter:

http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d08003
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

**Portugal:**

Article 6 of Law 41/2004 provides for the legal requirements for the lawful processing of traffic data and/or for providing traffic data services.

Pursuant to Article 6 of Law 41/2004, titled “Traffic data”:

1. Without prejudice to the following paragraphs, traffic data relating to subscribers and users which have been processed and stored by undertakings providing electronic communications networks and/or services shall be erased or made anonymous where they are no longer needed for the purpose of the transmission of a communication.

2. The processing of traffic data necessary for the purposes of subscriber billing and interconnection payments shall be permitted, namely:
   
   a) Number or identification, address and type of station of the subscriber;
   
   b) Total number of units to be charged for the accounting period, as well as the type, starting time and duration of the calls made and/or the data volume transmitted;
   
   c) Date of the call or service and called number;
   
   d) Other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

3. The processing referred to in the preceding paragraph shall be permissible only up to the end of the period during which the bill may lawfully be challenged or the payment be pursued.

4. Providers of electronic communications services shall only process the data referred to in paragraph 1 where the subscriber or user to whom the data relate has given his or her prior and explicit consent, which may be withdrawn at any time, and to the extent and for the duration necessary for the purpose of marketing electronic communications services or for the provision of value added services.

5. For the purposes mentioned in paragraph 2 and, prior to obtaining consent from subscribers or users, for the purposes mentioned in paragraph 4, undertakings providing electronic communications services shall provide them accurate and full information on the types of traffic data which are processed, the purposes and the duration of such processing, as well as on a possible transmission to a third party for the purpose of providing the value added service.

6. The processing of traffic data shall be restricted to workers and employees of undertakings providing electronic communications networks and/or publicly available services who are responsible for handling billing or traffic management, customer enquiries, fraud detection,
marketing publicly available electronic communications services or providing a value added service, and shall be restricted to what is necessary for the purposes of such activities.

7 - The preceding paragraphs shall apply without prejudice to the possibility for courts or other competent bodies to be informed of traffic data, in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.”

As we can notice from the translation provided above, the legal regime in Portugal for the lawful processing of traffic data and/or provision of traffic data services generally follows the contents and structure of Article 6 of the ePrivacy Directive, although a few variations have been introduced in Article 6 of Law 41/2004, namely:

(i) In paragraph 2, the legislator specifies in a list the categories of traffic data that can be processed for the purposes of subscriber billing and interconnection payments;
(ii) In paragraph 4, the consent of the subscriber or user must be “explicit”;
(iii) In paragraph 5, the information provided to subscribers or users must be “accurate and full”;
(iv) In paragraph 5, the service provider must inform the subscriber or user “on a possible transmission to a third party for the purpose of providing the value added service”, thus explicitly covering the provision of traffic data to third party controllers.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes.</td>
</tr>
</tbody>
</table>

Pursuant to Article 6, paragraph 1, of Law 41/2004, traffic data must be erased or made anonymous where such data is no longer needed for the purpose of the transmission of a communication.

There is no guidance from the CNPD or ANACOM on anonymisation, including the definition of its scope or the techniques to be used to that effect.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?  

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes. The Data Protection Authority has completed an infringement procedure in early 2014 for <em>inter alia</em> a breach of the traffic data regime by a mobile operator Optimus (Optimus has in the meantime merged with ZON, another operator, in order to form the provider NOS). The infringement was related to traffic data generated in connection with the provision of mobile services.</td>
</tr>
<tr>
<td>Other than the case previously indicated, I am not aware of any other case where traffic data rules have been applied against specific providers or sectors.</td>
</tr>
</tbody>
</table>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

**Portugal:**

The rules on the lawful processing of traffic data contained in Article 6 of Law 41/2004 have so far been effective.

However, the interaction of these rules with the rules on retention of data which implement the now invalidated Directive 2006/24/EC in Portugal (Law 32/2008, of 17 July), and with the rules of Law 109/2009, of 15 September, which implemented the Framework Decision 2005/222/JAI, of the Council, has been problematic.

In fact, such authorities often demand access to traffic data beyond the end of the period during which the bill may lawfully be challenged or the payment be pursued (in Portugal, such period is 6 months from the data of the service provision).

When confronted with the fact that such data has been erased under Law 41/2004, the authorities seek for a judicial order in order to access the special database for the purposes of data retention, even though the crimes under investigation would not be sufficiently serious to allow them access to data retained (for 1 year) under the data retention regime.

A recent decision from a first instance court decided that the investigation authorities were entitled to access electronically based traffic data under Law 109/2009, of 15 September, even after 6 months and when the crimes are not sufficiently serious to justify access under the data retention regime. This effectively poses a risk to the privacy of individual subscribers and users.

The Portuguese Data Protection Authority (CNPD) has been called to explain the boundaries of both the regimes of Law 41/2004 and of data retention to the criminal investigation authorities in the context of individual investigations, but no general public guidance has been adopted to date.
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portugal:</td>
</tr>
</tbody>
</table>

| Location data is defined in Article 7, paragraph 1, point e), of Law 41/2004, and the term means “any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service”. |

The definition is identical to that included in the ePrivacy Directive.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

### Portugal:

Article 7 of Law 41/2004, titled “Location data”, provides for the legal requirements for the lawful processing of location data and/or for providing location data services.

Article 7 provides:

“1 - Where location data other than traffic data, relating to subscribers or users of public communications networks or publicly available electronic communications services, are processed, such data may only be processed when they are made anonymous.

2 - The record, processing and transmission of location data to bodies with legal competence to deal with emergency calls, for the purpose of responding to such calls, shall be permitted.

3 - Likewise, the processing of location data shall be allowed to the extent and for the duration necessary for the provision of value added services, insofar as prior and explicit consent has been obtained from subscribers or users.

4 - Undertakings providing publicly available electronic communications services shall, namely, inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the duration and purposes of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

5 - Undertakings providing publicly available electronic communications services shall guarantee subscribers and users the possibility, using a simple means and free of charge:

a) To withdraw at any time their consent previously given for the processing of location data referred to in the preceding paragraphs;

b) To temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

6 - Processing of location data shall be restricted to workers and employees of undertakings providing electronic communications networks and/or publicly available services or of the third party providing the value added service, and shall be restricted to what is necessary for the purposes of the referred activity.”

The legal regime in Portugal for the lawful processing of traffic data and/or provision of traffic data services is identical to that of Article 6 of the ePrivacy Directive.

There are no material variations. The Portuguese legislator interfered very little with the text of the directive. One variation is that in Article 7 of Law 41/2004, the consent for the provision of value added services must be “prior and explicit”, a reference that was not included in article 9 of
the ePrivacy Directive.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes.</td>
</tr>
</tbody>
</table>

Pursuant to Article 7, paragraph 1, of Law 41/2004, “where location data other than traffic data, relating to subscribers or users of public communications networks or publicly available electronic communications services, are processed, such data may only be processed when they are made anonymous”.

There is no guidance from the CNPD or ANACOM on anonymisation, including the definition of its scope or the techniques to be used to that effect.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. There is no specific guidance issued by the CNPD or the ANACOM on the interpretation and/or application of “location data rules”. The CNPD has announced at the end of 2013 that it would adopt specific guidance on the geolocation of workers in a working environment.</td>
</tr>
<tr>
<td>b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)</td>
</tr>
</tbody>
</table>
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The rules on the processing of location data adequately protect the privacy of individuals who are subscribers or users of electronic communications services or networks.</td>
</tr>
<tr>
<td>However, Article 7 of Law 41/2004 does not cover location services provided by information society services, which is an area solely regulated by the legislation implementing the Data Protection Directive (the Data Protection Law). A specific protection of location data collected by such services could be adopted.</td>
</tr>
</tbody>
</table>
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

Portugal:

The Portuguese legislator transposed initially the provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications in Decree-Law 7/2004, of 7 January, with amendments, on certain aspects regarding information society services, which transposed Directive 2000/31/EC, of the Parliament and the Council, of 8 June 2000 (the “eCommerce Law”).

The ePrivacy Directive was initially transposed by two diplomas, namely Law 41/2004, which implemented the essential rules contained in the directive, and Decree-Law 7/2004, of 7 January, with amendments, which transposed Directive 2000/31/EC (the “eCommerce Law”).

The eCommerce Law implemented in its Article 22, titled “unsolicited communications”, Article 13 of the ePrivacy Directive, the rules with regard to advertising via e-mail.

Law 46/2012, of 29 August, deleted Article 22 of the eCommerce Law and integrated new provisions on spam in Law 41/2004, namely Article 13 – A on unsolicited communications, and Article 13-B on lists for the effect of unsolicited communications.

As a result the provisions with regard to unsolicited direct marketing communications (transposing the corresponding provisions of the ePrivacy Directive) are nowadays contained in Law 41/2004.

Pursuant to Article 13-A of Law 41/2004:

“1 - The sending of unsolicited communications for direct marketing purposes, inter alia through the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall be subject to the prior and explicit consent of a subscriber who is a natural person, or of a user.

2 - The preceding paragraph shall not apply to subscribers who are legal persons, and unsolicited communication for direct marketing purposes shall be allowed until subscribers refuse future communications and enter themselves in the list provided for in paragraph 2 of article 13-B.

3 - The preceding paragraphs shall not prevent a provider of a given product or service, who
obtained from its customers their electronic contact details for electronic mail, in the context of
the sale of a product or a service, in accordance with the Law on Protection of Personal Data, from
using such electronic contact details for direct marketing of its own similar products or services,
provided that customers clearly and distinctly are given the opportunity to object, free of charge
and in an easy manner, to such use of electronic contact details:

a) At the time of their collection; and

b) On the occasion of each message, in case the customer has not initially refused such use.

4 - The practice of sending electronic mail for the purpose of direct marketing which disguise or
conceal the identity of the sender on whose behalf the communication is made, in breach of article
21 of Decree-Law No 7/2004, of 7 January, which do not have a valid address to which the
recipient may send a request that such communications cease or which encourage recipients to
visit websites that contravene that article, shall be prohibited.

5 - Providers of publicly available electronic communications services shall be entitled to bring
legal proceedings against the offender of any of the provisions in this article, as well as in article
13-B, to protect the interests of their clients, as part of their own business interests.”

Article 13-A follows generally the wording of Article 13 of the ePrivacy Directive, with the
necessary adaptations.

In its paragraph 1, Article 13-A specifies the type of technologies covered by the opt-in
requirement concerning the sending of unsolicited communications for direct marketing
purposes.

In addition to the “automatic calling machines”, Article 13-A, paragraph 1, adds namely “facsimile
machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message
Service) and MMS (Multimedia Message Service) and other kinds of similar applications”.

Article 13-A, paragraph 1, also provides for the need for a “prior and explicit” consent for the
sending of unsolicited communications for direct marketing purposes.

Finally, article 13-A, paragraph 1, also transposes Article 13, paragraph 3, of the ePrivacy Directive
and requires opt-in also in the event of unsolicited communications by non-automatic means. The
legislator uses to that effect the expression “inter alia”: “The sending of unsolicited communications
for direct marketing purposes, inter alia through the use of automated calling and communication
systems without human intervention...”.

Therefore the opt-in consent is required when unsolicited communications are sent by both
automatic and by non-automatic means.

However, it must be acknowledged that the solution used by the Portuguese legislator to
transpose Article 13, paragraph 3, of the ePrivacy Directive does not ensure an entirely clear
result and could be improved in the future.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
</table>
The requirements for the lawful sending of unsolicited messages are contained in Article 13-A of Law 41/2004.

Pursuant to paragraph 1 of Article 13-A, the sending of unsolicited communications for direct marketing purposes, namely the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall be subject to the prior and explicit consent of a subscriber who is a natural person, or of a user.

Article 13-A, paragraph 1, transposes both paragraphs 1 and 2 of Article 13 of the ePrivacy Directive without material variations. It is worth noting that Article 13-A, paragraph 1, specifies the type of communications covered by the opt-in rule, as previously mentioned. Such specification is an addition to the contents of the ePrivacy Directive.
### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

**Portugal:**

Fully in line with Art. 13 of the ePrivacy Directive, Law 41/2004 exempts the opt-in consent mechanism when three cumulative conditions are met, namely:

1. **(i)** the customer’s electronic contact details have been obtained from the sale of a product or service in accordance with the legal and regulatory conditions on personal data protection;

2. **(ii)** the electronic contact data are used exclusively for marketing similar products or services to those previously sold and which allowed obtaining such contact data, and;

3. **(iii)** when collecting the contact data and, in the occasion of each message, in case the customers have not initially opted-out, the customers must be afforded the opportunity of easily objecting to future advertisement, free of charge.

In addition, unsolicited marketing communications can be sent for direct marketing purposes to legal persons without the need to obtain their prior consent. However, legal persons have an opt-out right and no more communications can be sent to them after they express their willingness not to receive such communications and request their inscription in an opt-out list prepared by the Directorate-General for the Consumer.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

<table>
<thead>
<tr>
<th>Portugal:</th>
</tr>
</thead>
</table>
| No. In its paragraph 1, Article 13-A of Law 41/2004 specifies the type of technologies covered by the opt-in requirement concerning the sending of unsolicited communications for direct marketing purposes. In addition to the “automatic calling machines”, Article 13-A, paragraph 1, adds namely “facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications”.

In our opinion, any direct marketing effected through Bluetooth messages, banners, instant messaging, newsfeeds and social media outreach does not qualify for the protection afforded by Article 13-A, given that such marketing is not undertaken through the use of a publicly available electronic communications services. In addition, other than Bluetooth, the other channels are information society services. |
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Since 2012, the supervisory authority for the enforcement of these rules is the Portuguese Data Protection Commission (“CNPD”, <a href="http://www.cnpd.pt">www.cnpd.pt</a>). However, in 2005 the CNPD adopted a guidance document on the general principles applicable to political marketing in the context of electronic communications:</td>
</tr>
<tr>
<td>In such guidance, the CNPD concludes that political marketing using e-mail or any form of electronic communication requires the prior, specific and informed consent of the addressee. In addition, the use of email addresses and other data for political marketing purposes must be notified to the CNPD.</td>
</tr>
<tr>
<td>In 2013, the CNPD issued an alert reminding political parties that in the context of the upcoming local elections, their electronic marketing had to be based in opt-in consent:</td>
</tr>
<tr>
<td>Both documents are drafted in Portuguese (the CNPD site does not provide an English translation).</td>
</tr>
<tr>
<td>b. As far as we are aware, there is no jurisprudence on the application of the rules with regard to unsolicited direct marketing communications. The CNPD is competent to enforce such rules since 2012 and before that ANACOM only conducted one single infringement procedure and the decision applying the fine was not appealed.</td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

**Portugal:**

The rules on unsolicited direct marketing communications are clear enough but the effectiveness of implementation has been extremely low. Enforcement was not a priority for ANACOM, while it had such responsibility. The CNPD has been undertaking enforcement procedures but no guidance or systematic monitoring has been undertaken as such, with the exception of political marketing, where the CNPD has been quite active.

Although the majority of spam does not have its origin in Portugal and escapes the scope of action of the CNPD, it would be possible to do more to inform companies and individuals of the need to obtain prior, express and informed consent before sending unsolicited commercial communications for direct marketing purposes.
COUNTRY REPORT

ROMANIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

Date: 25.08.2014
Contents
Part 1: Management summary ........................................................................................................... 3
Part 2: Answers to the questionnaire .................................................................................................. 4
Part 1: Management summary

In general, the transposition of the ePrivacy Directive into Romanian law closely follows the European text. The law mentions two competent authorities at a national level. While the national Data Protection Authority (ANSPDCP) deals with matters involving personal data processing, the National Authority for Management and Regulation in Communications (ANCOM) is assigned with aspects regarding billing.

The Constitution, the Criminal Code as well as the Civil Code, all contain provisions referring to confidentiality and the protection of private electronic communications. We note that the Romanian legislation pays much more attention to commercial communications sent via e-mail and lists in Law 365/2002 on electronic communications (and in the methodological norms for applying this law) the information to be made available to recipients of commercial communications and public authorities. However, it needs to be highlighted that the ePrivacy Directive has been transposed by Law 506/2004, therefore, Law 365/2002 is not part of the instruments transposing and implementing the Directive.

One particularity regarding the practical application of Law 506/2004 is that the national Data Protection Authority is declining in competence when it comes to protecting legal persons against unsolicited communications. Since the Romanian Constitution recognises the right to privacy of natural persons, the ANSPDCP declares inadmissible those complaints addressed by legal persons, despite the very clear text of Article 12 (4) of Law 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

Furthermore, the Romanian legislator did not transpose a definition of consent and for cookies it allows the possibility of expressing valid consent through the browser application, which is not the intention of Directive 2009/136/EC.

Law no. 298/2008 transposing Directive 2006/24/EC as well as Law no. 82/2012 on data retention have both been declared unconstitutional. Law 82/2012 has been declared unconstitutional on 8 July 2014, and therefore, as Article 147 of the Constitution mentions, after 45 days the law cease to produce legal effects. Provisions regarding data retention are still inserted in Law 506/2004 transposing the ePrivacy Directive via Emergency Government Ordinance 13/2012 amending Law 506/2004, but this does not mean that they become applicable ipso facto. Moreover, Article 152 of the Criminal Procedure Code describes the conditions in which competent authorities can access the retained data. The Constitutional Court underlined that Article 152 remains practically inapplicable until a new law on data retention is adopted.
Part 2: Answers to the questionnaire
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Directive 2002/58/EC was transposed into Romanian legislation by Law no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy in the electronic communications sector (hereafter Law 506/2004).

Following the 2009 amendments of the European Regulatory Framework for Electronic Communications, the Romanian legislator amended its legal framework by Emergency Government Ordinance no. 13 of 24 April 2012 (approved by Law no. 189 of 30 October 2012).

Also, Emergency Government Ordinance no. 111 of 14 December 2011 regarding electronic communications contains relevant definitions for this study such as electronic communications network (article 4 (6)), providing an electronic communications network (article 4 (7)), electronic communications network provider (article 4 (8)) and electronic communications service (article 4(9)). Emergency Government Ordinance no. 111 of 11 December 2011 (hereafter EGO 111/2011) replaced Law 304/2003 regarding universal service and users’ rights relating to electronic communications networks and services.

At the same time, the definitions must be complemented with the definitions found in Law no. 677 of 21 November 2001 on the protection of individuals with regard to processing personal data and on the free movement of such data (hereafter Law 677/2001).

Aside this, the National Audiovisual Council adopted through Decision no. 220 of 24 February 2011 the code for regulating audiovisual content; therefore, under Title III, articles 30 to 48 address the protection of human dignity and the right to protect one’s own image.

<table>
<thead>
<tr>
<th>Concordance table</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ePrivacy Directive</strong></td>
</tr>
<tr>
<td>---------</td>
</tr>
</tbody>
</table>
the protection of privacy in the electronic communications sector

Art. 13 (Unsolicited communications)  
Article 12 of Law no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy in the electronic communications sector, modified by Emergency Ordinance 13/2012.

Unrelated to the transposition of the ePrivacy Directive, at the same time, unsolicited communications are regulated by Article 6 of Law no. 365/2002 on electronic commerce.


<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)</td>
<td>The National Supervisory Authority for Personal Data Processing</td>
<td>Personal data processing</td>
<td><a href="http://dataprotection.ro/">http://dataprotection.ro/</a></td>
</tr>
</tbody>
</table>
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

There is no mentioning or reference in the actual text of Law 506/2004 transposing the ePrivacy Directive to the definitions of networks, electronic communications services and providers. However, Emergency Government Ordinance no. 111 of 14 December 2011 regarding electronic communications (hereafter EGO 111/2011) contains all the relevant definitions. There have been no changes of the definitions, even though Law 140/2012 further amended the Emergency Government Ordinance.

In Article 4 (1) (6) of EGO 111/2011, **electronic communications networks** are defined as: ‘transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical means or other electromagnetic means, including electronic communications networks via satellite, fixed terrestrial networks with circuit switching and packet-switching, including internet and mobile, power grids, to the extent that they are used for transmitting signals, networks used for broadcasting services of audiovisual and cable television networks, irrespective of the type of information conveyed’.

In Article 4 (1) (9) of EGO 111/2011, **electronic communications services** are defined as: ‘a service provided usually for a fee, which consists wholly or mainly in the conveyance of signals through electronic communications networks, including telecommunications services and the networks used for the transmission of audiovisual programs, but excluding services providing the content transmitted using electronic communications networks or services, or exercising editorial control over content; also, it does not include information society services, as defined in art. 1 para. 1 of Law no. 365/2002 on electronic commerce, republished, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks’.

In Article 4 (1) (7) of EGO 111/2011 defines **providing an electronic communications network** as: ‘the installation, functioning, control or making available an electronic communications network’.

Moreover, Article 4 (1) (8) of EGO 111/2011 defines the **electronic communications network provider** as: ‘a person whose activity consists wholly or mainly, in providing an electronic communications network under the general authorization regime’.

In Article 4 (1) (10) of EGO 111/2011 defines the **public electronic communications network** as: ‘an electronic communications network that is wholly or mainly used for providing publicly available electronic communications services’.

There is no definition of electronic communications providers, instead Article 4 (1) (27) of EGO 111/2011 uses the term **operator** to describe: ‘a person who installs, functions, controls or provides third parties a public electronic communications network or associated facilities, or a person who is authorized in this sense’.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

EGO 111/2011 defines electronic communications services as ‘a service provided usually for a fee, which consists wholly or mainly in the conveyance of signals through electronic communications networks […], excluding services providing the content transmitted using electronic communications networks or services, or exercising editorial control over content; also, it does not include information society services […].’

Therefore, there could be room for interpretation since it needs to be decided whether such services consist wholly or mainly in the conveyance of signals through electronic communications networks. When analysing VOIP services it could be weighted if the electronic communications service component remains marginal or if it is the core element of the service.

Email services appear to be excluded from the definition of electronic communications services since they usually represent a service providing the content transmitted using electronic communications networks. At the same time, since location based services typically rely on receiving location signals in order to send customized content, they tend to be categorized as information society services and not as electronic communications services.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

There is no public registry with cases on a specific law, therefore we are not aware of such cases. However, ANSPDCP’s 2008 activity report mentions that there has been a case involving a company offering a service for reverse searching of subscribers’ telephone numbers. The legal representative of this business declared that the website was not owned by the company which he was administering and that it belonged to a natural person in the US. The telecommunications operators did not allow the use of the subscribers’ registry; the subscribers were not notified about this processing, therefore they did not provide consent. The data processor was asked to comply with the legal requirements or stop the processing activities and delete the data. After the investigation, the website was suspended.

An electronic communications network provider is defined by EGO 111/2011 as: ‘a person whose business consists wholly or mainly, in providing an electronic communications network under the general authorization regime’. Therefore, the mentioning of the general authorization regime implies that the authorization is conducted in Romania. However, ANCOM Decision 987/2012 provides, with some exceptions, that any person who intends to provide public electronic communications networks or publicly available electronic communications services must send a notification to ANCOM.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. Since not all the definitions from the European data protection framework have been transposed, ANSPDCP recommends that the correct roles and responsibilities of all public and private parties involved in the implementation of the ePrivacy Directive are established according to the definitions found in Law 677/2001.

   Additionally, ANSPDCP Decision 11/2009 establishes that among the categories of personal data processing operations susceptible of presenting special risks for the personal rights and liberties are:

   ‘c) personal data processing operations using electronic means, for the purpose of evaluating personality aspects, as well as the professional competence, credibility, behaviour, or other aspects alike;

   d) personal data processing operations using electronic means within evidence systems for the purpose of private entities taking individual automatic decisions connected to analysing the
solvency, the economic and financial situation, the facts susceptible to engage the disciplinary, civil, or criminal liability of natural persons;’

The above processing operations are subject to prior check.

b. Not available.
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>The current rules leave room for considerable interpretation especially in respect to the notion of consent and, although the competent authorities apply sanctions, these sanctions are usually contested in court. Companies use this strategy in order to postpone payment until a final court decision is issued. Also, for some companies the fine does not represent a financial difficulty and does not guarantee future compliance, especially when, in some cases, the economic gain achieved by not respecting the legal obligations is greater than the sanction itself.</td>
</tr>
<tr>
<td></td>
<td>In practice, there are databases being sold directly on the market and there are numerous companies that use telephone numbers and e-mail addresses to send unsolicited communications. Actually, Romtelecom, one of the largest telecommunications companies in Romania, is listed number 9 in the list of spammers (UCE Protect, <a href="http://www.uceprotect.net/en/l3charts.php">http://www.uceprotect.net/en/l3charts.php</a>).</td>
</tr>
<tr>
<td></td>
<td>Abuse.ro is a Romanian portal providing a free service for reporting Romanian spam. As the abuse.ro 2013 activity report describes, on a daily basis, the average is 5% of positive results for rbl.abuse.ro (the list that publishes the IP addresses of spam senders) and 1.2% for uribl.abuse.ro (the list which publishes the top level domain names which are promoted via spam or which are used as a way to send spam). Since the figures only refer to Romanian spam, the numbers indicated are high. The lists are automatically checked by third party Internet services over 500,000 times per day.</td>
</tr>
<tr>
<td></td>
<td>An important inconsistency is the fact that while Article 12 (4) of Law 506/2004 mentions ad literam that both natural and legal persons are protected against unsolicited communications, ANSPDCP declines competence when it comes to legal persons since the Romanian Constitution recognises the right to privacy of natural persons. Therefore, legal persons cannot address complaints and are not protected in practice.</td>
</tr>
<tr>
<td>b.</td>
<td>Law 677/2001 did not implement a definition of consent and Law 506/2004 does not contain one as well. This leaves room for a greater degree of ambiguity and it also creates conflicts between the two laws. For example, Article 5¹ of Law 506/2004 allows the possibility of expressing a valid consent through the browser application, while Law 677/2001 demands explicit consent or other legal basis provided by law for processing information.</td>
</tr>
<tr>
<td></td>
<td>Furthermore, as already mentioned above, there should be a clarification regarding the competence of the National Data Protection Authority in respect of protecting legal persons from unsolicited communications.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Article 4 (1) of Law 506/2004 states that the confidentiality of communications transmitted through public electronic communications networks and publicly available electronic communications services, as well as the confidentiality of the related traffic data, is guaranteed.

In paragraph (2) of the same article it is mentioned that listening, tapping, storing and any other form of interception or surveillance of communications and traffic data are forbidden except when:
   a) it is done by the users taking part at that communication
   b) the users taking part at that particular communication gave prior written consent
   c) is done by competent authorities under legal requirements.

Also, paragraph (3) mentions that the technical storage for transmitting the communications is possible without prejudice to paragraphs (1) and (2) under the conditions of respecting confidentiality.

Moreover, Article 28 of the Constitution guarantees the right to the confidentiality of correspondence: ‘Secrecy of letters, telegrams and other postal communications, telephone conversations, and any other legal means of communication is inviolable.’

Furthermore, the confidentiality of communications is also included under Article 302 of the new Criminal Code (violation of the secrecy of correspondence):
‘(1) Opening, theft, destruction or retention, without right, of correspondence addressed to another, and without the right to disclose the contents of such communications, even when it was sent open or was opened accidentally, shall be punished with imprisonment from three months to one year or a fine.
(2) Interception, without right, of a conversation or communication by telephone or any electronic means of communication shall be punished with imprisonment from six months to three years or a fine.
(3) If the acts in para. (1) and (2) have been committed by a public official who has a legal obligation of professional secrecy and confidentiality of information to which they have access, the punishment shall be imprisonment from one to five years and interdiction of certain rights.
(4) Disclosure, dissemination, presentation or disclosure to another person or to the public, without right, of the content of calls or communications intercepted, even if the perpetrator is aware of it by mistake or by accident, is punishable by imprisonment from three months to two years or a fine.
(5) The committed act is not an offense:
   a) if the offender captures a crime or helps prove an offense;
   b) if it captures public acts that are meaningful to community life and if the disclosure of public benefits outweighs the damage caused to the person aggrieved. […]’

At the same time, Article 226 of the new Criminal Code (violation of private life) states that ‘the violations of privacy, without right, through photographing, capturing images or recordings,
listening with the use of technical means or audio recording a person in a house or room or annex which is having this private conversation will be punished with imprisonment one month to six months or a fine.

Additionally, Article 73 of the new Civil Code (the right to own image) states that for exercising the right to own image, any person can forbid or prevent the reproduction, in any way, of its physical appearance or voice or the use of such reproduction.

Law 506/2004 defines communications in Article 2 (1) d) as: ‘any information exchanged or transmitted between a limited number of participants through a publicly available electronic communications service; this does not include the information transmitted to the public through a electronic communication network as part of a service for audiovisual programmes, if a link between that information and the subscriber or identifiable user which receives the information cannot be established.’

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

Article 4 (4) of Law 506/2004 is a word by word transposition of Article 5.2 of the ePrivacy Directive and therefore it allows the possibility of performing legally authorized recordings of communications and related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or communication.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

There are several articles in the new Criminal Procedure Code that describe how surveillance and interception can be performed by competent authorities. Also, Law 51/1991 on national security and Law 14/1992 provide the rules for surveillance and intelligence activities that interfere with human rights and fundamental liberties. Moreover, Law 677/2001 mentions in Article 2 (7) that it ‘does not apply to the processing and transfer of personal data carried out during the activities in the field of national defence and security, within the limits and restrictions set by law.’

One of the articles referred to above is Article 152 of the new Criminal Procedure Code on obtaining data generated or processed by public electronic communications networks providers or publicly available electronic communications service providers, other than content of communications, data which is retained by them:

‘(1) With prior authorization of the judge of rights and freedoms, prosecution authorities may require a public electronic communications network provider or publicly available electronic communications service provider to transmit, in compliance with the special law on the retention of data generated or processed by public electronic communications networks providers and publicly available electronic communications service providers, the data retained, other than the contents of communications, if there is reasonable suspicion of committing a crime and if there are grounds for believing that the information requested constitutes evidence for the categories of offenses under the law on the retention of data generated or processed by public electronic communications network providers and publicly available electronic communications service providers.’

This article has been declared constitutional in July 2014, however the Constitutional Court underlined that the article remains practically inapplicable until a new law on data retention is adopted.

At the same time, the new Civil Code contains articles related to the right to private life, dignity and its own image, as well as the limits for these rights:

Article 71 of the new Civil Code: The right to private life
(1) Everyone has the right to respect for his private life.
(2) No one may be subject to any interference in his/her private, personal or family life at his/her domicile, residence or correspondence, without his/her consent or without respecting the limits set out in art. 75.
(3) It is also prohibited to use in every way, correspondence, manuscripts or other personal documents and private information without that person’s consent or without respecting the limits set out in art. 75.

Article 75 of the new Civil Code: Limits
(1) It is not a violation of the rights provided in this section, the interferences allowed by law or by international conventions and covenants on human rights to which Romania is a member.
(2) The exercise of constitutional rights and freedoms in good faith and in compliance with the covenants and international conventions to which Romania is a member does not constitute a violation of the rights provided in this section.
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
   - Whether the interception of MAC addresses would entail breach of confidentiality;
   - Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
   - Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Romanian legislation does not explicitly address ‘automated breaches of confidentiality without human intervention’. However, it is important to mention that Romania ratified the Cybercrime Convention by Law 64/2004.

Article 1 (j) of the Government Decision 1129/2008 defines a MAC address as: ‘the physical address, representing a series of numerical characters, which uniquely identifies communications equipment in a network.’ Although this definition refers to the above-mentioned Government Decision and is not automatically applicable in correspondence with other laws, it could still provide a reference point. In order to decide whether the interception of MAC addresses could be a breach of confidentiality, it first needs to be established if MAC addresses could be personal data. However, Recital 22 of Directive 2009/136/EC should at all times be kept in mind, meaning that new identifiers could emerge and the different possibilities should not be excluded.

The non-consent based capturing of content data from unencrypted Wi-Fi networks is a form of interception and could be a breach of Article 4 (2) of Law 506/2004. As mentioned, the exceptions for listening, tapping, storing and any other form of interception or surveillance of communications and traffic data are when:
   a) done by the users taking part at that communication
   b) the users taking part at that particular communication gave prior written consent
   c) is done by competent authorities under legal requirements.

However, the law does not specify if the first two conditions need to be achieved simultaneously or not. As the text is currently drafted, there is no hint towards concluding that the conditions should be fulfilled simultaneously.

Law 506/2004 distinguishes between content and traffic data by guaranteeing in Article 4 the confidentiality of both the communications as well as the traffic data of these communications. At the same time, the new Criminal Procedure Code also makes a distinction between content and traffic data in Article 152 (1) specified above. Furthermore, Article 5 of Law 506/2004 contains specific provisions on how traffic data can be retained.

The laws on data retention (Law no. 298/2008 transposing Directive 2006/24/EC as well as Law no. 82/2012) have both been declared unconstitutional. Law 82/2012 has been declared unconstitutional on 8 July 2014, and therefore, as Article 147 of the Constitution mentions, after 45
days the law cease to produce legal effects. Provisions regarding data retention are still inserted in Law 506/2004 transposing the ePrivacy Directive via Emergency Government Ordinance 13/2012 amending Law 506/2004, but this does not mean that they become applicable ipso facto. Moreover, Article 152 of the Criminal Procedure Code describes the conditions in which competent authorities can access the retained data and has been declared constitutional by the Constitutional Court’s Decision nr. 440 of 8 July 2014.

b. The provisions of the Constitution and of the Criminal Code are equally applicable for the protection of private electronic communications.

Besides the provisions already described in section B, question 1 of this questionnaire, Chapter VI of the new Criminal Code on crimes against the security and integrity of computer data and systems, details in Articles 360-366 the rules regarding illegal access, interception, disruption and unauthorised transfer of computer data.

Computer data and systems are described in Article 181 of the new Criminal Code as:
‘(1) Computer system means any device or group of interconnected devices, or devices in a functional relationship, out of which one or more is assuring automatic processing of data, with the help of a computer program.
(2) Computer data means any representation of facts, information or concepts in a form that can be processed by a computer system.’
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Article 4 (5) of Law 506/2004 provides that:</td>
<td></td>
</tr>
<tr>
<td>‘Storing information or obtaining access to the information stored in the terminal device of a subscriber or user is allowed only if the following conditions are simultaneously fulfilled:</td>
<td></td>
</tr>
<tr>
<td>a) the subscriber or user has expressed consent</td>
<td></td>
</tr>
<tr>
<td>b) prior to expressing consent and in accordance with Article 12 of Law 677/2001 (right to be informed) the subscriber or the user has been provided with clear and comprehensive information which:</td>
<td></td>
</tr>
<tr>
<td>(i) are expressed in an easily understandable language and are easily accessible for the subscriber or user</td>
<td></td>
</tr>
<tr>
<td>(ii) includes provisions with regard to the purpose of processing the stored information by the subscriber or user and to which it has access to.’</td>
<td></td>
</tr>
<tr>
<td>b. The same article mentions that when the provider allows third parties to store or to access the stored information on the terminal equipment of the subscriber or user, the provider has to include in the notification the general scope of processing such information by third parties and the way the subscriber or user can use the settings of the Internet navigation application or other similar technologies to delete the stored information or to refuse third party access to this information.</td>
<td></td>
</tr>
<tr>
<td>The law can be interpreted to distinguish between types of cookie but it does not differentiate between the types of devices used. Complementing the above-mentioned provisions, Article 4 (6) of Law 506/2004 mentions that storing and obtaining access to the information stored is also possible a) when these operations are performed exclusively for the purpose of transmitting communications through an electronic communications network and b) when these operations are strictly necessary for providing an information society service explicitly requested by the user or subscriber. Therefore, if the service was explicitly requested, first party cookies can be stored on the user’s or subscriber’s terminal equipment without consent.</td>
<td></td>
</tr>
</tbody>
</table>
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

In respect to the consent mentioned in Article 4 (5) (a), paragraph 5 of the same article mentions that consent for storing information or obtaining access to the information stored in the terminal device of a subscriber or of a user can be given using the settings of the ‘Internet navigation application or other similar technologies through which it can be considered that the subscriber or user has expressed consent’.

This provision does not fully and correctly transpose Recital 66 of Directive 2009/136/EC which mentions that: ‘Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.’

As we can observe, the Recital recommends that the user’s consent may be expressed by using the appropriate settings of a browser or other application, where it is technically possible and effective. The Romanian law does not include this condition and it implies that consent can be given at all times using browser settings. Furthermore, the law does not enhance the powers of the national Data Protection Authority to make these technical requirements more effective or to assess if these technical requirements are enough for consent (for example in the case of browsers implementing the Do Not Track standard).

With respect to Recital 66 of Directive 139/2009, Article 29 Working Party has provided in Opinion 2/2010 on online behavioural advertising a detailed interpretation on this issue and has underlined that ‘a relevant question is to determine the conditions under which the browser settings will meet the requirements of Directive 95/46/EC, and thus constitute a valid consent [in accordance with Directive 95/46]’.

IAB Romania, the marketing and online advertising industry association (member of IAB Europe) has issued both recommendations as well as a template document for informing users about cookies. One of these recommendations refers to the fact that the user must be made aware that the site is using cookies and that he/she is recommended to check the additional information in relation to this. The recommendations for implementing are ‘through a banner placed on the first screen, through a sticky ribbon or through a widget placed visibly’.

Neither the law nor the available guidance mentions distinctions when it comes to mobile devices. When it comes to the different types of cookies, Article 4 (6), Law 506/2004 allows technical storage or access to the stored information when:

a) such operations are performed solely for the purpose of transmitting communications through a

---

b) such operations are strictly necessary for the providing an information society service, specifically requested by the subscriber or user.

Therefore, it can be interpreted that when you access a certain website, you specifically make a request for first party cookies as well.
7. How are the exceptions to the informed consent rule implemented in national law?
Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Article 4 (5) of Law 506/2004 mentions that when the provider allows third parties to store or to access the stored information on the terminal equipment of the subscriber or user, the provider has to include in the notification the general scope of processing such information by third parties and the way the subscriber or user can use the settings of the ‘Internet navigation application or other similar technologies’ to delete the stored information or to refuse third party access to this information. The legislator’s intention is not to include this provision as an exception from the informed consent rule. Instead, it states that the provider has to include information about how the subscriber or user can use the browser settings to delete the stored information or to refuse third party access to the stored information. Therefore this provision needs to be interpreted in line with Article 5 (3) of the ePrivacy Directive which states that: ‘the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.’

As already mentioned, Article 4 (6) of Law 506/2004 allows technical storage or access to the stored information when:
- a) such operations are performed solely for the purpose of transmitting communications through an electronic communications network;
- b) such operations are strictly necessary for the providing an information society service, specifically requested by the subscriber or user.
<table>
<thead>
<tr>
<th>8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice? Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In practice there is either very diverse implementation of the cookie rules or no compliance at all. The vast majority of websites do not ensure transparency and they usually do not mention or describe the types of cookies used. Actually, some of them usually just copy and paste the general information about cookies provided by IAB Romania.</td>
</tr>
</tbody>
</table>
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. ANSPDCP was requested to provide guidance as regards recording client telephone calls for the purpose of improving its own services. For obtaining the client’s consent for recording the conversation, the data processor would play a welcoming message explaining this. ANSPDCP opined that, in relation to the declared purposes, this modality of obtaining consent was in compliance with the legal requirements.

However, the authority underlined that if the collection involves sensitive data, the requirements of Law 677/2001 are applicable and written consent would thus be necessary. At the same time, the Authority highlighted that the subscriber or user must be given the possibility to object to storage or to access to the stored information and recommended that the subscriber or user be informed about the consequences of the refusal and whether there are alternative calling methods.

b. Not available
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. As observed, Article 4 (5) of Law 506/2004 mentions that consent for storing information or obtaining access to the information stored in the terminal device of a subscriber or of a user can be given using the settings of the ‘Internet navigation application or other similar technologies through which it can be considered that the subscriber or user has expressed consent’.

Although this is not an exception in connection to national law, Article 4 (5) does not respect Directive 95/46/EC provisions regarding consent, since under the directive consent means ‘any freely given specific and informed indication of data subject’s wishes by which it signifies his/her agreement to personal data relating to him/her being processed.’

b. In respect to cookies, the Romanian law does not mention that the user’s consent may be expressed by using the appropriate settings of a browser or other application, where it is technically possible and effective. Instead it states that consent can be given at all times using the browser settings. As commented by Article 29 Working Party in Opinion 2/2010 on online behavioural advertising: ‘[…] if the browser settings were predetermined to accept all cookies, such consent would not comply with Article 5(3) insofar as, in general, such consent cannot constitute a true indication of the data subject wishes.’

Furthermore, the law does not enhance the powers of the national Data Protection Authority in order to be able to ensure compliance with the technical requirement and regarding the efficiency of expressing consent by using browser settings, as Recital 66 recommends.

Additionally, the national law should be revised as regards the exceptions for listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data. In this sense, Article 4 (2) should clarify whether the first 2 circumstances for listening, tapping, storage or other kinds of interception or surveillance of communications need to be fulfilled simultaneously. Currently, this article includes three separate exceptions from the prohibition to the listening, tapping or storing or other kinds of interception or surveillance of communications:

   a) it is done by the users taking part at that communication
   b) the users taking part at that particular communication gave prior written consent
   c) is done by competent authorities under legal requirements.

Therefore, as it is currently drafted, the article leaves the possibility to argue that listening, recording, storage and any other form of interception or surveillance of communications or of traffic data could be performed when the users taking part in that communication without having any of them agree to that. In this sense, Article 73 of the Civil Code also needs to be reminded since it states that every person has the right to his/her own image and that he/she can exercise this right by forbidding or stopping any kind of reproduction of his/her voice or physical appearance.

At the same time, since neither Law 677/2001 nor Law 506/2004 implemented a definition of consent, this could also be taken into consideration in order to reduce the level of ambiguity and

---

prevent possible conflicts of laws. Despite the legislator’s motivation that the definition of consent can be understood from the Civil Code’s provisions, we still believe that a definition of consent is necessary. However, the concept of consent should not be the only driver for achieving personal data protection since fundamental rights and freedoms can be easily ‘clicked away’ when entering contractual relationships not respecting and guaranteeing such rights.

C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

| Article 2 of Law 506/2004 defines traffic data as: ‘any data processed for the purpose of transmitting communications through a public electronic communications network or for the purpose of billing the cost of that operation’. |
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects.

| Article 5 of Law 506/2004 states that traffic data relating to subscribers and users which is processed and retained by public electronic communications network providers or publicly available electronic communications service providers must be erased or made anonymous when no longer needed for the transmission of the communication, except as provided in paragraphs (2), (3) and (5):
| (2) Processing of traffic data for billing subscribers or for establishing payment obligations for interconnection is allowed only until the expiry of a period of 3 years from the due date of the corresponding payment obligation.
| (3) The provider of a publicly available electronic communications service may process traffic data related to subscribers and users for marketing its services or for providing value added services, only to the extent and for the duration necessary for marketing or providing such services, and only with prior explicit consent of the subscriber or user to which that data is related to. The subscriber or respectively, the user may withdraw consent regarding traffic data processing at any time.
| (4) In cases mentioned in paragraphs (2) and (3), the publicly available electronic communications service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing. For the purposes mentioned in paragraph (3) above, this information must occur prior to obtaining the consent of the subscriber or user.
| (5) Traffic data processed under paragraphs (1) - (4) may be performed only by persons acting under the authority of public electronic communications network providers and publicly available electronic communications service providers with attributions for billing or traffic management, customer relations, fraud detection, marketing electronic communications services or providing value-added services, and is permitted only to the extent in which it is required for these tasks.
| There is no distinction between the definition in Law 506/2004 and the text of the ePrivacy Directive.
<table>
<thead>
<tr>
<th>3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 5 of Law 506/2004 states that traffic data relating to subscribers and users which is processed and</td>
</tr>
<tr>
<td>retained by public electronic communications network providers or publicly available electronic communications</td>
</tr>
<tr>
<td>service providers must be erased or made anonymous when no longer needed for the transmission of the</td>
</tr>
<tr>
<td>communication, except as provided in paragraphs (2), (3) and (5) described above.</td>
</tr>
</tbody>
</table>
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

To our knowledge there are no cases on substantive issues where traffic data rules have been applied against specific providers or sectors. However, there is one court case which needs to be mentioned, the MyClicknet – Phorm case. The issues at stake included more than just traffic data, however the initiated court case only contested the fine applied by the Romanian Data Protection Authority (ANSPDCP).

MyClicknet was a value added service launched in 2011 by Romtelecom, one of the largest telecommunications providers in Romania. The service was meant to customize the Internet experience of subscribers and users by offering more relevant content and displaying behavioural advertising. The service was performed by placing cookies on the terminal devices of subscribers and users and it entailed redirecting a copy of the traffic data, before as well as after accepting the service, in order to analyse and process traffic data related to subscribers and users. This service was implemented by using the Phorm application and by installing Phorm equipment on the provider’s network.

The provider was not able to demonstrate compliance with Articles 4 and 5 of Law 506/2004 since it could not prove obtaining prior written explicit and informed consent from subscribers and users for traffic data processing and for installing cookies. At the same time, the provider did not install opt out cookies for subscribers and users objecting to such processing.

The service was intercepting communications and traffic data for the purpose of scanning them in order to build a user profile and, allegedly, it could exclude certain types of content.
5. **What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?**

The level of implementation of these requirements is minimal and in general there is lack of awareness about the privacy implications from both the users’ side as well as the providers’. However, there are several providers that retain data for at least 6 months in order to be able to respond to law enforcement requests.

Furthermore, as already mentioned the laws on data retention (Law no. 298/2008 transposing Directive 2006/24/EC as well as Law no. 82/2012) have both been declared unconstitutional. Yet, competent authorities may still have a legal basis for accessing traffic data under Article 152 on obtaining data generated or processed by public electronic communications networks providers or publicly available electronic communications service providers.
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 2 of Law 506/2004 as amended by Emergency Government Ordinance 13/2012 defines location data as: ‘any data processed in an electronic communications network or through an electronic communications service which indicates the geographical position of the terminal equipment of a user of a publicly available electronic communications service’. There is no difference between the definition in Law 506/2004 and the text of the Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Article 8 (1) of Law 506/2004 states that, when it is possible, processing location data, other than traffic data, relating to users or subscribers of public electronic communications networks or publicly available electronic communications services, is allowed only in one of the following cases:

a) data is made anonymous;

b) with prior explicit consent of the user or subscriber to which that data refers to, to the extent and for the duration necessary for providing a value added service;

c) when the value-added service with location function has the purpose of unidirectional and non differentiated transmission of information to users.

(2) The publicly available electronic communications service provider is required to provide the user or subscriber, prior to obtaining consent, in accordance with para. (1) b) information regarding:

a) the type of location data, other than traffic data, which will be processed;

b) the purposes and the duration of processing;

c) any transmission of these data to a third party for the purpose of providing the value added service.

(3) Users or subscribers consenting to the processing of data in accordance with para. (1) b) have the right to withdraw, at any time, their consent regarding the processing of data or to temporarily refuse the processing of those data for each connection to the network or for each transmission of a communication. Publicly available electronic communications service providers shall make available to users or subscribers a simple and free of charge procedure for exercising these rights.

(4) Processing location data, other than traffic data, under para. (1) - (3) can be performed only by persons acting under the authority of public electronic communications network providers or publicly available electronic communications service providers or under the authority of a third party provider of value added services and must be limited only to what is necessary for providing the value added service.

Paragraph 5 of this article has been deleted and paragraph 6, regarding access by competent authorities to the retained data, has been declared unconstitutional by the Constitutional Court’s Decision nr. 440 from 8 July 2014.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Article 8 (1) (a) of Law 506/2004 provides that one of the conditions for the lawful processing of location data other than traffic data is when data is made anonymous.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Not available</td>
</tr>
<tr>
<td>b.</td>
<td>Not available</td>
</tr>
<tr>
<td>5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>
| The level of implementation of these requirements is minimal and in general there is lack of awareness of privacy implications from both the users’ side as well as the providers’.
|
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. Provisions regarding unsolicited communications are found in Article 12 of Law 506/2004, transposing the ePrivacy Directive. Additionally, Article 6 of Law 365/2002 on electronic communications contains provisions on commercial communications. At the same time, Decision no. 1308 of 20 November 2002 approving the methodological norms for the application of Law 365/2002 on electronic communications sets in Chapter II, articles 7-9, contains further provisions regarding commercial communications.

   Article 6 of Law 365/2002 establishes the rules for commercial communications only sent by electronic mail, while the scope of Article 12 of Law 506/2004 is much broader.

   b. Article 12 of Law 506/2004 provides that commercial communications are forbidden through the use of automated calling systems that do not need human intervention, through fax or electronic mail or through any other method which uses publicly available electronic communications services, except when the respective user or subscriber has expressed prior explicit consent for receiving such communications.

   There are no differences when it comes to the scope and substance of Article 13 of the ePrivacy Directive and the same terminology is being used, except for the fact that the term used is commercial communications (and not unsolicited communications) and that explicit prior consent is required.

   At the same time, although the provisions of Article 12 of Law 506/2004 refer to both natural and legal persons, the national Data Protection Authority is declining its competence in respect of legal persons. ANSPDCP position is that the Constitution grants the right to personal, family and private life only to natural persons. Therefore, legal persons have no protection and no possibility to successfully address the competent authority.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

There are more detailed rules in respect of sending commercial communications via electronic mail. In this respect, Article 12 (3) of Law 506/2004 provides that ‘in all cases, it is prohibited to send commercial communications by electronic mail where the actual identity of the person on behalf of whom they are sent is hidden, in violation of art. 5 of Law no. 365/2002, republished, or which does not specify a valid address to which the recipient may send its request to cease such conduct or communications which encourages recipients to visit websites that contravene art. 5 of Law no. 365/2002, republished.’

Article 5 of Law no. 365/2002 includes a detailed list of information to be made available to recipients or public authorities and mentions that service providers must allow easy, direct, permanent and free of charge access to such information.

At the same time, Article 6 of Law 365/2002 mentions that:
(1) Sending commercial communications by electronic mail is prohibited, unless the recipient has given his prior explicit consent to receive such communications.
(2) Commercial communications constituting an information society service, or part thereof, in so far as they are permitted, you must meet the following conditions:
   a) must be clearly identifiable as such;
   b) the natural or legal person on whose behalf they are sent must be clearly identified;
   c) promotional offers, such as discounts, prizes and gifts must be clearly identified and the conditions for obtaining them must be easily accessible and clearly presented;
   d) promotional competitions or games must be clearly identifiable as such, and the conditions for participation shall be easily accessible and clearly presented;
   e) any other conditions imposed by the laws in force.
(3) Commercial communications constituting an information society service, or part thereof where the service is provided by a member of a regulated profession is permitted subject to compliance with the laws and regulations governing that profession, in relation to the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of that profession.
(4) Information society service providers performing commercial communications are required to comply with par. (1) - (3).’

Additionally, Chapter II of Decision no. 1308 of 20 November 2002 approving the methodological norms for the application of Law 365/2002 on electronic communications contains much more detailed provisions regarding consent and the way of sending commercial communications, for example by including the word ‘publicity’ in capital letters at the beginning of the subject of the e-mail.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Since the directive has been exactly transposed, there are no other exceptions rather than the ones included in the directive itself when the natural or legal person who, in compliance with Law 677/2001, has directly obtained the client’s e-mail address in the context of a sale of a product or service. He/she can use that e-mail address for sending commercial communications referring to its own similar products or services, under the condition that the clients are clearly and distinctively given the opportunity to object, free of charge and in an easy manner at the time of collection of the e-mail address and with the occasion of each message in case the customer has not initially refused such use.

The provisions of Article 12 of Law 506/2004 are applied to both natural and legal persons.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

There is no other distinction between the communication channels used, other than the one already mentioned in respect of electronic mail. As long as the communications (be it e-mail, fax, banners, instant messages, newsfeeds etc) do not require the intervention of a human operator, they all fall under the same provisions. As Article 2 (1) (g) of Law 506/2004 states, electronic mail is defined as ‘the service consisting of the transmission, through a public electronic communications network, of text messages, voice, sound or image that can be stored in the network or in the recipient’s terminal equipment until receipt by the addressee.'
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. There is no particular guidance offered by enforcement authorities, however in its annual activity reports, ANSPDCP (the national Data Protection Authority) describes specific cases regarding unsolicited communications. The reports also mention that the complaints and investigations regarding unsolicited communications increases in number yearly and that they are the most common types of complaints received from individuals. Unsolicited communications are usually sent by e-mail or by SMS.

   The annual activity reports usually mention investigations where it has been found that the data processor did not obtain prior explicit consent for sending commercial communications. As an additional example, in one case, the authority obliged the data processor to modify the text of the e-mail sent with the commercial communication in order to make reference to Law no. 506/2004 and not to legislation inapplicable in Romania, such as the US CAN SPAM ACT 2003.

   At the same time, IAB Romania issued standards for e-mail marketing.

   b. Certain cases related to unsolicited communications can be observed from the national Data Protection Authority annual activity reports. However, these cases refer to the fact that data processors usually contest the sanctions applied by the authority. Nevertheless, for example in the activity report for year 2008, the authority observes that courts have adopted a unitary practice in dealing with personal data protection cases.

---

3 The standards are freely available for download here: http://iab-romania.ro/standarde-iab/standarde-email-marketing/
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

In practice, on one hand side there is widespread noncompliance with the provisions regarding commercial communications and on the other side, although the number of complaints is increasing, there is still little awareness and understanding of these rules both by regular citizens as well as companies.

Additionally, an inconsistency is the fact that Article 12 (1) of Law 506/2004 mentions that unsolicited communications sent, among others, by using automated calling and communications systems that do not require the intervention of a human operator are forbidden. Per a contrario, unsolicited communications send by using automated calling and communications systems that do require the intervention of a human operator are allowed. However, under Law 677/2001 this type of unsolicited communications, which require the intervention of a human operator, would still need explicit consent or other legal basis provided by the law for processing data as well as the possibility to opt out at any time.

There are many companies sending commercial communications without prior explicit consent and without offering opt-out mechanisms along with each commercial communication sent. We again stress that, even if prior explicit consent is obtained, the provisions of Article 4 of Law 677/2001 are still applicable. Therefore, among other requirements, personal data can be collected only for determined, explicit and legitimate purposes.
Part 3: Interview Report

Interviews focused primarily on issues that were not covered by the desk research.

Interview I

<table>
<thead>
<tr>
<th>Author of the interview report:</th>
<th>Valentina Pavel Burloiu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the authority (original language + translation into English):</td>
<td>Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)</td>
</tr>
<tr>
<td></td>
<td>The National Supervisory Authority for Personal Data Processing</td>
</tr>
<tr>
<td>Name(s) of person(s) interviewed + official position(s):</td>
<td>Head of the Legal and Communication Department, Head of the International Relations Department (plus one representative), Head of the Complaints Department, Head of the Control Department and Head of Notification Department</td>
</tr>
<tr>
<td>Date of the interview:</td>
<td>28.09.2014</td>
</tr>
<tr>
<td>Location of the interview:</td>
<td>ANSPDCP office</td>
</tr>
</tbody>
</table>

Once Law 506/2004 was adopted, the ANSPDCP’s responsibilities expanded from overseeing the application of Law 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, to include personal data processing in the electronic communications sector as well. Regrettably, there has not been an increase of resources (either financial or in terms of staff) in order to have full capabilities to handle the new responsibilities.

It was noted that the only known court cases deal with operators contesting the Data Protection Authority’s decision to apply a fine. As it was observed, so far the courts have fully sustained the Data Protection Authority decisions.

The ANSPDCP annually issues reports that include factsheets with cases, findings from inspections and recommendations for improving the legal framework. It needs to be noted that there is an increase in the number of complaints, especially in respect of unsolicited communications that are usually sent via e-mail and SMS. All reports are available here (in Romanian): [http://dataprotection.ro/?page=Rapoarte%20anuale&lang=ro](http://dataprotection.ro/?page=Rapoarte%20anuale&lang=ro)

In respect of the definitions implemented in the Romanian legislation, it has been highlighted that there is no contradiction between the definitions of operator and provider, since an operator can also be an electronic communications provider and vice versa. Therefore, it will be held responsible in compliance with the respective applicable law.

Moreover, although the Romanian data protection legislation did not implement a definition of consent, in its analysis, the ANSPDCP always refers to the definition of consent in Directive 95/46/EC.
An important element of controversy is that, despite the clear provisions of Article 12 of Law 506/2004, the ANSPDCP does not handle complaints on unsolicited communications that are addressed by legal persons. The ANSPDCP’s motivation for rejecting these complaints as inadmissible is that the Romanian Constitution recognises the right to privacy of natural persons and not of legal persons.

Below are a number of statistical data we requested from the Authority:

1. number of security breach notifications from 2012 until present: 1.

The notification was reported to ANSPDCP the next day and no sanctions have been applied.

2. number of providers who proved that they apply adequate protection measures in order to be exempt from notification: not applicable

Article 3 (8) of Law 504/2006 states that: ‘The notification in paragraph (7) is not necessary if the provider demonstrated to ANSPDCP, in a way which ANSPDCP considers satisfactory, that it applied adequate technological measures for protection and that these respective measures were applied to the data affected by the security breach. These technological measures for protection need to assure the fact that the data becomes unintelligible to persons which are not authorized to access them.’

3. number of investigations performed by ANSPDCP in light of Article 3 (9) of Law 506/2004: not applicable

Article 3 (9) of Law 504/2006 states that: ‘Without prejudice to the provider’s obligation to notify subscribers or users, when the provider did not already notify the personal data security breach to the respective subscriber or user, ANSPDCP can, after analysing the possible negative effects of the breach, to request the provider to do this notify.’

4. number of requests made by ANSPDCP in respect of the internal procedures established by providers for replying to users’ requests in light of Article 3 (1) of Law 504/2004: not applicable

Article 3 of Law 506/2004 states that:

‘(1) The provider of a publicly available electronic communication service is obliged to take adequate technical and organizational measures in order to ensure the security of the personal data processing. If necessary, the provider of a publicly available electronic communication service will take these measures together with the publicly available electronic communications network provider.

(4) ANSPDCP can audit the measures taken by providers in light of paragraph (1) and can issue recommendations and best practices in respect to the security level which needs to be reached by those measures.’
5. number of complaints and/or inspections in light of Article 4 (confidentiality of communications): in 2014 there have been 3 complaints and 2 investigations

6. number of complaints and/or inspections in light of Article 5 (traffic data): not applicable

7. number of complaints and/or inspections in light of Article 8 (location data, other than traffic data): not applicable

8. number of complaints and/or inspections in light of Article 12 (unsolicited communications): in 2014 there has been one ex oficio investigation, 87 complaints and 20 investigations for solving the complaints (until 31.07.2014)

All relevant information discussed or referenced to during the interview has been integrated in the questionnaire.
When it comes to ANCOM’s competence, it has been highlighted that the Authority has a single task in respect of personal data processing in the electronic communications sector, which is to verify the conditions for issuing invoices. This competence is established under the provisions of Article 6 of Law 506/2004 (detailed billing).

As it was shown in the questionnaire above, although ANSPDCP is declining in competence, ANCOM did not take over responsibilities related to unsolicited communication complaints addressed by legal persons. Furthermore, since the Minister for Information Society has taken over the supervision and control of applying Law 365/2002 on electronic commerce, we could expect that the responsibility of dealing with complaints related to unsolicited communication and which are addressed by legal persons could fall under the Ministry’s competence.

At the same time, it has been underlined that Chapter IV of EGO 111/2011, the Security and integrity of electronic communications networks and services, contains all the provisions regarding the technical and organizational measures for mitigating the risks which could impact the security of networks and services. Publicly available electronic communications network or service providers need to be in compliance with these measures. These measures are meant to ensure the security of personal data processing at the same time.

In terms of concrete measures that have been adopted by ANCOM on the security and integrity of electronic communications networks and services, the latest document issued by the Authority is Decision no. 512/2013 establishing minimum safety measures to be adopted by providers of publicly available electronic communications networks or services. In light of the same decision, providers also need to report incidents of significant impact on the electronic communications networks and services. This decision covers the technical and organizational measures which need to be adopted.
by publicly available electronic communications networks and services for assuring an adequate level of security and integrity of networks and services. It also contains the circumstances, format and procedures applicable to the notification of the security breach or integrity loss that has a significant impact on providing electronic communications networks and services.

At the same time, it was noted that, while ANCOM and ANSPDCP cooperate and exchange views on issues regarding personal data processing in the electronic communications sector, the only official cooperation document regarding Law 506/2004 relates to activities connected to creating and making the subscriber’s registry and the service information about subscribers publicly available. The document is available (in Romanian) at: http://www.ancom.org.ro//uploads/files/9968/precizari_ANSPDCP+ANC_SIA.pdf.

Furthermore, ANCOM has not identified any issues regarding the practical applicability of the definitions of operator and provider under Law 506/2004. Besides the Emergency Government Ordinance no. 111/2011, ANCOM’s Decision nr. 987/2012 on the general authorization regime for providing electronic communications networks and services (available here in Romanian) is also taken into consideration.

In respect of VoIP services, ANCOM sees them as electronic communications services since they fall within the definition provided in Article 4 (1) of Emergency Government Ordinance no. 111/2011 on electronic communications, namely "public telephone service - a public service which allows initiating and receiving, directly or indirectly, of national or national and international calls by using a number or several numbers from the national or international numbering plan".

On the other hand, ANCOM interprets that web-mail services and geo location services are content related services and not electronic communications services, to the extent that the actual transmission of information itself is performed by providers of data transmission and Internet access.

There are no known court cases and there are no recorded incidents of security breaches where a resident of a different country has been affected. More information (in English) on security issues can be found here: http://www.ancom.org.ro/en/rapoarte-si-studii-privind-securitatea-si-integritatea-retelelor-si-serviciilor-de-comunicatii-electronice-4958.
COUNTRY REPORT

SWEDEN

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Christine Kirchberger & Pam Storr

Date: 26 August 2014
Contents

Part 1: Management summary ........................................................................................................3
Part 2: Answers to the questionnaire .............................................................................................4
Part 1: Management summary

Management Summary for Sweden
The transposition of the ePrivacy Directive into Swedish law can be summarised as follows:

- The provisions with regard to the scope of the Directive have been transposed into the Electronic Communications Act as the complete 2002 EU Regulatory Framework for electronic communications was transposed into one national act. The framework is seen as one framework, which is why ePrivacy questions were regulated in the same act. In some cases this leads to legal questions on ePrivacy overlapping with general privacy questions. As Sweden has assigned the Swedish Data Inspection Board (Datainspektionen) with the supervision of data protection and privacy question, and the Swedish Post and Telecom Authority (Post- och telestyrelsen - PTS) with the supervision of ePrivacy questions, these overlapping questions have to be solved through cooperation by the authorities, which is working out well, however.

- Sweden transposed most of the provisions in the Electronic Communications Act. The Act applies to electronic communication networks and services and their operators. A model created by PTS stipulates several factors in order to determine if an entity falls under the definition of networks and/or services. While the application of the Act does not seem to lead to any problems in practice, the question of its applicability to foreign entities seems not completely clear from a legislative point of view.

- Art. 5.3 of the Directive (about “cookies” etc.) has been more or less literally transposed into Swedish law. The wording as such leads to several questions on its interpretation (e.g. fingerprint access technologies on mobile devices), though this has not been an issue in practice. The main focus in Sweden at the moment is to ensure compliance by regular websites, which is why PTS has initiated an investigation into the matter which hopefully leads to clarified rules on different types of cookies, the responsibility in case of third party cookies and how consent can be ensured by website owners.

- Sweden has transposed the rules on traffic and location data according to the wording of the ePrivacy Directive. Whether or not the rules are applied correctly in practice is yet to be seen, and an investigation of operators by the supervisory authority as to the processing, storage and deletion of such data has been put on hold. This delay is due to the developments at both the European and national level following the CJEU’s judgment in spring 2014 on the status of the Data Retention Directive.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications (Art 13) were transposed into Section 19 of the Swedish Marketing Act (Marknadsföringslag (2008:486)). The previous provision in the eCommerce Directive was never transposed, as an opt-out solution did not require any legislative measures according to the government bill. The application of Section 19 is supervised by the Swedish Consumer Agency (Konsumentverket) which is responsible for the Swedish Marketing Act in general. Sweden has had a long tradition of industry standards concerning direct marketing, starting from a blacklist for direct advertisement via phones and now including ethical rules on all types of direct marketing including e-mail and interactive technologies. In other words, Section 19 completes the ethical rules from a legislative point of view.
Part 2: Answers to the questionnaire
A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Sweden transposed the ePrivacy Directive, together with the other Directives concerning the regulatory framework for electronic communications into Swedish national law in 2003 by enacting the Electronic Communications Act (Lag (2003:389) om elektronisk kommunikation). The 2009 amendments¹ to the Directive were implemented into Swedish law in 2011 by amending the Electronic Communications Act.

Article 7 Electronic Commerce Directive, dealing with unsolicited commercial communication, was not directly transposed by the Swedish Electronic Commerce Act in 2002 (Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster) though this Act transposed the main provisions of the Electronic Commerce Directive. The main reason for not introducing a specific provision was the opinion that an opt-out solution did not require any specific legislative measures. However, when transposing the ePrivacy Directive, Sweden introduced an opt-in solution into national law, which was done with the old Marketing Act (Marknadsföringslag (1995:450)), and was transferred into the current Marketing Act (Marknadsföringslag (2008:486)) in Section 19.

**Concordance table**

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 3 (Scope)</td>
<td>Electronic Communications Act (Lag (2003:389) om elektronisk)</td>
<td>In Swedish at <a href="http://www.riksdagen.se/sv/Dokument">http://www.riksdagen.se/sv/Dokument</a></td>
</tr>
</tbody>
</table>

| Art. 5.2 (Business exception) | Not transposed |

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions
transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
   a. the full name in your national language
   b. the English translation of the short name
   c. the part or the provision(s) of the ePrivacy Directive it supervises
   d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post- och telestyrelsen (PTS)</td>
<td>Swedish Post and Telecom Authority</td>
<td>Electronic Communications Act</td>
<td><a href="http://www.pts.se">www.pts.se</a></td>
</tr>
<tr>
<td>Konsumentverket</td>
<td>Swedish Consumer Agency</td>
<td>Provisions with regard to unsolicited communications</td>
<td><a href="http://www.konsumentverket.se">www.konsumentverket.se</a></td>
</tr>
<tr>
<td>Datainspektionen</td>
<td>Swedish Data Inspection Board</td>
<td>Personal Data Act (no direct supervision of ePrivacy issues)</td>
<td>datainspektionen.se</td>
</tr>
</tbody>
</table>

The Swedish Post and Telecom Authority (Post- och telestyrelsen - PTS) is the authority that generally supervises electronic communications network and service providers. In this capacity ePrivacy questions are also included. As the provision on cookies is included in the Electronic Communications Act, PTS is also the supervisory authority in this regard.

The provisions on unsolicited commercial communications are regulated in the Swedish Marketing Act and therefore fall under the supervision of the Swedish Consumer Agency.

The Swedish Data Inspection Board is the general supervisory authority for privacy and data protection in Sweden and some ePrivacy questions are related to general privacy questions, which is why the Data Inspection Board and PTS have an ongoing cooperation in these questions.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

Chapter 1 Section 7 Electronic Communications Act contains definitions for networks, services and providers. The provision defines **electronic communication networks** (elektroniskt kommunikationsnät) as ‘transmission systems and, where applicable, switching or routing equipment as well as network elements, which are not active, and other resources which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, irrespective of the type of information conveyed.’ The definition contains, in other words, parts of the exact same wording as the definition in Article 2 Directive 2002/21. According to the Government Bill (Prop 2002/03:110) the scope is the same as the Directive.

Services (**elektronisk kommunikationstjänst**) are also defined in Chapter 1 Section 7, as ‘a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks.’ Also this definition is a literal shorter version of the wording in Directive 2002/21.

PTS, the supervisory authority has clarified the terms network and service in guidelines published in 2009\(^2\). Instead of purely stating examples of networks and services, PTS created a model for deciding if a service falls under the Electronic Communications Act. The model builds on three requirements for an electronic communications service to fall under the Act:

- the service is provided to another (external) party, on commercial grounds, and
- the service mainly comprises the transmission of signals, and
- the service provider has the power to control the transmission,

Chapter 1 Section 7 Electronic Communications Act also defines providers (**operatör**). A provider is somebody who owns or in any other way controls a public communications network or associated facilities.

---

4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

As the Electronic Communications Act is rather abstract when describing its application area, PTS issued guidelines to define services more in detail (see previous question). One important factor is the question if the ‘service mainly comprises the transmission of signals’. In some cases of pure storage services such as web hotels no transmission takes place; the same applies to pure content services, which fall outside the Act too.

The word ‘mainly’ means that internet service providers who also offer e-mail services fall within the definition, but not pure e-mail providers (see next paragraph).

The other important factor is, if ‘the service provider has the power to control the transmission’. In other words, if the service provider relies on another communication service for its own service to work, it would not fall within the definition and therefore the Electronic Communications Act would not apply to it. Often, the one who also issues IP addresses or other types of identities, such as phone numbers to the end user, is also considered having the power to control the transmission.

PTS has issued decisions against Skype Communications with regards to notification requirements for their services SkypeIn, SkypeOut, and Skype To Go, so certain VoIP services are included in the application of the Electronic Communications Act, depending on the type of VoIP service.

The question of location based services was not discussed in the preparatory works leading to the implementation of the Electronic Communications Act. PTS mentions, though, the challenges with location based services in connection with mobile communications in a few reports.

In 2010, PTS investigated in cooperation with the Swedish Data Inspection Board the processing of traffic data in mobile content services. The impression from the report is that pure content services that are not part of the communication as such fall within the Swedish Personal Data Act and not necessarily with the Swedish Electronic Communications Act. This interpretation would also be in line with PTS’ 2009 guidelines that require ‘control of the transmission’ in order for the Electronic Communications Act to apply. The 2010 report also distinguishes between content services that are offered by a company acting on assignment by the communications provider and content services by independent companies. In the former case the Electronic Communications Act would be applicable to all processing of personal data (including the one done by the content provider), in the latter case the Electronic Communications Act would only be applicable to the transfer of personal data.

---

4 Decision by Swedish Post and Telecom Agency (PTS) of 2 Jul. 2009, no. 06-14224. See also PTS Report PTS-ER-2009:12 on provision of services and networks that require notification.
data from the communications provider to the content provider. For the personal data processed by the content provider the Personal Data Act would be applicable. So, purely content services such as webmail would not fall within the scope.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

Interestingly enough, unlike the Swedish Personal Data Act (Personuppgiftslag (1998:204)), that specifically applies to controllers who are established in Sweden or who use equipment that is situated in Sweden (Section 4), the Electronic Communications Act does not mention any territorial scope in its wording.

Despite this lack of territorial scope in the actual law, in practice PTS uses its supervisory competencies for companies that operate in Sweden, though they may be established outside of Sweden. There have not been any decisions with regards to ePrivacy where Swedish law was applied to foreign operators, but Sweden does not differentiate between applying the ePrivacy parts of the Electronic Communications Act and the regular communications rules (authorization, etc). In other words, if an operator falls within the general provisions of the Act, it will also fall within its privacy provisions. The question to what extent foreign operators fall within the Act has not been tested in court, however.

With regards to commercial communications, the Swedish Consumer Agency seems to cooperate on an EU and international level to the extent possible and has issued decisions against foreign entities.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. As stated, PTS, the supervisory authority, published guidelines in 2009 clarifying the terms network and service.\(^7\) In these guidelines, PTS created a model for deciding if a network or service falls under the Electronic Communications Act. The model builds on several requirements for an electronic communications network or service and was complemented by a flow chart in order to help determine which operators fall within the Act.

   b. No case law is available regarding the definitions or scope.

---

7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

<table>
<thead>
<tr>
<th>a. One legal challenge in my personal opinion is to what extent foreign entities fall under the scope of the Electronic Communications Act.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Another challenge concerns operators that only provide certain services, without any transmission of signals. In this case the Electronic Communications Act will not apply and the service will be regarded an information society service in accordance with the eCommerce Directive.</td>
</tr>
<tr>
<td>b. A possible improvement from an EU perspective could be to clarify which national legal framework applies to an operator established in one member state, but offering services in several other member states.</td>
</tr>
<tr>
<td>Another possible improvement is to be clearer as to what extent electronic communication services and information society services overlap or are different. The question here is what the deciding factor is for distinguishing between them and if this should be a technological factor or something related to the purpose of the service.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

Chapter 6 Section 20 Electronic Communications Act transposes Article 5 ePrivacy Directive and stipulates the principle of confidentiality of communications. The principle does not apply to the subscribers themselves or any other party taking part in the message.

Confidentiality (tystnadsplikt) applies to:
- information about a subscription (name and address of the subscriber, telephone number, IP-number);
- the content of an electronic message; or
- any other data concerning a particular electronic message (traffic and location data, such as telephone number/IP address of the sender and receiver, the date and time of a communication, the identification number of the terminal equipment (IMEI-number)).

Confidentiality applies to providers of electronic communications networks or services and means that the information must not be shared or used where unauthorised. Though authorised is not defined, it seems to cover releasing of information according to Chapter 6 Sections 22 or 23 (dealt with below), as well as with the consent of the subscriber.

Chapter 6 Section 1 defines ‘communication’ in accordance with the Directive, but uses the term ‘electronic message’ instead in order to avoid confusion with electronic communication. According to the Government Bill the definition only applies to Chapter 6 of the Act. An electronic message is defined as ‘all information that is exchanged or transmitted between a limited number of parties via a public electronic communications network, except information that is transmitted as part of a radio or TV broadcast that is aimed at the public via an electronic communications network if this information cannot be linked to an individual subscriber or user.’

Chapter 6 Section 17 Electronic Communications Act prohibits wiretapping in general and stipulates that anybody other than the user may not access or in any other way process information in an electronic message without the consent of the user. This provision not only applies to network operators but to any third party who accesses electronic messages.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

---

12

---

8 Prop 2002/03:110 Lag om elektronisk kommunikation, m.m., at 389.
When transposing the ePrivacy Directive, the Swedish government did not see a need to transpose the exception in Article 5.2.\(^9\) In general, the principle of confidentiality does not prohibit someone from recording or saving a message to which he or she is a party. The exception in Article 5.2 does not refer to this type of situation; therefore the exception would go further than the original purpose of Article 5.1, according to the government bill. As no specific need for such an exception could be proven, Article 5.2 was not transposed into Swedish law.

\(^9\) See Government Bill (Prop. 2002/03:110), at 255.
### Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Chapter 6 Section 22 stipulates several exceptions to the confidentiality principle of Chapter 6 Section 20 Electronic Communications Act. According to Chapter 6 Section 22 network or service operators shall upon request release information regarding a subscription (1), about the content of an electronic message (2) or traffic and/or location data (3):

1. information about a subscription to public authorities if the information is needed for service (delivery) of people if there is reason to believe that they are avoiding service;
2. information about a subscription to public prosecutors, police authorities, Swedish Security Service (Säkerhetspolisen) or other crime fighting authorities if the information concerns suspected crimes;
3. information about a subscription and traffic/location data to police authorities if the information is needed to trace people that have disappeared in such a manner that may indicate a risk for their life or health;
4. information about a subscription to the Swedish Enforcement Authority (Kronofogden) if the information is essential for the public authority in their enforcement activity;
5. information about a subscription to the Tax Authority (Skatteverket) if the information is essential for a matter of tax control or to check the correct place of residence in the civil registration database;
6. information about a subscription to police authorities if the information is needed for investigations or identification in case of accidents or deaths, or for a task according to Section 12 Police Act (polislagen (1984:387)) (concerning people under 18 years who can be taken into custody in order to protect their health);
7. information about a subscription to police authorities or public prosecutors if the information is needed in order to inform a young person’s (under 15) guardian according to Section 33 Act with special provisions for young offenders (lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare)
8. information about a subscription and traffic/location data to regional emergency control centers (alarmeringscentral) that fall under the Act on Activities of Certain Regional Emergency Control Centers (lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler).

One exception that seems rather unique for Sweden and which can be explained by the historic Swedish perception that the “air is free” is Chapter 6 Section 23. According to the provision one is allowed to listen to radio transmitted messages, also to ones that are not aimed at her or him. It is however, prohibited to share these messages unless one is authorised to do so.
4. a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Whether the interception of MAC addresses would entail breach of confidentiality;</td>
</tr>
<tr>
<td>2</td>
<td>Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;</td>
</tr>
<tr>
<td>3</td>
<td>Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?</td>
</tr>
</tbody>
</table>

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. Swedish law does not explicitly mention automated breaches, but Chapter 6 Section 17 Electronic Communications Act stipulates that nobody except the user involved is allowed to access or otherwise process information in an electronic message. The wording ‘nobody’ might lead to the conclusion that a natural person has to be involved at some stage. Read in connection with the liability provision in the Electronic Communications Act (Chapter 7 Section 15 para 2), criminal liability requires intent or negligence and entails fines, not imprisonment. In other words, a person has to be behind the breach, and have acted with intent or negligence, but it does not matter which technology is employed.

The principle of confidentiality in Chapter 6 Section 20 lists different types of information and the exceptions from the principle vary depending on the type of information. The types listed are:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>information about a subscription (name and address of the subscriber, telephone number, IP-number);</td>
</tr>
<tr>
<td>2</td>
<td>the content of an electronic message;</td>
</tr>
<tr>
<td>3</td>
<td>any other data concerning a particular electronic message (traffic and location data, such as telephone number/IP address of the sender and receiver, the date and time of a communication, the identification number of the terminal equipment (IMEI-number));</td>
</tr>
</tbody>
</table>

None of the exceptions to the principle of confidentiality in Chapter 6 Section 22 apply to the content of the message. In other words, the Electronic Communications Act does not allow any sharing of the content of messages (in this case traditional procedural rules apply with regards to wiretapping by crime fighting authorities). Information about a subscription has to be shared in all exceptions, while traffic data only has to be shared with police authorities in order to find missing people who are in danger, or with regional emergency control centres.

b. Already before the ePrivacy Directive, the Swedish Criminal Code protected postal and telecommunication secrecy. Chapter 4 Section 8 Swedish Penal Code (Brottsbalk (1962:700)) protects the content of a message and stipulates criminal liability for breach of postal or telecommunication secrecy. Chapter 4 section 9c Penal Code furthermore covers breach of data secrecy (dataintrång).
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

<table>
<thead>
<tr>
<th>a.</th>
<th>Chapter 6 Section 18 Electronic Communications Act deals explicitly with cookies and transposes Article 5.3 of the Directive. Electronic communication networks may be used to store or gain access to information stored in the terminal equipment of a subscriber or user only if the subscriber or user is provided with information about the purpose of the processing and has consented to the processing by the data controller.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>The 2009 amendment to the Directive was implemented into the Swedish Electronic Communications Act in 2011 and exchanged the earlier ‘right to refuse’ with the requirement of consent. The requirement has, however, not been interpreted in a clear manner in practice.</td>
</tr>
<tr>
<td></td>
<td>The supervisory authority, PTS, is looking into legal compliance at the moment and is investigating a sample of websites that were chosen in order to cover a spectrum that can be of guidance for many others. The websites include news sites, authorities, banks and social media sites. PTS might also issue clearer guidelines on the requirements of consent in the next year.</td>
</tr>
<tr>
<td></td>
<td>The information and consent requirement does not apply in the event that the storage or access are necessary in order to carry out the transmission of an electronic message over an electronic communication network, or is otherwise required to provide a service explicitly requested by the subscriber or user. For example, if the user wishes to access a banking service that requires cookies to be stored or accessed on the user’s computer, the data controller is allowed to employ cookies in the technical process. Caching necessary for a transmission for technical reasons is also permitted according to Chapter 6 Section 18 Electronic Communications Act.</td>
</tr>
<tr>
<td></td>
<td>b. The provision in the Electronic Communications Act is very abstract and does not mention the word cookie in general. As a consequence, it does not distinguish between different types of cookies either. PTS has published some general information on its website with regards to the use of cookies. The information mentions third party cookies and also describes Flash cookies, although more from a technical perspective. In both cases Chapter 6 Section 18 is applicable, however.</td>
</tr>
</tbody>
</table>

---

10 See some information in Swedish at www.pts.se/sv/Bransch/Internet/Integritet/Regler-och-tillsyn/.
11 In Swedish at www.pts.se/sv/Bransch/Regler/Lagar/Lag-om-elektronisk-kommunikation/Cookies-kakor/Fragor-och-svar-om-kakor-for-webbplatsinnehavare/
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

PTS has published some general information on a dedicated page on its website about cookies. The supervisory authority does not, however, prescribe any particular way to ensure consent or how the information needs to be provided. PTS does not mention mobile devices nor does it distinguish between different types of cookies with regards to consent. Due to the current investigation, more detailed guidelines might be expected in the next year.

In addition, PTS is looking into how consent in general is ensured within electronic communications. This would have implications for the consent requirements with regards to cookies.

In addition to the supervisory authority, there is an attempt by an industry organization to clarify the rules on cookies. The Swedish Interactive Advertising Bureau (IAB Sweden), together with some other industry organizations has produced a Recommendation for the use of cookies by market players. IAB’s recommendation builds upon the OBA-Framework (Online Behavioural Advertising) by IAB Europe. With regards to consent, the Recommendation states that certain browser settings can be regarded as consent by the user. It seems doubtful if this interpretation can hold on the long run, now that PTS is looking into the requirements more in detail.

---

13 [iabsverige.se](http://iabsverige.se)
14 More information at [www.minacookies.se](http://www.minacookies.se) and [iabsverige.se/standards-och-guidelines/oba-framework/](http://iabsverige.se/standards-och-guidelines/oba-framework/)
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

According to Chapter 6 Section 18 Electronic Communications Act, the information and consent requirement does not apply in the event the storage or access are necessary in order to carry out the transmission of an electronic message over an electronic communication network or is otherwise required to provide an information society service explicitly requested by the subscriber or user. The wording ‘or facilitate’ the transmission was deleted in the 2011 amendment of the section, thereby restricting the allowed use of cookies to cases where cookies are necessary for the transmission and not where they simply facilitate the transmission.

For example, if the user wishes to access a banking service that requires cookies to be stored or accessed on the user’s computer, the data controller is allowed to employ cookies in the technical process. Caching necessary for a transmission for technical reasons is also permitted according to Chapter 6 Section 18.

Neither the Act nor the information by PTS differentiates between different types of cookies in this regard.
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

Though PTS is currently investigating compliance with a selected number of websites, our personal view is that compliance is not very strong at this point. One major challenge is that many website owners use platforms (Wordpress, etc) or content management systems that automatically set up the technical framework for them. In this case many are unaware that they are using cookies on their own websites. An excellent initiative in this regard is PTS’ e-service ‘Find cookies’.  

There are no statistics available on compliance or the users’ view. PTS’ investigation also only focuses on a selected few websites.

15 e-tjanster.pts.se/internet/kakor/
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law

a. At the moment, PTS only has published general information on its website, though it is very detailed and aimed at website owners or operators.\textsuperscript{16} The guidance explains cookies from a technical perspective (including an explanation of flash cookies), their use and risks. The guidance then answers questions such as:

- What does the law say? (The Swedish Electronic Communications Act requires information and consent)
- What is the purpose of the regulation?
- Do I have to change the website of my organisation/company in order to fulfil the legal requirements? (It is not forbidden to use cookies, but you have to inform your visitors and ensure their consent.)
- How do I phrase the required information on my website? (A user has to receive information that the website uses cookies and for which purposes. The information provided should at least contain details about the names of the different cookies, which domain they belong to, which data is being stored in the cookies, how long they are stored, the purpose of the cookies and if the data from them will be shared with third parties.)
- How should users give their consent to the use of cookies? (As the website owner you are required to ensure consent. PTS does not want to state the exact technical solution but wants website owners to find the best technical solutions available).
- How do I find out which cookies are used on my website? (You can use PTS’s service hittakakor.pts.se.)
- Which questions should I ask the provider of my website? (1. Which cookies can be stored in the web browser of the visitor? 2. Are the cookies used to create user profiles? 3. How long are the cookies stored in the user’s computer?)
- Are there any alternatives to using cookies?
- Can the information be in English or does it have to be in all different languages? (As the legislation applies in Sweden, the information should be understandable by Swedes who cannot be expected to understand English.
- Do we have to conclude contracts with our visitors? (No, there are no formal requirements for consent.)
- Can a user save a webpage without any information being provided? (Yes, caching is one of the exemptions.)
- What are the rules when it comes to third party providers of cookies? (The website owner has the responsibility to provide information and ensure consent for all cookies that are used, including third party cookies.)

b. No case law on cookies is available.

\textsuperscript{16} \url{www.pts.se/sv/Bransch/Regler/Lagar/Lag-om-elektronisk-kommunikation/Cookies-kakor/Fragor-och-svar-om-kakor-for-anvandare/}
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

a. The general view as well as our personal view is that the wording of the cookie rule is very complicated and leads to many challenges regarding interpretation to begin with. The Swedish setup with PTS supervising communications operators and the Swedish Data Inspection Board (Datainspektionen) supervising organisations, authorities and companies with regards to privacy in general, does not facilitate this challenge.

In addition, the practical application has been hampered by the lack of knowledge of many website owners. Though they tend to comply as soon as being made aware of the legal issue, the figures for compliance will still be low for a long time, especially as not all users are aware of the rules either, so not many file complaints to the relevant authorities.

Furthermore, the legal view on different types of cookies, especially third party cookies is not very clear. Though third party cookies are included in the definition, it is not clear who would be responsible to inform and receive the consent of the user. Most probably the website owner, but they might not always be aware of third party cookies.

b. The question is if the provision on cookies is closer related to electronic communication or to digital information in general. Considering the growing amount of mobile applications that use techniques similar to cookies but that might fall outside the Electronic Communications Act as they do not ‘store or gain access to information already stored’, one possible improvement could be to move the provision from electronic communications to the general privacy regulation. In this case, the data protection rules would also apply to the complete process of storing, accessing, utilising, sharing, of personal data acquired through cookies. This would allow one legislative framework to cover all different steps of the personal data processing instead of focusing only on the first step of collecting the personal data.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 6 Section 1 paragraph 7 of the Electronic Communications Act defines traffic data as “information that is processed in order to transmit an electronic message in an electronic communications network or in order to bill this message.”</td>
</tr>
<tr>
<td>This definition agrees with the definition in Article 2(b) of the Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Chapter 6 of the Electronic Communications Act contains the Swedish legal framework with regard to the lawful processing of traffic data.

Chapter 6 Section 5 stipulates an obligation for providers of public communications networks and publicly available electronic communication services to erase or anonymise traffic data of end users or subscribers. This applies when the data is no longer needed for the transmission of an electronic communication. The section states that this obligation does not apply when the data is needed for billing, where prior consent has been given, or for the purposes of law enforcement. These exceptions are detailed below. This section as such reflects the wording of Article 6(1) of the Directive.

Chapter 6 Section 6 paragraph 1 states that processing for billing purposes or the payment of charges is permitted until payment has been made or until it is no longer possible for the user to object to the billing or charge.

Chapter 6 Section 6 paragraph 2 states that where the user has consented, processing for the marketing of electronic communications services or for the provision of other services where data is required is permitted, to the extent and for the time necessary for the service or marketing. Such consent can be withdrawn at any time.

Where data is processed in accordance with Section 6 paragraphs 1 or 2, the provider must inform the user of the type of traffic data that will be processed and for how long the data will be processed. This information must be provided before consent is obtained (Chapter 6 Section 6 paragraph 3). Here, the Swedish law goes further than the definition provided in the Directive, as prior consent must be obtained not only for marketing and other services (Chapter 6 Section 6 paragraph 2, which reflects Article 6(3) Directive) but also for billing and payment purposes (Chapter 6 Section 6 paragraph 1, which reflects Article 6(2) Directive).

According to Chapter 6 Section 7 the processing of traffic data in accordance with Sections 5 and 6 may be carried out by a person entrusted by the operator to be responsible for handling billing, traffic management, customer inquiries, marketing of electronic communications services or the provision of other services where the data is needed. The processing of data shall be limited to that necessary for the activity. “Fraud detection” was left out of the wording of this section, as it was deemed to fall within the exception for the prevention and detection of unauthorised use of an electronic communications network or service, referred to in Chapter 6 Section 8 paragraph 3 (detailed below).

Chapter 6 Section 8 states that Sections 5-7 do not apply:
1. where a government agency or a court needs access to such data in order to resolve disputes;
2. in relation to electronic messages that are the subject of secret wiretapping or secret surveillance, technical assistance for such interception or monitoring, data collection according to the Act on Retrieval of Data on Electronic Communication by Law Enforcement Agencies

(2012:278);

3. to the extent that data referred to in Section 5 is necessary to prevent and detect the unauthorised use of an electronic communications network or service.

The Act on Retrieval of Data on Electronic Communication by Law Enforcement Agencies (2012:278) mentioned above allows the police and customs to request traffic data, including location data, under certain circumstances with regards to their intelligence activities. However, any such request must be reported to a specific supervisory authority, the Swedish Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden)\(^{18}\).

Additional sections were added to the Electronic Communications Act following the transposition of the Directive 2006/24/EC (the Data Retention Directive). Obligations for operators to store traffic data for crime fighting purposes were added and were added as exceptions to the obligation in Chapter 6 Section 5 to erase or anonymise data; Chapter 6 Section 16a states that an operator is required to store data necessary to trace and identify:

- the communication source;
- the destination of the communication;
- the date, time and duration of the communication;
- the type of communication and communication equipment;
- the location of mobile communication equipment at the beginning and end of the communication.

The provisions are further specified by Sections 37–44 Ordinance on Electronic Communication (Förordning (2003:396) om elektronisk kommunikation). The obligation to store traffic data covers even data generated or processed from unsuccessful calls (Section 16a paragraph 2 Electronic Communications Act).

\(^{18}\) www.sakint.se.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Chapter 6 Section 5 Electronic Communications Act stipulates an obligation for network operators to erase or anonymise traffic data. This applies when the data is no longer needed for the transmission of an electronic communication.

Exceptions to this rule are stated explicitly in Section 5: this includes where data is processed for billing purposes, or where consent has been given (Chapter 6 Section 6) and where data is processed for law enforcement purposes (Chapter 6 Sections 16a and 16c).
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

PTS has issued a number of regulations relating to traffic data in recent years. These tend to deal with specific issues, such as:

- provisions for compensation to operators for costs related to the disclosure of stored data for law enforcement purposes;\(^{19}\)
- provisions and general guidelines on protective measures in relation to storage and other processing of data for law enforcement purposes;\(^{20}\)
- provisions for giving location data to emergency services.\(^{21}\)

More general information on traffic data rules can be found on PTS’ website.\(^{22}\)

PTS announced in November 2013 that it was to investigate the processing of traffic data and location data by operators; namely what traffic and location data is processed by operators, the duration and conditions of storage, how backups are handled, and how the data is deleted and destroyed.\(^{23}\) This work has, however, been put on hold following the developments in spring 2014 relating to the Data Retention Directive. PTS intends to continue this work at a later stage.\(^{24}\)

There is an ongoing case relating to Chapter 6 Section 16a (an operator’s obligation to store traffic data). PTS has notified an operator, Tele2, that it found reasons to believe that Tele2 was not complying with its obligations in relation to Chapter 6 Section 16a.\(^{25}\) Tele2 had, following the recent decision of the CJEU regarding the Data Retention Directive,\(^{26}\) decided to give precedence to Chapter 6 Sections 5 and 6 (the obligation to erase or anonymise traffic data) over Chapter 6 Section 16a (the storage of traffic and location data) and had announced that it would stop storing data. PTS ordered

---


\(^{22}\) www.pts.se/sv/Bransch/Internet/Integritet/Regler/#trafikuppgifter,

www.pts.se/sv/Bransch/Internet/Integritet/Regler/Lagring-av-uppgifter/

\(^{23}\) Mötensanteckningar, Integritetsforum 13 November 2013, PTS, p. 2,


\(^{24}\) Meeting with Staffan Lindmark, PTS, 25 August 2014.


\(^{26}\) C-293/12 and C-594/12.
Tele2 to continue to store traffic data in accordance with Chapter 6 of the Electronic Communications Act. Tele2 has followed this order, but has also appealed the decision to the Swedish courts.  


5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The provisions of Chapter 6 of the Electronic Communications Act are generally clear and consistent. They reflect the wording of the Directive regarding traffic data and the coverage is sufficiently wide, as operators who are providers of public communications networks or publicly available electronic communication services fall within the scope of the provisions (Chapter 2 Section 1 Electronic Communications Act).

It has yet to be seen in Sweden, however, whether the rules are sufficiently effective in practice and are being followed by operators. The PTS investigation on the processing of traffic data by operators (what data is processed, the duration and conditions of storage, how backups are handled, and how the data is deleted and destroyed) that was started in autumn 2013 has for the moment been put on hold. This type of investigation is essential to conclude whether the overriding deletion or anonymity principle is being put into practice effectively. The results of such an investigation would also allow the supervisory authority to issue any clarifications that may be needed for operators and lead to greater protection of privacy of such data.
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location data is defined in Chapter 1 Section 7 paragraph 8 Electronic Communications Act as “data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user.”</td>
</tr>
</tbody>
</table>

The difference from the definition provided in the Directive is that the type of user is not specified, whereas the Directive refers to a user of a publicly available communications service.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Chapter 6 of the Electronic Communications Act also contains the Swedish legal framework with regard to the lawful processing of location data.

Chapter 6 Section 9 Electronic Communications Act states that location data, other than traffic data, that relates to users who are natural persons or subscribers shall only be processed after being made anonymous or after the user or subscriber has given consent. Such processing is permitted only to the extent and for the duration necessary for the provision of the service.

Section 9 paragraph 2 further states that before consent is given, the service provider must provide information on:
1. the type of data that will be processed;
2. the purpose and duration of the processing;
3. whether the data will be given to third parties.

The user or subscriber has the right to withdraw consent at any time, following Section 9 paragraph 3.

Section 9 paragraph 4 states that even in case where consent has been given, a user or subscriber in a specific case shall have the possibility, in a way that is simple and free, to refuse the processing of data from the connection or transmission of an electronic message.

Chapter 6 Section 10 details who may process data in accordance with Section 9, namely only a person who acts on behalf of the provider of a public communications network or publicly available electronic communications service, or the provider of the service where the data is needed.

Chapter 6 Section 10a states that location data subject to decisions on data collection in Chapter 27 Code of Judicial Procedure and the Act on Retrieval of Data on Electronic Communication by Law Enforcement Agencies (2012:278) may be processed, notwithstanding Chapter 6 Sections 9 and 10.

As can be seen from the definitions above, Chapter 6 Sections 9 and 10 of the Electronic Communications Act reflect the wording of Article 9 of the Directive. The provision in Section 9 paragraph 2(3) explicitly covers third parties, requiring that the user is notified of any transfer of information to third parties, before consent to processing can be given.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

According to Chapter 6 Section 9 Electronic Communications Act location data other than traffic data relating to users who are natural persons or subscribers shall only be processed after being made anonymous (or after the user or subscriber has given consent). Such processing is permitted only to the extent and for the duration necessary for the provision of the service.

Otherwise the general rule in Chapter 6 Section 5 to erase or anonymise traffic data applies, see above.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. PTS issued a regulation relating to location data in 2011. This was within the area of emergency calls and included provisions for giving location data to emergency services. No other general guidelines regarding location data rules have been published. General information on location data rules is available on PTS’ website.

   b. We are not aware of any court cases or administrative procedures where location data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)

---

30 www.pts.se/sv/Bransch/Internet/Integritet/Regler/#lokaliseringsuppgifter
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| The provisions of Chapter 6 of the Electronic Communications Act relating to location data are generally clear and consistent, and they reflect the wording of the Directive regarding location data. Clarification in respect to the difference of location data that falls under traffic data and “location data other than traffic data” would lead to more logical rules and make the general obligation to erase data in Chapter 6 Section 5 more clear. |
| As for traffic data, it has yet to be seen in Sweden whether the rules are sufficiently effective in practice and are being followed by operators. The PTS investigation on the processing of location data by operators is therefore essential to conclude whether the overriding deletion or anonymity principle is being put into practice effectively. Any problems arising from such an investigation would again here allow the supervisory authority to issue any necessary clarifications for the protection of privacy. |
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation
b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

a. Article 7 Directive on Electronic Commerce, dealing with unsolicited commercial communication, was not explicitly transposed into the Swedish Electronic Commerce Act in 2002, mainly because an opt-out solution did not require any specific legislative measures.

However, in transposing the ePrivacy Directive, Sweden introduced an opt-in solution into national law, which was done in old Marketing Act (Marknadsföringslag (1995:450)), and was transferred into the current Marketing Act (Marknadsföringslag (2008:486)). The provision on unsolicited advertisement (Section 19 Marketing Act) also implements Article 10 Distance Contracts Directive into Swedish law.

Section 19 Marketing Act stipulates that an undertaking may only use email, telefax, automated calling systems or other similar automated systems that allow individual communication, and do not involve a natural person, in their marketing to natural persons, if prior consent has been given.

With regards to direct marketing in general and good marketing practices, the Swedish industry has employed initiatives for a long time; one of them being the Swedish Ethical Board for Direct Marketing (DM-nämnden - Etiska nämnden för direktmarknadsföring)\(^{31}\). Consumers and legal persons can report companies that do not follow the industry’s rules on ethical direct or interactive marketing (including fixed and mobile telephones, direct advertisement, search engines, e-mail or other personally addressed commercial communications.) In addition, with regards to phone marketing, the Swedish industry has managed a blacklist for phone marketing for many years. Consumers can (for free) register their phone number (mobile and fixed) in the blacklist (Nix-register)\(^{32}\) and avoid receiving phone calls regarding commercial advertisement.

b. With regards to the definition of “electronic mail”, the Directive talks about “messages” while the Swedish Marketing Act talks about “an addressed or otherwise individualised electronic message”. The rest of the definition is the same (“any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient”).

\(^{31}\) dm-namnden.org

\(^{32}\) nixtelefon.org
### 2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Section 19 Marketing Act stipulates that an undertaking may only use email, telefax, automated calling systems or other similar automated systems that allow individual communication, and do not involve a natural person, in their marketing to natural persons, if prior consent has been given.

The scope of the Swedish provision is the same as the Directive.

### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

According to Section 19 Swedish Marketing Act, the consumer’s consent is, however, not necessary if the company has acquired the contact details in the context of the sale of a product to that person and:

- the natural person has not refused that the electronic address is used for marketing purposes;
- the marketing concerns the undertaking’s own products; and
- the natural person clearly and distinctly is given the opportunity to object, free of charge and in an easy manner, to use the contact details for marketing purposes when they were collected, and on the occasion of each following message.

The Swedish Market Court decided on 18 June 2006 (MD 2006:18) that the possibility to object can be given by clicking a button on a website and also by unselecting an already checked box.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

The Swedish Marketing Act defines electronic mail as an electronic text, voice, sound or image message which is addressed or otherwise individualised and sent over a public communication network, and which can be stored in the network or in the recipient’s terminal equipment until the recipient collects it. (Section 3 Marketing Act in accordance with Art 2 ePrivacy Directive).

As this definition is rather broad, the term electronic mail also includes SMS, multimedia messages (MMS) and may include other types of messages that can be sent via instant message services such as Skype or ICQ. In addition, messages left on answering machines as well as communication within a network addressed directly to an IP-address can be considered email.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. The Swedish Consumer Agency (Konsumentverket) published some information about ‘spam’ on its website.\(^{33}\) It informs about the general rules and offers the possibility to report spam directly to the Agency (with some limitations regarding SMS and MMS messages). The Swedish Consumer Agency also offers practical guidance on how to avoid spam.\(^{34}\)

   b. In MD 2012:14 the Swedish Marketing Court applied Section 19 Swedish Marketing Act to an online game, where pop-up messages inside the game were considered electronic messages.

---

\(^{33}\) [www.konsumentverket.se/Vagledning--kontakt/Gor-en-anmalan/Anmal-via-webben/Spam/](www.konsumentverket.se/Vagledning--kontakt/Gor-en-anmalan/Anmal-via-webben/Spam/)

\(^{34}\) [www.konsumentverket.se/Lagar--regler/marknadsforing-och-reklam/Nej-till-reklam/Sa-kan-du-undvika-spam](www.konsumentverket.se/Lagar--regler/marknadsforing-och-reklam/Nej-till-reklam/Sa-kan-du-undvika-spam)
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The rules are rather clear and easy to interpret in practice. The challenge lies in the enforcement of the provision. Though the Swedish Consumer Agency facilitates the reporting of unsolicited commercial communications, the senders of spam are often foreign entities, often situated outside the EU. This makes enforcement actions by the Consumer Agency almost impossible.

So while the rules are rather clear, the challenge remains in the enforcement; which is why a technical solution could be more feasible, e.g. e-mail programmes with better spam filters, more information campaigns for the general public, so users do not open spam mails.

In 2008 a report by the Swedish Consumer Agency (referring to statistics by PTS) counted 177 consumer complaints about ‘marketing and spam’\(^\text{35}\). In a phone conversation with a lawyer from the Swedish Consumer Agency, it was mentioned that the number of complaints seems to be lower than a few years ago when awareness of spam might have been higher.

COUNTRY REPORT
SLOVAK REPUBLIC

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Tomáš Gábriš, Comenius University in Bratislava

Date: 22.08.2014
Contents

Part 1: Management summary ............................................................................................. 3
Part 2: Answers to the questionnaire .................................................................................. 4
Management Summary for Slovakia

The transposition of the ePrivacy Directive into Slovakian law can be summarized as follows:

- Transposition of the ePrivacy Directive 2002/58/EC into the law of the Slovak Republic can be found mostly in the Act on electronic communications no. 351/2011 Coll., as amended. It was partially transposed also to the Act on personal data protection no. 122/2013 Coll., the Act on electronic commerce no. 22/2004 Coll., and partially the Civil Procedure Code.

- In principle, the provisions of the Act are applicable to “operators”, i.e. in Slovakian terminology, “undertakings”. The Act does not deal with cross-border situations at all, with the exception of cross-border dispute resolution where Slovakian undertakings are involved. This might be considered a drawback. As far as the scope of the legislation is concerned, neither the Acts, nor any guidelines address the issues of VoIP and similar services, which might be considered a problem in the near future.

- The Act on electronic communications mostly regulates privacy protection with respect to “undertakings” ("operators"). Still, the processing of traffic and location data by network and service providers other than “undertakings” is also supervised by the E-Communications Office under the Act on e-communications, as well as unsolicited communications originating from other entities than undertakings. In addition, personal data may also seek protection under the general data protection legislation, where the Personal Data Protection Office is competent. The competence is hence split between the two Offices with respect to these issues.

- The Act on e-communications does not explicitly mention the exception of business practice; however, it regulates the possibility to record communication with the subscriber, user or undertaking instead, which might be considered equivalent to the wording of the business practice exception.

- With respect to cookies, there are no differences made between the types of cookies. There are neither specific rules nor recommendation on how to obtain the prior consent. The solution can currently be found in the wording of the Act on e-communications, which allows a tacit acceptance through the “use of a respective setting of the web browser or other computer programmes.” The majority of users hence ignores the warning and accepts the cookies automatically. Despite of that, no problems in this regard have been reported so far.

- The provisions of the ePrivacy Directive with regard to unsolicited direct marketing communications have been transposed into Sec. 62 (2, 3, 4) of the Act on electronic communications, Sec. 4(6) of the Act on electronic commerce and Sec. 3 of the Code of Civil Procedure. With respect to methods of direct marketing communication, in addition to the wording of the Directive, in the Slovakian Act on e-communications, short message services (SMS) are specifically mentioned, the consent has to be “provable”, and it can be revoked any time. Still, many types of spam (other than direct marketing communications, such as e.g. political advertising) do not fall under any statutory definition, since all definitions require that spam is a commercial communication. This issue falls within the competence of the E-Communications Office instead of Data Protection Office, being perceived as a potentially problematic split in competences.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

- Transposition of the ePrivacy Directive 2002/58/EC into the law of the Slovak Republic can be found mostly in the Act on electronic communications no. 351/2011 Coll., as amended. It was partially transposed also to the Act on personal data protection no. 122/2013 Coll., the Act on electronic commerce no. 22/2004 Coll., and the Code of Civil Procedure
- Previous regulation was to be found mainly in the Act no. 610/2003 Coll. on electronic communications, replaced by the current Act following the changes at the EU level.
- Additionally, regulation of unsolicited communication in the nature of direct marketing can also be found in Sec. 4 (6) of the Act no. 22/2004 Coll. on electronic commerce and in the Act on advertising no. 147/2001 Coll., as amended, in Sec. 3 para. 6.
- Finally, telemarketing is regulated by the Act no. 108/2000 Coll. on the Consumer Protection in Doorstep Selling and Distance Selling, with supervision being regulated by the Act no. 128/2002 Coll. on state control of the internal market in consumer protection matters.

<table>
<thead>
<tr>
<th>Concordance table</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>traffic data – Sec. 57(1) of the Act on electronic communications no. 351/2011 Coll.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>location data – Sec. 57(2) first sentence of the Act on electronic communications no. 351/2011 Coll.</td>
<td></td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
<td>Sec. 1 of the Act on electronic communications no. 351/2011 Coll.</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sec. 79 of the Act on electronic communications no. 351/2011 Coll. – which only invokes the ePrivacy Directive, instead of explicitly giving the scope of the Act.</td>
<td></td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
<td>Sec 55(3) of the Act on electronic communications no. 351/2011 Coll.</td>
<td></td>
</tr>
<tr>
<td>Art. 5.2 (Business exception)</td>
<td>Sec. 55(4) of the Act on electronic communications no. 351/2011 Coll.</td>
<td></td>
</tr>
<tr>
<td>Art. 5.3 (Cookies)</td>
<td>Sec. 55 (5) of the Act on</td>
<td></td>
</tr>
</tbody>
</table>
| **Art. 6 (Traffic data)** | Art. 6 (1) transposed into: Sec. 57(4), of the Act on electronic communications no. 351/2011 Coll., and Sec. 17 of the Act on personal data protection no. 122/2013 Coll.  
Art. 6 (2) transposed into: Sec. 57(5) first sentence of the Act on electronic communications no. 351/2011 Coll.  
Art. 6 (3) transposed into: Sec. 57(7) of the Act on electronic communications no. 351/2011 Coll.  
Art. 6 (4) transposed into: Sec. 56(4), Sec. 57(7) of the Act on electronic communications no. 351/2011 Coll.  
Art. 6 (5) transposed into: Sec. 57(6) of the Act on electronic communications no. 351/2011 Coll.  
| **Art. 9 (Other location data)** | Art. 9(1) transposed into: Sec. 57(2) sentences 2-4 of the Act on electronic communications no. 351/2011 Coll.  
| Art. 13 (Unsolicited communications) | Art. 13(1) transposed into: Sec. 62(2) of the Act on electronic communications no. 351/2011 Coll.  
Art. 13(2) transposed into: Sec. 62(3) sentences 1-2 of the Act on electronic communications no. 351/2011 Coll.  
Art. 13(3) transposed into: Sec. 4(6) of the Act on electronic commerce no. 22/2004 Coll.  
Art. 13(4) transposed into: Sec. 62(3) third sentence of the Act on electronic communications no. 351/2011 Coll.  
Art. 13(5) transposed into: Sec. 62(4) of the Act on electronic communications no. 351/2011 Coll.  
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)
For each authority please provide in the table below:
   a. the full name in your national language
   b. the English translation of the short name
   c. the part or the provision(s) of the ePrivacy Directive it supervises
   d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky</td>
<td>Ministry of Transport, Construction and Regional Development</td>
<td>Is the supreme strategic body which oversees compliance</td>
<td><a href="http://www.telecom.gov.sk/index/index.php?lang=en">http://www.telecom.gov.sk/index/index.php?lang=en</a></td>
</tr>
<tr>
<td>Rada pre vysielanie a retransmisiu</td>
<td>Council for Broadcasting and Retransmission</td>
<td>Cooperates with the Electronic Communications Office in relevant matters</td>
<td><a href="http://www.rvr.sk/en/">http://www.rvr.sk/en/</a></td>
</tr>
<tr>
<td>Úrad na ochranu osobných údajov Slovenskej republiky</td>
<td>Office for Personal Data Protection</td>
<td>Cooperates with the Electronic Communications Office in personal data protection issues</td>
<td><a href="http://www.dataprotection.gov.sk/uuou/en">http://www.dataprotection.gov.sk/uuou/en</a></td>
</tr>
</tbody>
</table>
- The Electronic Communications Office also cooperates with the European Commission, national regulators of other Member States, and with the network operators acting in the territory of Slovakia.
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

According to Sec. 1(3) of the Slovak Act on electronic communications, no. 351/2011 Coll., electronic communication provides for the exchange and transfer of information especially in the form of video, audio and text within electronic communications networks.

Electronic communications network is defined in Sec. 2(1) as a functionally interconnected system of transmission systems and, where necessary, interconnection of routing devices, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed networks, circuit-switched and packet-switched, Internet and mobile terrestrial networks, networks for the distribution of electricity to the extent that they are used for transmitting signals, networks of radio and television broadcasting and cable distribution systems regardless of the type of information conveyed.

Public network defined in Sec. 2(2) means a network which is used wholly or mainly for the provision of publicly available electronic communications services, which support the transfer of signals between network termination points.

The Act also operates with the notion of “special network” – in Sec. 49. This is a network which is established and operated for military purposes and only for a specified group of entities. Special network is not a public network. The right to establish and operate a special network belongs to the Ministry of Defence, Ministry of Interior, the National Security Authority and the Slovak Information Service. Only one Section of the Act on e-communications deals with special networks. The operators of special networks shall neither provide public services nor enable the provision of such services by means of special networks to third parties. The connection of the special network to a public network shall take place only in case of an important national interest, based on the request of the operator (here the notion of “operator is being used instead of the “undertaking”) of the special network. The undertaking as an operator of the public network shall be obliged to satisfy the justified request, if technically feasible. General rules of the Act on e-communications, concerning general authorization to provide electronic communications services, are not applicable to special networks. Their operators are attributed individual authorisations.

The electronic communications service is defined in the Act on e-communications in Sec. 3(1) as a service normally provided for remuneration, which consists wholly or mainly in the conveyance of signals over networks, including telecommunications services and transmission services in networks used for broadcasting. Service is not the provision of content or ensuring or the exercise of editorial oversight over content transmitted through networks and services, and it also does not include those information society services, which do not consist wholly or mainly in the conveyance of signals over networks.

Under Sec. 3(2), public service means a publicly available service, use of which may be requested by everybody. Public telephone service means a public service for direct or indirect making and receiving national and international calls by means of one or more numbers from the national or international numbering plans.
Definitions of “Provider” or “Operator” are not given in the Slovak Act on e-communications. Sec. 5 (1) of the Act defines an “undertaking”, instead: “For the purposes of this Act, undertaking means every person who provides a network or service; undertaking’s activity means a network or a service provision in the electronic communications sector for the third party”.

Deviations from the wording of the Directive with respect to the definitions are marked in bold italics in the previous paragraphs of this text; to sum them up - definition of electronic communications network includes additional words “including network elements which are not active” (i.e. fibre, etc.), and a definition of public service is added: “Public service means a publicly available service, use of which may be requested by everybody. Public telephone service means a public service for direct or indirect making and receiving national and international calls by means of one or more numbers from the national or international numbering plans.”

4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

The services such as VoIP, webmail and location based services are not mentioned explicitly in the Act; nevertheless, they could fall under the definition of electronic communications service, if they consist “wholly or mainly in the conveyance of signals over networks”. Still, in practice, the E-Communications Office does not specifically address these services at all, neither does it include these into its analyses of relevant e-communications markets. They are rather considered information society services.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities? By way of example: have there been cases where your national law has been applied to a foreign entity?

The Act does not deal with the territorial scope or cross-border situations at all, with the exception of cross-border dispute resolution in Sec. 76 of the Act on electronic communications, provided that a Slovakian undertaking is involved.

In principle, the provisions of the Act are applicable to “operators”, in Slovakian terminology, “undertakings” whereas with respect to general principles of applicability of Slovakian laws it is clear they may be applicable only to Slovakian entities and to the entities performing their activities in the territory of Slovakia. Hence, the Slovakian E-Communications Office is only competent in relation to undertakings providing services in Slovakia.

No cases where national law has been applied to a foreign entity are available.
6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There is no guidance document on the definitions mentioned in this section.</td>
</tr>
<tr>
<td>b.</td>
<td>We are not aware of any court cases in Slovakia with regard to the interpretation of the term “operator” or “undertaking”, or with regard to the territorial and personal scope of the Act on e-communications, or to any of the other definitions mentioned in this section.</td>
</tr>
</tbody>
</table>
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

<table>
<thead>
<tr>
<th>a. The rules are far from clear as seen from the given definitions and scope of the Act. However, honestly speaking, disputed do not come up in Slovakia at all, except of the cases of unsolicited communications; this may be due to the small market and the low level of public awareness of the possibilities of privacy protection within electronic communications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. The competence of both the E-Communications Office and of the Personal Data Protection Office should be specified explicitly (and potentially the privacy protection might be entrusted only to the Personal Data Protection Office), since the competences are split in the current situation, whereby the unsolicited communications, data breach notification and protection of traffic and location data is entrusted to the E-Communications Office, and the data protection is entrusted to the Personal Data Protection Office. Additionally, clarification might be necessary with respect to foreign operators. Awareness raising among the public is to be recommended with respect to possibilities of legal protection, since it is so far only direct marketing unsolicited communications that are recognized by the public as worth legal protection. Finally, the definitions are not clear with respect to latest technologies, specifically in relation to the VoIP and similar services.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

<table>
<thead>
<tr>
<th>1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?</th>
</tr>
</thead>
</table>

Sec. 55(3) of the Act on e-communications reiterated the wording of Art. 5.1 of the Directive. It added a sentence: “The undertaking shall not be held liable for protection of the conveyed information if such information can be directly listened to or obtained at the location of broadcasting or location of reception.”

The whole relevant section of the Act is worded as follows: “(3) The undertaking that provides a public network or service shall be obliged to ensure technically and organisationally confidentiality of communications and the related traffic data which are conveyed by means of its public network and public services. It shall be prohibited in particular tapping, listening, storage or other kinds of interception or surveillance of communications and the related data by persons others than users or without the consent of the users concerned, unless stipulated otherwise by this Act. This shall not prevent the technical storage of data which is necessary for the conveyance of communications without prejudice to the principle of confidentiality. The undertaking shall not be held liable for protection of the conveyed information if such information can be directly listened to or obtained at the location of broadcasting or location of reception.”

The definition of “communication” is given in Sec. 55(2) of the Act on e-communications as follows: “Communication means any information exchanged or conveyed between a finite number of parties by means of a public service; apart from the information conveyed as part of radio or television broadcast through a network which cannot be related to an identifiable user receiving the information.”
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations.

<table>
<thead>
<tr>
<th>This provision has been transposed into Sec. 55(4) of the Act on e-communications as follows: “(4) The ban under Subsection 3 Sentence 2 shall not apply to the temporary recording and storing messages and the related traffic data if it is necessary for the provision of value added services ordered by a subscriber or user, to prove a request to establish, change or withdraw the service or to prove the existence or validity of other legal act which the subscriber, user or undertaking has made.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Act hence does not explicitly mention business practice; however, it similarly regulates the possibility to record communication with the subscriber, user or undertaking.</td>
</tr>
</tbody>
</table>
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Sec. 63 (4-6) of the Act on e-communications provide for obligatory cooperation with state authorities:

(4) For the purposes of working in conjunction with other state bodies under Section 55, Subsection 6, the undertaking that provides public services may collect and process the subscribers’ data in the scope defined in Section 56, Subsection 3. (Sec 56(3) reads: “For the purposes of conclusion and fulfilment of a contract for the provision of public services, amendment thereof, termination or number portability, billing, receipt and registration of payments, claims and claim transfer and producing a directory of subscribers, the undertaking providing public services may obtain and process personal data of users which shall be the telephone number, amount of unpaid obligations and:

a) name, surname, degree, permanent residence address, birth certificate number, identity card number or other identity document of a natural person,
b) business name and place of business and identification number of a natural person–entrepreneur, or

c) business name and place of business and identification number of a legal person.)

(5) On the basis of a written request, the undertaking providing public networks or public services shall be obliged under Section 55, Subsection 6 to permit online, direct and continuous access to the subscribers’ data of its own network or services in the scope of data under Subsection 4 and the user allocated identification and Internet protocol address; it shall be obliged, upon a request, to provide such data together with the data on the base stations of the public telephone network and database of International Mobile Subscriber Identity (IMSI) in an electronic form and intelligible manner without delay also on a physical information carrier. The state body to which such access has been enabled shall cover the cost for ensuring the online access up to the interface of the undertaking and the physical information carrier.

(6) The undertaking shall be obliged to provide other state body under Section 55, Subsection 6 for the purposes of fulfilling its tasks under special regulations, on the basis of a written request and with the court’s consent or on court’s order under special regulations, with the data which are subject to telecommunications secrecy under Subsection 1, Letter b) to d); in case of the data necessary for searching for missing persons and stolen motor vehicles this shall be regulated under a special regulation. The undertaking shall be obliged to provide the data to other state body under Section 55, Subsection 6, in a written form or encrypted electronic form and in an intelligible manner. The state body to which such data have been provided shall cover the cost for physical carriers.

Sec. 63 (7) of the Act on e-communications provides for six exceptions to the confidentiality of communication:

(7) The undertaking providing public networks or public services shall be also obliged:

a) To operate public networks or provide public services by means of such technology, including its individual parts and software, which makes it possible to connect and operate the equipment for listening and tapping of traffic in a network owned, by the state and the online access under Subsections 5 and 6,

b) On the basis of Section 55, Subsection 6, to permit other state body the connection of the equipment for listening and tapping of traffic under the technical specification of such equipment to
be connected; the state body which has requested the connection of the equipment for listening and tapping of traffic in the network shall cover the cost for the procurement of the equipment for listening and tapping of traffic in the network, including software and the provision of maintenance support of such equipment,

c) To cooperate with the Police corps and authorities acting in a criminal proceedings when disclosing malicious calls and scaremongering,

d) On the basis of a justified summons, to restrict, without delay, the traffic of a public network or the provision of a public service for the time and in the scope necessary, if it is necessary to protect the constitutional establishment or internal order or state security or state defence and there is an imminent danger to the detriment of life and health; the Minister of Interior of the Slovak Republic and in case of his absence the Minister of Defence of the Slovak Republic shall issue the summons. The state body upon which request the network traffic was restricted, shall be responsible for any detriments incurred by restricting the network traffic,

e) On the basis of a written request in justified cases related to fulfilling the tasks of state security and defence, to provide other state body under Section 55, Subsection 5 with the service presentation of calling line identification, and this even in case that the calling line has restricted presentation of its identification; the state body shall be held responsible for any detriment caused by the misuse of the information provided about personal data since the moment it was provided with the requested data,

f) To act in subsequent conjunction with the court, the authority acting in criminal proceedings and other state body under Section 55, Subsection 6, as is necessary to fulfil their tasks and execute their powers under this Act and special regulations.

Finally Sec. 63(8) concerns encrypted data:

(8) The undertaking providing public networks or public services which uses coding, compression, encryption or other manner of concealing of signal conveyance, shall be obliged, at its own expense, to provide, in a comprehensible manner, the information collected while listening and tapping traffic in networks, to other state body or authority acting in a criminal proceedings. On the basis of a proposal of the National Security Office, the Slovak Intelligence Service, the Military Intelligence or Police corps, the Office shall issue a list of equipments using coding, compression, encryption or similar equipment which shall be prohibited to connect to the network.

Sec. 90 of the Code of Criminal Procedure regulates storing and delivering (handing over) of computer data:

If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, the presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data is, or to a service provider of such services, with the view of:

a) storing and keeping completeness of such data
b) enabling production and possession of copies of such data
c) making access to such data impossible
d) removing such data from a computer system
e) handing over such data for the purposes of criminal proceedings.

The order must state a period of time during which data storage shall be carried out. Maximum period is 90 days, and if repeated storage is necessary, new order shall be issued. If
storage is no longer necessary, presiding judge or prosecutor in the stage before the commencement of criminal prosecution or within pre-trial proceedings shall issue the order to cancel data storage without delay. An order shall be served on a person in whose possession or control the data is or to a provider of such services.

The finding of the Constitutional Court no. III U.S. 68/2010-61 held that it is necessary to determine the time for keeping data by the police. Unrelated seized items should not be kept throughout the proceedings. This is due to the fact that Sec. 90 of the Criminal Procedure Code represents an interference with the right to privacy and the right to the protection of correspondence and other documents under Art. 19 para. 3 and Art. 22 para. 1 of the Constitution of Slovakia, as well as Art. 8 of the Convention on Human Rights. This was confirmed also by the finding of the Constitutional Court II. CC 53/2010 of 9 December 2010 and II. CC 96/2010 of 3 February 2011.

Sec. 116 of the Code of Criminal Procedure also regulates the interception of telecommunications – it ensures the preservation of operation data and it may be ordered by the presiding judge (under Sec. 90 this may be ordered by the prosecutor).

The Act no. 351/2011 Coll. on electronic communications also includes a specific obligation to retain data for the purposes of criminal procedure (Sec. 58). This was required by the Data Retention Directive 2006/24 as retention of traffic and location data (subject to telecommunications secret) specified in Annex 4 to the Act on electronic communications. This provision might however be considered unconstitutional, as stated in similar cases by the constitutional courts of other states (Romania, Germany or the Czech Republic). The Constitutional Court of Slovakia has suspended these provisions in the meanwhile (April 2014), taking into account also the relevant CJ EU award in this respect.

Legal ways of using the technological means of information and communication control in the territory of the Slovak Republic, are regulated also in numerous other laws besides the Criminal Procedure Code and the Act on electronic communications – mainly in Act no. 166/2003 Coll. on privacy protection against unauthorized use of information and technical resources (Act on protection against eavesdropping), the Act on Slovak Intelligence Service (46/1993 Coll., Sec. 10), and the Act on Military Intelligence (198/1994 Coll., Sec. 10).
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. The Slovak legislation does not explicitly address “automated breaches of confidentiality without human intervention”. (Only with respect to unsolicited communications, Sec. 62(2) of the Act on e-communications reads: For the purposes of direct marketing, the call or use of automated calling and communications systems without human intervention, facsimile machines, electronic mail, including SMS to the subscriber or user is allowed only after their preceding consent, while such consent shall be provable. The consent given may be recalled anytime.)

In principle any breaches of confidentiality will be considered an infringement of the Act on e-communications if they are outside the scope of the exceptions provided in the Act. Sec. 63 of the Act on e-communications, on telecommunications secrecy/confidentiality, covers both content as well as traffic and location data, notwithstanding whether related to “undertakings” or any other persons (providers) – the latter competence however only comes clear from the competence of the E-Communications Office with respect to sanctioning as given in Sec. 73 of the Act. This competence towards any other providers than undertakings is not explicitly stated in the relevant Sec. 63 of the Act.

Additionally, Sec. 57 of the Act on e-communications regulates manipulation with traffic data and location data as follows:

(4) Traffic data related to subscribers or users shall not be stored without the consent of the person concerned and the undertaking shall be obliged, after the end of a communication transmission, without delay, to destroy or make them anonymous except for the cases defined by this Act. This is without prejudice to the data storing under Section 58.

(5) If it is necessary for the billing of subscribers and network interconnection payments, the undertaking shall be obliged to store the traffic data until the expiration of the period, during which the bill may be legally challenged or the claim for the payment may be asserted. The undertaking shall be obliged to provide traffic data to the Office or court in case of a dispute between undertakings or between an undertaking and a subscriber. In case of the initiation of a claim, an out-of-court dispute resolution or court proceedings, in particular in case of disputes related to the network interconnection or billing, the undertaking shall be obliged to store the traffic data until the expiration of the period during which all legal means be used, and this until the closing of proceedings. The scope of the stored traffic data shall be limited to the inevitably necessary minimum.

(6) Traffic data under Subsections 4, 5 and 7 shall be processed only by persons acting as entrusted or on the basis of power of attorney of the undertaking, in the scope necessary for the purposes of ensuring the network traffic control, billing, answering user requests,
exposing frauds, cooperation with other state bodies under Section 55, Subsection 6, service marketing purposes or for the provision of value added service.

(7) The undertaking may process the traffic data of a subscriber or user for the purposes of marketing services or purposes of ensuring the value added services only with his prior consent. The undertaking shall be obliged to inform the subscriber or user prior to obtaining its consent about the type of traffic data, the purpose of traffic data processing and time of data processing. The subscriber or user may withdraw, anytime, his consent given for the processing of the traffic data for the marketing purposes or ensuring the value added services.

(8) Where the subscriber or user has given his consent for the processing of location data other than traffic data, the undertaking shall be obliged to enable him, by a simple means and free of charge, temporarily refuse the processing of such location data for each connection to the network or each transmission of a communication.

(9) Processing of location data under Subsections 2 and 8 shall be restricted to the persons acting under the authority of the undertaking that provides public networks or public services or of a third party that provides the value added service and shall be restricted to the purposes necessary for providing the value added service.

(10) In case of emergency calls, the undertaking may obtain and process and shall be obliged to provide, free of charge, the coordination centre of the integrated rescue system or the operation centre of emergency call with the calling line identification and location data, and this also in case that the calling party uses the service of the elimination of the presentation of calling line identification or has not given its consent to the processing of location data; where the user concerned is the Slovak Intelligence Service, the undertaking shall by obliged, without delay, to inform the Slovak Intelligence Service about the provision of such data. The coordination centre of the integrated rescue system and the operation centre of emergency call shall be taken responsible for any detriment incurred by misuse of the provided information on personal data and location data from the moment they are provided with the requested data.

Finally, Sec. 58 of the Act on electronic communications regulates retention of data (meanwhile suspended by the Constitutional Court).

b. The Criminal Code no. 300/2005 Coll. in its Sec. 196 regulates breach of mailing secrets, which includes also the secrecy of information transferred via electronic communications service:

Sec. 196:

(1) Any person who intentionally breaches
a) the secrecy of letter through spying or opening a sealed letter or other written communication delivered by postal service or in other habitual manner,
b) the secrecy of information transferred via electronic communications service, or
c) the secrecy of private transfer of computerized data to the computer system, out of it or within it, including electromagnetic radiation from computer system transferring such computerized data,
shall be liable to a term of imprisonment of up to three years.
(2) Any employee of the provider of postal service or electronic communications service who commits the offence referred to in paragraph 1, or wilfully enables another to commit such offence, or who alters or withholds a written communication delivered by postal service or in other habitual manner or communication transferred via electronic communication service, shall be liable to a term of imprisonment of one to five years.

(3) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraphs 1 or 2,

a) and causes substantial damage through its commission,
b) by reason of specific motivation,
c) acting in a more serious manner.

Sec. 197:
(1) Any person who, with the intention to cause damage to another, or to obtain an unlawful benefit for himself or another, a) divulges a mail secret which he got knowledge of from a closed letter or other written communication delivered by postal service or in other habitual manner that were not addressed to him, or from the information transferred via electronic communications service, or b) makes use of such secret, shall be liable to a term of imprisonment of up to three years.

(2) Any employee of the provider of postal service or electronic communications service who commits the offence referred to in paragraph 1, or wilfully enables another to commit such offence, shall be liable to a term of imprisonment of one to five years.

(3) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraphs 1 or 2,

a) and causes substantial damage through its commission,
b) by reason of specific motivation,
c) acting in a more serious manner.

Sec. 198:
(1) Any person who, in breach of a generally binding legal regulation, manufactures, procures for himself or another, or possesses the equipment capable of intercepting the information transferred via electronic communications service, shall be liable to a term of imprisonment of up to three years.

(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1,

a) and obtains larger benefit for himself or another through its commission, or b) acting in a more serious manner.

Additionally, Sec. 90 and Sec. 116 of the Code of Criminal Procedure also regulate the interception of telecommunications – it ensures the preservation of operation data and it may be ordered by the presiding judge (under Sec. 90 this may be ordered by the prosecutor within proceedings prior to commencement of criminal prosecution or within pre-trial proceedings).

Other legal ways of using the technological means of information and communication control in the territory of the Slovak Republic are regulated also in numerous other laws – mainly in the Act no. 166/2003 Coll. on privacy protection against unauthorized use of information and technologic resources (Act on protection against eavesdropping), Act on Slovak Intelligence Service (46/1993 Coll., Sec. 10), and Act on Military Intelligence.
Additionally, e.g., with respect to traffic data, Sec. 17 of the Act on personal data protection provides:

(1) The operator shall, after fulfilling the purpose of processing, without undue delay ensure destruction of personal data.

(2) Paragraph 1 shall not apply where personal data is part of the registry record. An operator shall ensure destruction of registry record under a special regulation.

(3) The operator shall, without undue delay, ensure destruction of personal data other than personal data referred to in Sec. 10 (3d) even if there no longer exist reasons which prevented obtaining the consent of the data subject under Sec. 11(4), and consent was not given.

(4) If the data subject raises an objection pursuant to Sec. 28(3a), the operator is obliged to promptly discard processed personal data except for personal data contained in Sec. 10(3d).

(5) If the data subject raises an objection pursuant to Sec. 28(3b), the operator shall, without undue delay, terminate the use of personal data contained in Sec. 10(3d) in the mail correspondence.

(6) If the data subject raises an objection pursuant to Sec. 28(3c), the operator shall, without undue delay, no later than within three working days, notify in writing any person to whom the personal data referred to in Sec. 10(3d) were provided; a ban on the provision of personal data specified herein is valid for the operator and anyone to whom the operator has provided the data from the day following the date of receipt of the objections of the data subject, or from the delivery of the written notice of the operator.

(7) If a record made under Sec. 15(7) is not used for the purpose of criminal proceedings or proceedings concerning administrative offences, is the one who created it obliged to dispose of it no later than 15 days from the day following the day on which the recording was made, unless a special law provides otherwise.
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third
      party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the
      type of device (e.g. general computers, mobile phones, tablets)?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Article 5.3 of the Directive was transposed into Sec. 55(5) of the Act on e-communications as follows: “Every person that stores or gains access to information stored in the terminal equipment of a user shall be authorised for that only if the user concerned has given his consent on the basis of clear and comprehensive information about the purpose of the processing; for this purpose the consent shall be also the use of a respective setting of the web browser or other computer programme. The obligation to gain the consent shall not apply to a body acting in criminal proceedings or other state body. This shall not prevent any technical storage of data or access thereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network or if it unconditionally necessary for the provider of an information society service to provide information society services if explicitly requested by the user.”</td>
</tr>
<tr>
<td>b.</td>
<td>There is no distinction made at all.</td>
</tr>
</tbody>
</table>
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

These issues are not regulated in the Act on E-Communications, and there are no guidelines of the E-Communications Office, or the Personal Data Protection Office.

Sec. 55(5) only states that “for this purpose the consent shall be also the use of a respective setting of the web browser or other computer programme.”
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

<p>| There is an almost literal translation of these provisions in Sec. 55(5) of the Act on electronic communications: “This shall not prevent any technical storage of data or access thereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network or if it is unconditionally necessary for the provider of an information society service to provide information society services if explicitly requested by the user.“ There is no specific rule concerning cookies in this respect. |</p>
<table>
<thead>
<tr>
<th>8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice? Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)? Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are no statistics, reports on enforcement actions, nor any related data, as far as we know. The usual way is a tacit acceptance through the “use of a respective setting of the web browser or other computer programme.” The majority of users hence ignores the warning and accepts the cookies automatically.</td>
</tr>
</tbody>
</table>
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law

   a. There is no guidance so far by the national authorities.

   b. There is no case law in this respect so far.
10. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

   a. The rules do not represent any practical problems, maybe also due to the possibility of considering *respective setting of the web browser or other computer programme* as a way of expressing consent.

   b. In practice, website owners (information society service providers) have started to implement the rules and inform users about the possibility to accept or refuse cookies usually in the form of a one-time banner that can easily be “clicked away” or ignored, or even be unnoticed. It is hence questionable whether it really meets the intended goals. On the other hand, regulation requiring the notice to be displayed in such a manner as not to go unnoticed, or to be additionally accessible any time later (after “clicking away”) by the user, might be considered burdensome to both the providers and users.
C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

Under Sec. 57(1) of the Act on e-communications, “Traffic data means any data related to the user and the particular conveyance of information in the network and arising during such a conveyance, which are processed for the purpose of conveyance of a communication in the network or for billing purposes.”

The difference in comparison to the Directive is in the use of the words: related to the user and the particular conveyance of information in the network and arising during such a conveyance. This might be in order to make sure that only data concerning the user and the specific conveyance and data arising from such specific conveyance will be considered traffic data, and enjoy the relevant legal status and protection. Any other data, mostly of technical nature, that are not directly connected to the user and specific conveyance of information shall not be considered traffic data.
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

Sec. 57 (4-7) of the Act on e-communications regulates the traffic data basically in the same manner as in the Directive:

(4) Traffic data related to subscribers or users shall not be stored without the consent of the person concerned and the undertaking shall be obliged, after the end of a communication transmission, without delay, to destroy or make them anonymous except for the cases defined by this Act. This is without prejudice to the data storing under Section 58.

(5) If it is necessary for the billing of subscribers and network interconnection payments, the undertaking shall be obliged to store the traffic data until the expiration of the period, during which the bill may be legally challenged or the claim for the payment may be asserted. The undertaking shall be obliged to provide traffic data to the Office or court in case of a dispute between undertakings or between an undertaking and a subscriber. In case of the initiation of a claim, an out-of-court dispute resolution or court proceedings, in particular in case of the disputes related to the network interconnection or billing, the undertaking shall be obliged to store the traffic data until the expiration of the period during which all legal means be used, and until the closing of proceedings. The scope of the stored traffic data shall be limited to the inevitably necessary minimum.

(6) Traffic data under Subsections 4, 5 and 7 shall be processed only by persons acting as entrusted or on the basis of power of attorney of the undertaking, in the scope necessary for the purposes of ensuring the network traffic control, billing, answering user requests, exposing frauds, cooperation with other state bodies under Section 55, Subsection 6, service marketing purposes or for the provision of value added service.

(7) The undertaking may process the traffic data of a subscriber or user for the purposes of marketing services or purposes of ensuring the value added services only with his prior consent. The undertaking shall be obliged to inform the subscriber or user prior to obtaining his consent about the type of traffic data, the purpose of traffic data processing and time of data processing. The subscriber or user may withdraw, anytime, his consent given for the processing of the traffic data for the marketing purposes or ensuring the value added services.
### 3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

Sec. 57(4) of the Act on e-communications reads: “Traffic data related to subscribers or users shall not be stored without the consent of the person concerned and the undertaking shall be obliged, after the end of a communication transmission, without delay, to **destroy or make them anonymous** except for the cases defined by this Act. This is without prejudice to the data storing under Section 58.“

Additionally, Sec. 17 of the Act on personal data protection provides:

(1) **The operator shall, after fulfilling the purpose of processing, without undue delay ensure destruction of personal data.**

(2) Paragraph 1 shall not apply where personal data is part of the registry record. An operator shall ensure destruction of registry record under a special regulation.

(3) **The operator shall, without undue delay, ensure destruction of personal data other than personal data referred to in Sec. 10 (3d) even if there no longer exist reasons which prevented obtaining the consent of the data subject under Sec. 11(4), and consent was not given.**

(4) If the data subject raises an objection pursuant to Sec. 28(3a), the operator is obliged to promptly discard processed personal data except for personal data contained in Sec. 10(3d).

(5) If the data subject raises an objection pursuant to Sec. 28(3b), the operator shall, without undue delay, terminate the use of personal data contained in Sec. 10(3d) in the mail correspondence.

(6) If the data subject raises an objection pursuant to Sec. 28(3c), the operator shall, without undue delay, no later than within three working days, notify in writing any person to whom the personal data referred to in Sec. 10(3d) were provided; a ban on the provision of personal data specified herein is valid for the operator and anyone to whom the operator has provided the data from the day following the date of receipt of the objections of the data subject, or from the delivery of the written notice of the operator.

(7) If a record made under Sec. 15(7) is not used for the purpose of criminal proceedings or proceedings concerning administrative offences, is the one who created it obliged to dispose of it no later than 15 days from the day following the day on which the recording was made, unless a special law provides otherwise.
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

| No information is available. |
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

| The Act on e-communications mostly regulates privacy protection with respect to “undertakings” (“operators”), but the Sec. 73 of the Act on electronic communications entrusts the E-Communications Office also with sanctioning other entities than “undertakings” with respect to breach of telecommunications secrecy, the notion of which under Sec. 63 involves also traffic and location data. First of all, this legislative technique is not clear enough for the addressees of the Act, and additionally, this causes a split in competences with regard to privacy protection between the E-Communications Office and the Personal Data Protection Office, leading to a potential inconsistency in their activities related thereto. |
D. Location data

<table>
<thead>
<tr>
<th>1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location data is defined in Sec. 57(2) of the Act on e-communications, as follows: “Location data means any data processed in a network or by a service that indicate the geographic location of the terminal of a user of a public service.” This is almost verbatim the definition from the ePrivacy Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

<table>
<thead>
<tr>
<th>Sec. 57(2, 8-9) of the Act on electronic communications regulates location data as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) The undertaking may process location data other than traffic data which relate to a subscriber or user of a public network or public service only if they are made anonymous or with their consent, and in the scope and time necessary for the provision of a value added service. The undertaking shall be obliged to inform the subscriber or user, prior to obtaining its consent on location data other than traffic data which will be processed, on the purpose and duration, and whether the data will be provided to a third party for the purposes of the provision of the value added service. The subscriber or user may revoke the consent for the processing of the location data anytime.</td>
</tr>
<tr>
<td>(8) Where the subscriber or user has given his consent for the processing of location data other than traffic data, the undertaking shall be obliged to enable him, by a simple means and free of charge, to temporarily refuse the processing of such location data for each connection to the network or each transmission of a communication.</td>
</tr>
<tr>
<td>(9) Processing of location data under Subsections 2 and 8 shall be restricted to the persons acting under the authority of the undertaking that provides public networks or public services or of a third party that provides the value added service and shall be restricted to the purposes necessary for providing the value added service.</td>
</tr>
</tbody>
</table>

There is no difference in comparison with the Directive.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

Sec. 57(2) of the Act on e-communications reads:

(2) The undertaking may process location data other than traffic data which relate to a subscriber or user of a public network or public service only if they are made anonymous or with their consent, and in the scope and time necessary for the provision of a value added service.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:
   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. There is no such guidance published, and no specific cases were reported.
   b. There is no relevant case law.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

| The Act on e-communications seems not to protect individuals sufficiently against illegitimate processing of location data, because the relevant Section of the Act is limited to “undertakings”, and only the final provisions of the Act entrust the E-Communications Office also with sanctioning potential breaches of privacy by other entities. There might also be a problem with respect to the general competence of the Personal Data Protection Office – the competence with respect to privacy is namely entrusted to two separate Offices – the E-Communications Office and the Personal Data Protection Office. |
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

   a. Art. 13 of the Directive was transposed into Sec. 62 (2,3, 4) of the Act on electronic communications, Sec. 4(6) of the Act on electronic commerce and Sec. 3 of the Code of Civil Procedure:

   13(1) was transposed into Sec. 62(2) of the Act on e-communications:
   (2) For the purposes of direct marketing, the call or use of automated calling and communications systems without human intervention, facsimile machines, electronic mail, including SMS to the subscriber or user is allowed only after their preceding consent, while such consent shall be provable. The consent given may be recalled anytime.

   13(2) was transposed into Sec. 62(3) sentence 1 and 2 of the Act on e-communications:
   (3) The preceding consent of the recipient of an electronic mail under Subsection 2 shall not be required if it is a case of direct marketing of own similar products and services of the person that has obtained the contact information for the electronic mail delivery in relation to the product or service sale and in accordance with this Act or a special regulation. The recipient of an electronic mail shall be offered a possibility, simply and free of charge and anytime, to reject such use of contact information at the time of their collection and on the occasion of each message delivered in case he has not initially refused such use.

   13(3) was transposed into Sec. 4(6) of the Act on electronic commerce:
   The service provider must not deliver commercial communications information by electronic mail unless the recipient of services has asked for it in advance.

   13(4) was transposed into Sec. 62(3) sentence 3 of the Act on e-communications:
   It shall be prohibited to send an electronic mail which does not disclose the sender’s identity and address to which the recipient may send a request that such communications cease, and which encourages to a visit of a website in contradiction with a special regulation.

   13(5) was transposed into Sec. 62(4) of the Act on e-communications:
   (4) Subsections 2 and 3 shall apply to subscribers who are natural persons.

   13(6) was already present in the Slovak legal system – in Sec. 3 of the Code of Civil Procedure:
   Civil procedure is one of the guarantees of fairness and justice, serving the consolidation and development of the principles of private law. Any person may request the court to protect the private right which has been endangered or violated.

Additionally, unsolicited communication in the nature of direct marketing can be also found regulated in the Act on advertising no. 147/2001 Coll., as amended, in Sec. 3 para. 6. It states that
advertising must not be disseminated via automated call system, telefax and e-mail without the prior consent of the user, who is the recipient of advertising. Sec. 3(7) states that advertising must not be disseminated to specific addressees, if the addressee refused in advance the delivery of advertisement.

Furthermore, telemarketing is regulated by the Act no. 108/2000 Coll. on the Consumer Protection in Doorstep Selling and Distance Selling, with supervision being regulated in the Act no. 128/2002 Coll. on state control of the internal market in consumer protection matters.

b. Art. 13(1) of the Directive was transposed into Sec. 62(2) of the Act on e-communications whereby in addition to the wording of the Directive, short message services (SMS) are specifically mentioned, the consent has to be “provable”, and it can be revoked any time. No other differences were identified.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>13(1) was transposed into Sec. 62(2) of the Act on e-communications:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) For the purposes of direct marketing, the call or use of automated calling and communications systems without human intervention, facsimile machines, electronic mail, including SMS to the subscriber or user is allowed only after their preceding consent, while such consent shall be provable. The consent given may be recalled anytime. In addition to the wording of the Directive, short message services (SMS) are specifically mentioned, the consent has to be “provable”, and it can be revoked any time. No other differences were identified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13(3) was transposed into Sec. 4(6) of the Act on electronic commerce:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The service provider must not deliver commercial communications information by electronic mail unless the recipient of services has asked for it in advance. Additionally, the Act on advertising no. 147/2001 Coll., as amended, in Sec. 3(6) states that advertising must not be disseminated via automated call system, telefax and e-mail without the prior consent of the user, who is the recipient of advertising. Sec. 3(7) states that advertising must not be disseminated to specific addressees, if the addressee refused in advance the delivery of advertisement.</td>
</tr>
<tr>
<td>3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>There are two exceptions to the opt-in consent mechanism:</td>
</tr>
<tr>
<td>13(2) was transposed into Sec. 62(3) sentence 1 and 2 of the Act on e-communications:</td>
</tr>
<tr>
<td><strong>(3)</strong> The preceding consent of the recipient of an electronic mail under Subsection 2 shall not be required if it is a case of direct marketing of own similar products and services of the person (N.B. meaning person entitled to provide services or products – it includes both legal persons as well as natural persons - mostly being natural persons-entrepreneurs) that has obtained the contact information for the electronic mail delivery in relation to the product or service sale and in accordance with this Act or a special regulation. The recipient of an electronic mail (N.B. the notion of “recipient” is used explicitly in the Act, rather than “addressee”) shall be offered a possibility, simply and free of charge and anytime, to reject such use of contact information at the time of their collection and on the occasion of each message delivered in case he has not initially refused such use.</td>
</tr>
<tr>
<td>This exception exempts consent by one’s customers to send them direct marketing commercial communication by electronic mail when three conditions have been met, cumulatively:</td>
</tr>
<tr>
<td>- Firstly, the customer’s electronic data must have been obtained via the sale of a product or service in accordance with the legal and regulatory conditions on privacy protection.</td>
</tr>
<tr>
<td>- Secondly, the electronic contact data may be used exclusively for similar products or services.</td>
</tr>
<tr>
<td>- Thirdly, when collecting the contact data, the customers must be afforded the opportunity of easily objecting to future advertisement, free of charge. In addition, the customer has the option to object on the occasion of each message delivered.</td>
</tr>
<tr>
<td>The second exception concerns legal persons. It is not necessary to obtain a legal person’s prior consent before being allowed to send advertisements by electronic mail:</td>
</tr>
<tr>
<td>13(5) was transposed into Sec. 62(4) of the Act on e-communications:</td>
</tr>
<tr>
<td><strong>(4)</strong> Subsections 2 and 3 shall apply to subscribers who are natural persons.</td>
</tr>
</tbody>
</table>
Legislation mentions SMS explicitly:
13(1) was transposed into Sec. 62(2) of the Act on e-communications:
(2) For the purposes of direct marketing, the call or use of automated calling and communications systems without human intervention, facsimile machines, electronic mail, including SMS to the subscriber or user is allowed only after their preceding consent, while such consent shall be provable. The consent given may be recalled anytime.

However, this was not necessary since the Sec. 62(1) of the Act on e-communications defines electronic mail in very broad terms anyway:
(1) Electronic mail means any text, voice, sound or image message sent over a public network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

- a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
- b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>There are no guidance, but only individual standpoints have been issued with respect to individual complaints. This issue might seem to belong rather to the scope of activities of the Personal Data Protection Office, but currently it is the E-Communications Office that is entitled to impose fines in case of unsolicited communications.</td>
</tr>
<tr>
<td>b.</td>
<td>There is no reported case law.</td>
</tr>
</tbody>
</table>
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

The problem of legal regulation of unsolicited communication in all three Acts (on e-communications, on e-commerce and on advertising) is that many kinds of spam (other than commercial – direct marketing – communications) do not fall under any statutory definition. Each definition namely requires that spam is a commercial communication, thus the prohibition in the abovementioned Acts has only a limited effectivity.
COUNTRY REPORT

SLOVENIA

For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Mark Pohar, Agency for Communication Networks and Services of the Republic of Slovenia

Date: 18.08.2014
Contents

Part 1: Management summary ........................................................................................................... 3
Part 2: Answers to the questionnaire ................................................................................................ 4
Part 1: Management summary

Executive Summary for Slovenia:

The transposition of the ePrivacy Directive into Slovenian law can be summarized as follows:

- The ePrivacy Directive has been transposed into Slovenian legislation by the Electronic Communication Act (ECA-1) which came into force in January 2013. However, enforcement of provisions regarding cookies only began in June 2013 as there has been a 5-month transitional period set in the ECA-1. The law almost entirely follows the provisions of the Directive. It is applicable to the processing of personal data in connection with the provision of publicly available electronic communications services over public communications networks. Terms such as “electronic communication network” and “electronic communication service” entirely correspond to the definitions in article 2 of the Directive. Broadcasting services and information society services are excluded from the scope of privacy rules in the ECA-1. Beside the ECA-1 some other acts have impact on e-privacy (i.e. the E-Commerce Market Act, Consumer Protection Act and Personal Data Protection Act) and there are also some bylaws adopted by the ministries and Agency for Communication Networks and Services (AKOS) applicable. National enforcement authorities (i.e. AKOS and the Information Commissioner) have power to provide further guidance by adopting non-binding “soft law” such as recommendations and opinions. Both authorities are also actively participating in some national projects on promoting e-privacy.

- Any kind of surveillance or interception of communications by third parties is prohibited by the ECA-1. However, the ECA-1 also prohibits the recording and retention of communications of the user without obtaining the prior consent of the participants of the communications, if such processing is not usual and where the participants in communication do not expect it. There are four exceptions to confidentiality provided in the ECA-1 (lawful interception, data retention, technical storage, supplying data to police in case of missing person). Additionally, the recording of communication is allowed for the purpose of lawful business practice if certain conditions are met. The same rules are also applicable to state bodies if a legal basis is provided by law. Regarding cookies, the ECA-1 now stipulates an opt-in regime with informed consent. To determine whether the information given has been clear and precise enough, the provisions of the Personal Data Protection Act and guidelines of the Information Commissioner are taken into account. However, some cookies may be installed even without prior consent, but only if said cookie is necessary for transmitting a message or for providing a service, requested by the user. Additional guidance on exceptions is provided by the recommendation/opinions of the Information Commissioner, who is the competent enforcement authority.

- The provisions of the ePrivacy Directive with regard to traffic data have been more or less literally transposed into Slovenian law. The definition of traffic data corresponds to that in the Directive and the substantive provisions almost entirely correspond to art. 6 of the Directive (the only difference is that Slovenian law requires that the information on processing of traffic data regarding the billing should be stated in the General Terms of the service provider). The ECA-1 allows operators to process traffic data for purposes of billing/interconnection payments or for marketing of electronic communication services or value added services (VAS), accordingly. However, there are certain conditions provided in law (such as time limitation of processing and prior notification) while the consent of the user/subscriber is required only in case of VAS.

- As for location data, the situation is very similar. Processing of location data is allowed only if it is made anonymous, or with the prior consent of the user/subscriber in case of VAS. In this respect, Slovenian law follows provisions of the e-Privacy Directive, with some additional provisions on supplying location

---

1 Adopted in 2006 and amended in 2009
3 Adopted in 2007
data to the police in case of search of missing persons (art. 153) and in case of emergency phone calls or phone calls to the police (art. 152(5)). The processing of location data without the consent of user is also allowed in case of data retention.

- In the case of unsolicited communications the same four acts are applicable (Electronic Communications Act, Electronic Commerce Act, Consumer Protection Act and Personal Data Protection Act), implementing the ePrivacy Directive, e-Commerce Directive and Data Protection Directive. Although the competence for enforcement of SPAM rules lies within the NRA, two other authorities are also competent (i.e. the Information Commissioner and Market Inspectorate). Such a situation does not aid legal certainty and leads to confusion in practice. Nevertheless, Slovenian legislation requires opt-in for receiving commercial communications. However, the law allows sending commercial emails without the consent of the user if the address has been obtained in previous business contact and if it is used for marketing similar products and services.

Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:
   - the full title of the law in English
   - the short title of the law in English
   - the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

**Slovenia:**
- The ePrivacy Directive has been first transposed into Slovenian legislation by the Electronic Communication Act (ECA), which was published in Official Gazette on 26.4.2004 (OG RS, no. 43/04) and entered into force on 01.05.2004
- Amendments to the ECA followed in 2004, 2006, 2007, 2009 and 2011. However, only amendments from 2006 (i.e. ECA-A) and 2007 (i.e. ECA-B) influenced the provisions regarding the privacy in electronic communications. ECA-A (OG RS no. 129/06) transposed the Directive 2006/24/EC on data retention, while ECA-B (OG RS no. 102/07) brought some corrigendum on data retention and introduced the provisions on supplying traffic data to competent authorities in case of searching of missing persons.
- After the adoption of the 2009 EU Regulatory Package, new rules have been transposed in national legislation by Electronic Communication Act (ECA-1) which replaced the previous law with all its amendments. The ECA-1 was adopted on 31.12.2012 (OG RS, no. 109/12) and entered into force on 15.1.2013. After that two minor amendments to the law were passed in 2013 in 2014, both having no effect on the provisions regarding privacy in electronic communications.
- The text of the ECA-1 (in Slovenian only) can be found at the following link: [http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405](http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405)
- Unofficial translation of ECA-1 in English can be found at the following link: [https://www.ip-rs.si/index.php?id=504](https://www.ip-rs.si/index.php?id=504)
Besides the Electronic Communication Act (ECA-1) the following bylaws regarding privacy in electronic communication are also applicable:
- Rules on the equipment and interfaces for lawful interception (OG RS, no. 89/13),
  [http://pisrs.si/Pis.web(pregledPredpisa?id=PRAV6488](http://pisrs.si/Pis.web(pregledPredpisa?id=PRAV6488)
- Regulations on the way of execution of article 153. of Electronic Communications Act (OG RS, no. 73/13)
  [http://www.uradni-list.si/1/objava.jsp?urlurid=20132742](http://www.uradni-list.si/1/objava.jsp?urlurid=20132742)
- Rules on the method of transmitting retained data on the traffic of telephone and data services in mobile and fixed electronic communications networks (OG RS, no. 89/13)*  [http://www.uradni-list.si/1/objava.jsp?urlurid=20133220](http://www.uradni-list.si/1/objava.jsp?urlurid=20133220)
- General act on data retention (OG RS, no. 75/13)* [http://www.pisrs.si/Pis.web(pregledPredpisa?id=AKT_863](http://www.pisrs.si/Pis.web(pregledPredpisa?id=AKT_863)
* Bylaws which refer only to data retention

It should be brought to attention that besides the Electronic Communications Act in Slovenia provisions on unsolicited communications are also included in three additional acts:
- Electronic Commerce Market Act-ZEPT [art. 6](http://www.pisrs.si/Pis.web(pregledPredpisa?id=ZAKO6405)
- Consumer Protection Act-ZVPot [art. 15a](http://www.pisrs.si/Pis.web(pregledPredpisa?id=ZAKO6405)
- Personal Data Protection Act-ZVOP [art. 15](http://www.pisrs.si/Pis.web(pregledPredpisa?id=ZAKO6405)

<table>
<thead>
<tr>
<th>Concordance table</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePrivacy Directive</td>
</tr>
<tr>
<td>Art. 2 (Definitions)</td>
</tr>
<tr>
<td>Art. 3 (Scope)</td>
</tr>
<tr>
<td>Art. 5.1 (Confidentiality)</td>
</tr>
</tbody>
</table>

---

* Adopted in 2006 and amended in 2009
* Adopted in 2007
<table>
<thead>
<tr>
<th>Article</th>
<th>Description</th>
<th>Act</th>
<th>Paragraph(s)</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2</td>
<td>Business exception</td>
<td>Electronic Communications Act</td>
<td>art. 147, para. 7 and 8</td>
<td>[Here](<a href="http://www.pisrs.si/Pis.web/pr">http://www.pisrs.si/Pis.web/pr</a> egledPredpisa?id=ZAKO6405)</td>
</tr>
<tr>
<td>5.3</td>
<td>Cookies</td>
<td>Electronic Communications Act</td>
<td>art. 157</td>
<td>[Here](<a href="http://www.pisrs.si/Pis.web/pr">http://www.pisrs.si/Pis.web/pr</a> egledPredpisa?id=ZAKO6405)</td>
</tr>
<tr>
<td>6</td>
<td>Traffic data</td>
<td>Electronic Communications Act</td>
<td>Art. 151</td>
<td>[Here](<a href="http://www.pisrs.si/Pis.web/pr">http://www.pisrs.si/Pis.web/pr</a> egledPredpisa?id=ZAKO6405)</td>
</tr>
<tr>
<td>9</td>
<td>Other location data</td>
<td>Electronic Communications Act</td>
<td>art. 152</td>
<td>[Here](<a href="http://www.pisrs.si/Pis.web/pr">http://www.pisrs.si/Pis.web/pr</a> egledPredpisa?id=ZAKO6405)</td>
</tr>
<tr>
<td>13</td>
<td>Unsolicited communications</td>
<td>Electronic Communications Act</td>
<td>art. 158</td>
<td>[Here](<a href="http://www.pisrs.si/Pis.web/pr">http://www.pisrs.si/Pis.web/pr</a> egledPredpisa?id=ZAKO6405)</td>
</tr>
</tbody>
</table>
2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

a. the full name in your national language
b. the English translation of the short name

c. the part or the provision(s) of the ePrivacy Directive it supervises

d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agencija za komunikacijska omrežja in storitve Republike Slovenije (AKOS)</td>
<td>Agency for Communication Networks and Services (AKOS)</td>
<td>All provisions regarding processing of personal data processing and protection of the privacy of electronic communications (Chapter XII of ECA-1) except art. 149, 153, 155 and 157</td>
<td><a href="http://www.akos-rs.si/akos-ang">http://www.akos-rs.si/akos-ang</a></td>
</tr>
<tr>
<td>Informacijski pooblaščenec (IP)</td>
<td>Information Commissioner (IP)</td>
<td>Provisions of ECA-1 regarding: -establishing of internal procedures for responding to requests from competent authorities for access to users’ personal data (art. 149) - procedures of supplying traffic and location data in case of missing persons (art. 153) -tracing of malicious or nuisance calls (art. 155) -cookies (art. 157)</td>
<td><a href="https://www.ip-rs.si/">https://www.ip-rs.si/</a></td>
</tr>
<tr>
<td>Državni Zbor Republike Slovenije, Komisija za nadzor nad delom varnostno obveščevalnih služb</td>
<td>The Parliament of the Republic of Slovenia, Commission for the Supervision of Intelligence and Security Services</td>
<td>Additional competence regarding the lawful interception</td>
<td><a href="http://www.dz-rs.si/wps/portal/en/Home">http://www.dz-rs.si/wps/portal/en/Home</a></td>
</tr>
</tbody>
</table>
Additional explanations:

The Commission for the Supervision of Intelligence and Security Services is part of the Parliament. Under the Parliamentary Supervision of the Intelligence and Security Services Act (OG RS no. 93/07-UPB), special parliamentary body supervises lawful interception operations conducted by intelligence and security services of the Ministry of Defence and the Ministry of Interior.

The Market Inspectorate is part of the state administration. It monitors compliance of legislation on the fields of consumer protection, product safety, trade, catering, crafts, services, pricing, tourism, competition protection and copyrights. According to the Electronic Commerce Market Act (OG RS, no 96/09-UPB), the Market Inspectorate is competent for monitoring the commercial communications which are part of information society services (art. 6). Market Inspectorate is also competent for monitoring the provisions of Consumer Protection Act (art. 15a) regarding the marketing of information society services.

3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The ECA-1 defines electronic communication networks as follows (see art. 3(5)):

“transmission systems and, where applicable, switching or routing equipment and other resources, including inactive network elements, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed.”

According to art. 3(6) of the ECA-1 electronic communication service means a “...service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks including telecommunications services and transmission services in networks used for broadcasting”, the ECA-1 explicitly excludes media services (i.e. services providing or exercising editorial control over content) and information society services but only if they do not, wholly or mainly, include the transmission of signals over electronic communications networks.

When it comes to the privacy and processing of personal data, the ECA-1 only refers to publicly available electronic communications services over public communications networks. Therefore processing of personal data falls within the scope of the ECA-1, but only if two cumulative conditions are met: (i) data should be in connection with provision of publicly available electronic communications services and (ii) services should be provided over public communications networks (see art. 144(2)). Publicly available electronic communication service is defined as a service which is available to public and public communications network is defined as “an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services and enabling the transmission of information between network termination points”. For processing the data over non-public communications services the Personal Data Protection Act...
applies.

As for the subjects who are obliged by the provision of the ECA-1, the law distinguishes between “network operator” and “service provider”. The former is defined as “a natural person or legal entity which provides public communications networks or associated facilities, or which has notified a competent regulatory authority of the intended provision of a public communications network or associated facilities.” (art. 3, para 42) and the latter is defined as “a natural person or legal entity which provides publicly available communications services or which has informed the competent regulatory authority of its intent to provide publicly available communications services.” (art. 3, para 16). The ECA-1 also introduced the term “operator” which means both, service provider and network operator (art. 3, para 41). This distinction is important as some provisions of Chapter XII of the ECA-1 refer only to “service providers” while others refer to “operators” (eg. art. 147, 151, 153, 158 and 160).

Attention should be brought to the provisions of art. 158 of the ECA-1 (unsolicited communications). Although it is not explicitly provided for in the text of the law, it seems that this provision is addressed to any legal or natural person which is selling his/her products/services by means of direct marketing. Therefore, besides the operators also other subjects are obliged by the certain provisions of ECA-1.

One may conclude that definitions of the networks, services and providers in the ECA-1 mainly correspond to those in ePrivacy Directive.
4. Do services such as VoIP, webmail and location based services fall within the scope of the implementing legislation (either according to the text of the law or according to its interpretation/application in practice)?

**Slovenia:**
According to the definition in the ECA-1 art. 144, para. 2, only those electronic communication services which are publicly provided over public electronic communication network fall within the scope of Chapter XII of the ECA-1. The law *ex lege* excludes all media services and information society services (the latter only in case if they do not wholly or partly consist of transmission of electronic signals) from the scope of e-privacy rules.

In Slovenia, VoIP has been considered as a part of the relevant market for mobile and fixed termination (i.e. Market 3 and Market 7) and thus regarded as an electronic communication service. In case an operator/service provider is offering VoIP to end-users, the provisions of personal data protection and privacy from Chapter XII of the ECA-1 would apply.

Other communication services such as Skype, Io, Viber, WhatsApp, etc. are characterised as unmanaged VoIP and are not considered to be an electronic communication service but rather an information society service based on internet. Such a service is therefore excluded from the scope of the ECA-1, but falls within the provision of the Personal Data Protection Act which governs general data protection. The same goes with webmail and location based services (so far they have been considered as information society services). However, if the main focus of above mentioned services would be the transmission of the signals over an electronic communications network and not the content, such service could be recognized as an electronic communication service.

The answer obviously lies in interpretation of the definition of electronic communication service which according to the ECA-1 excludes “...information society services that do not include, wholly or mainly, the transmission of signals on electronic communications networks”. We are not aware of any formal decisions of competent authorities on this problem. So far there were also no court disputes decided over the delimitation between electronic communication services and information society services this mater.
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

**Slovenia:**

The ECA-1 is applicable on the territory of the Republic of Slovenia, which means that any natural person or legal entity acting on the territory of Slovenia shall respect its provisions. This is especially true when it comes to the question of supervision and compliance. Any breach of Slovenian legislation on the territory of Slovenia is remedied by the Slovenian enforcement authorities regardless of the origin of the person who is committing a breach. The supervisory procedure is conducted by the Agency for Communication Networks and Services (AKOS) and Information Commissioner in accordance with provisions of the ECA-1.

The ECA-1 provides an instrument for dealing with cross-border issues in the form of cross border dispute resolution procedures. There are no other instruments provided in the ECA-1.

So far we are not familiar with any cases where the ECA-1 would be applied to a foreign network operator or service provider. Operators which provide publicly available electronic communication services within the Slovenian territory usually establish a daughter company with its seat in Slovenia. Such company has its own legal personality and is therefore considered as a Slovenian subject.

As provisions of the ECA-1 regarding unsolicited commercial communications (see art. 158) are applicable to any legal or natural persons offering their products/services by the means of direct marketing, a cross-border situation could easily happen. By example, if a foreign seller sent a (commercial) email without prior consent to the Slovenian customer, that would constitute a breach of art. 158(1) ECA-1. However, in such case the problem of *locus delicti* would be raised (i.e. was the breach committed in the place of the seller or in the place of the consumer?) putting in question the jurisdiction of Slovenian authorities. It seems that provisions of the ECA-1 do not give a sufficient answer to that question.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:
### Slovenia:

**a. National Enforcement Authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)**

AKOS may issue non-binding recommendations as part of its regulatory competencies. The recommendations are published on their website. AKOS may in the course of auditing the security measures taken by operators regarding their networks also issue recommendations regarding best practices concerning the level of security which those measures should achieve (art. 145, para. 5).

AKOS has not issued any such recommendations on the field of the privacy or other activities addressed by the provisions of the ePrivacy Directive.

AKOS participates in several projects managed by NGOs which provide guidance and empower consumers/users in the field of e-privacy:

- **Safe Internet Center Slovenia** is the national project promoting and ensuring a better and safer internet for children (http://safe.si/en/center/safer-internet-centre). It consists of three components: Awareness Centre Safe.si, Helpline »Tom telefon« and hotline »Spletno oko«.

- **“Varni na internetu” (Safe Internet)** is a project which aims to enhance safety on internet. It deals with many aspects of net security (fraud, online shopping, antivirus protection, phishing), among others also with SPAM and privacy on internet (https://www.varninainternetu.si/kdo-smo).

According to art. 49 of the Personal Data Protection Act, the Information Commissioner may issue non-binding opinions, clarifications and positions on issues in the area of protection of personal data, and publish them on the website or in another appropriate manner. The Information Commissioner may also issue non-binding instructions and recommendations regarding protection of personal data.

Regarding the provisions of the ePrivacy Directive, the Information Commissioner has so far published a recommendation on cookies (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_uporabi_piskotkov.pdf) and a recommendation on privacy in cloud computing (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Mnenje_o_racunalnistvu_v_oblaku_in_delovni_dokument_t_glede_zavezujocih_poslovnih_pravil za pogodbene obdelovalce.pdf).

It has also published many opinions/answers to questions regarding data retention and other privacy issues in electronic communications. However, it has not published any opinion regarding the interpretation and/or application of the terms such as “networks”, “services” and “providers” from ePrivacy Directive.

**b. National Courts through rendering of case law**

We are not familiar with any court decisions on the interpretation of legal provisions of ECA-1 regarding the scope of definitions of network, service or provider. There are some decisions of the Constitutional Court, but the interpretation of the Court does not depart from the provisions of the ECA-1 (e.g. in case Up-106/05 from 2.10.2008 the Court interpreted that ‘traffic data’ is part of ‘communication’, which is in line with the art. 147 ECA-1).
7. What is your individual view of:
   a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?
   b. possible improvements of the effectiveness of this legal framework.

<table>
<thead>
<tr>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>As the national legislation has been changed a lot, there is sometimes confusion regarding the meaning and the use of different articles. Additionally, some issues are regulated in several laws at the same time (e.g. unsolicited communication, which is covered in ECA-1, the Consumer Protection Act and the Electronic Commerce Act). There has also been a change in competence: according to the previous ECA, AKOS was competent for supervising the provisions regarding nuisance calls, under new ECA-1 this has become a competence of the Information Commissioner.</td>
</tr>
<tr>
<td>In some parts, the rules in the ECA-1 are too general. The reason for that mainly lies in the style of transposition of the ePrivacy Directive by which rules are often only copied into the national legislation without any further elaboration. In addition, rules implemented in the ECA-1 seem to be fragmented as the same topics are regulated in different articles (e.g. unsolicited phone calls are partly regulated in the article on directories (art. 150/3) and partly in the provisions regarding unsolicited communication (art. 158)).</td>
</tr>
<tr>
<td>There is also an issue regarding cross border cooperation. The ECA-1 lacks any provisions which would enable AKOS to adopt measures to ensure effective cross-border cooperation. In this regard the enforcement of the national laws adopted pursuant to the ePrivacy Directive and the creation of harmonised conditions for the provision of services involving cross-border data flows could be difficult.</td>
</tr>
</tbody>
</table>
### B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

**Slovenia:**

Confidentiality of communications from art. 5.1 of the ePrivacy Directive is implemented in ECA-1 art. 147, para 5, which prohibits any kind of surveillance or interception of communications by third parties, such as listening, tapping, recording, retention and forwarding of the communications without the consent of the users concerned. Confidentiality of communications refers to any kind of electronic communication services (e.g. fax, email, voicemail, SMS, MMS, inbox etc.).

However, the ECA-1 prohibits recording and retention of communications also by the user without obtaining the prior consent of other participants of the communications, if such processing is not usual and where the participants do not expect it (art. 147(6)). This provision would, by example, prohibit recording of phone call without a consent of other party, as it is not a common practice to record the private phone calls. On the other hand, recording of SMSs or emails on terminal equipment is quite usual practice and should be expected by the sender, therefore such recording is allowed.

The ECA-1 defines the term communication as “...any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This shall not include any information conveyed as part of a broadcasting service to the public over an electronic communications network, except to the extent that the information can be related to an identifiable subscriber or user receiving the information.” (art. 3 para 27). This definition entirely corresponds to the definition in the ePrivacy Directive.

Confidentiality of communications relates to:

1. the content of communications;
2. traffic and location data relating to the communications referred to in the previous point;
3. the facts and circumstances relating to the interruption of the connection or the connection not being established.

The ECA-1 in art. 147(5) explicitly provides four exceptions to confidentiality:

- recording/retaining communication in relation technical storage which is necessary for the conveyance of specific publicly available communications (art. 147(3,4))
- supplying data regarding location of a mobile communications device to the police on its written request in case of missing person and saving lives (art. 153)
- lawful interception of communication (art. 160). Conditions and scope of lawful interception is prescribed in Criminal Proceedings Act (art. 150) and in Slovenian Security Agency Act (art. 24)
- data retention (ECA-1, art. 162 to 168). Slovenian Constitutional Court, following the recent judgement of CJEU, annulled the provisions of ECA-1 art. 162 to 168 in its decision from 3.7.2014
2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn’t affect “legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

**Slovenia:**

The provision on the recording of communication for the purpose of lawful business practice (5.2 of the ePrivacy Directive) is implemented in the ECA-1 art. 147 para 7 and 8:

“ (7) Without prejudice to the provisions of the fifth paragraph of this Article, the recording of communications and related traffic data shall be permitted in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication, on condition that the parties to the communication are notified in advance of the recording, its purpose and the period of retention of the recording (e.g. automated answering machines). The recorded communication must be erased as soon as possible and, in any case, no later than by the end of the period during which the transaction can be lawfully challenged.

(8) The notification of recording must be given via the same medium and in the same form as the recorded communication.”

The law stipulates that the recording of phone calls (or any other communication) and related traffic data is allowed if:

- it is conducted in course of business communication
- it is necessary for providing evidence of commercial transaction
- the parties involved in communication receive a prior notification, which must be given in the same medium as the communication itself. This notification should provide at least following information:
  - a) that the communication is being recorded
  - b) the purpose of recording
  - c) the period of the retention of recorded communication

The recorded communication must be erased as soon as possible but in any case at the end of the period in which the transaction can be legally challenged.

In this respect, Slovenian legislation does not significantly depart from the provisions of the ePrivacy Directive. However, the ECA-1 provides some additional legal basis for recording of communications (art. 147/9 ECA-1). Besides the exceptions for business, the recording of communication and acquisition of the related data is also allowed to certain state bodies and organisations competent for intelligence, security, protection, defence, law enforcement (police) and rescue. In this case, the calling user* must be notified and informed on the purpose of such recording and the duration of retention.

Any other state bodies may record the content of communications under the same conditions if legal basis is provided in any other law. For example, such exemption is provided in the Court Act, which allows recording of the phone calls to the courts.

*Although the law explicitly uses term “calling” user, it cannot be interpreted in such way, that it is limited only to the phone calls. The scope of art. 147 is broader and includes any type of communication. However, the majority of such recording will happen in connection to phone calls.
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

Slovenia:
Besides the exceptions provide in the ECA-1 (described above) we are not familiar with any other law allowing exceptions to the confidentiality principle set in the ePrivacy Directive.
4.
a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:
- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?
b. Is there any other important legislation with regard to the protection of private electronic communications?

**Slovenia:**
a) There are no special legal provisions in the ECA-1 regarding automated breaches of confidentiality. Whether committed with or without human intervention the breach is regarded the same way.

- MAC address is considered as a personal data of a user and not data which is related to the terminal equipment (opinion of the Information Commissioner no. 0712-14/2013 from 28.3.2013; [http://bit.ly/155XKHT](http://bit.ly/155XKHT)). Any unlawful processing of a MAC address would therefore constitute a breach of confidentiality. However, in its opinion from 27.11.2013, the Information Commissioner is of the opinion that automated processing of MAC address without a prior consent of user could be allowed for the purpose of aggregated and anonymised statistics about the presence of a specific MAC address in a given area at a given time, but only if certain conditions are met ([https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=2325&cHash=04f4ad2284f511cfbc6db33bf243b21d](https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=2325&cHash=04f4ad2284f511cfbc6db33bf243b21d)).

- According to ECA-1 (art. 147, para 5) all forms of interception of communications by third parties, such as “... listening, tapping, recording, retention and forwarding of the communications...”, without the consent of the users concerned are prohibited. In this extent, capturing of content from non-encrypted networks would constitute a breach of confidentiality. However, regarding the question whether such act would be punishable, the answer depends on whether the person who intercepted the content, acted with intent: If he/she was intentionally intercepting or trying to intercept the content (and other conditions from criminal legislation are met) than such act would constitute an offence or even a criminal act. On the other hand, if a third party coincidently captures the content transmitted over non-encrypted network it would be very hard to regard it as a crime.

- ECA-1 (art. 147, para. 1) explicitly provides that the confidentiality of communications applies to:
  1. the content of communications;
  2. traffic and location data relating to the communications
  3. all data and circumstances relating to the interruption of the connection or the connection not being established
In this context, the Slovenian law does not distinguish between protection of content and related data. Both are treated the same way. However, there are some additional rules in ECA-1 which additionally deal with the traffic data and location data other than traffic data (see art. 151 and 152 of ECA-1).
b) On a general level, confidentiality of communication is protected by the Constitution of the Republic of Slovenia. The Constitution in Article 37 guarantees the protection of secrecy of correspondence, whereby the term "other means" includes also the correspondence in electronic communication (e.g. mobile telephony, internet). The second paragraph of Article 37 stipulates that only the law may prescribe that under a court order for a certain period of time the confidentiality of correspondence may be suspended, if this is necessary for the conducting of criminal proceedings or for security of the country. The right to privacy provided in Article 37 connects with a right to protection of personal data under Article 38 of the Constitution.

There are also some criminal acts, which can be related with the infringement of the privacy in electronic communications. In this regard the Criminal Code of the Republic of Slovenia (OG RS no. 55/2008)* incriminates following actions:

Unlawful Eavesdropping and Sound Recording (art. 137, para 1):
> Whoever unlawfully eavesdrops on or records a private conversation or statement by use of special devices, or whoever directly transmits such a conversation or statement to a third person or otherwise directly allows him to learn of such a conversation or statement shall be punished by a fine or sentenced to imprisonment for not more than one year.

Violation of Secrecy of Means of Communication (art. 139, para 2):
> The following shall be punished by a fine or by imprisonment for not more than one year:
> ...
> 2) whoever, by use of technical instruments, learns of the content of a message transmitted by telephone or any other means of electronic telecommunication;

Attack on Information Systems (art. 221, para 1):
> (1) Whoever breaks into an information system, or illegally intercepts data during a non-public transmission into or from the information system, shall be sentenced to imprisonment for not more than one year.

When it comes to the scope of criminal legislation, one should bear in mind that above mentioned provisions refer to any natural person (under certain circumstances also to any legal person) and not only to operators/service providers.

*The Criminal Code in English is available at the following link: [www.wipo.int/clea/en/details.jsp?id=6074](http://www.wipo.int/clea/en/details.jsp?id=6074)
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:
   a. the scope and substance of your national implementation
   b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

**Slovenia:**
The ePrivacy Directive provisions on cookies have been transposed in art. 157 of ECA-1. The deadline for harmonisation was set to five months, so the new rules came into force on 15.6.2013. The law provides the following:

(1) The retention of information or the gaining of access to information stored in a subscriber’s or user’s terminal equipment shall be permitted only on condition that the subscriber or user gives their consent thereto, after having been given clear and comprehensive information in advance about the information manager and the purpose of the processing of this information, in accordance with the act governing personal data protection.

(2) Without prejudice to the provisions of the preceding paragraph, the technical retention of information or access to this data may be permitted exclusively for the purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

(3) If technically feasible, effective and in accordance with the act governing personal data protection, a user may also signal the consent referred to in the first paragraph of this Article by using appropriate settings in a browser or other applications. The consent of a user or subscriber shall mean personal consent in accordance with the act governing personal data protection.

(4) The provisions of this Act shall be applied in the case of a violation of the rules on informing a individual and acquiring his consent as referred to in the first paragraph of this Article and in the case of a violation of the act governing personal data protection.

(5) Inspection and supervision of the implementation of the provisions of this Article shall be carried out by the Information Commissioner.

The ECA-1 now stipulates an opt-in regime with informed consent of the user/subscriber (see art. 157, para 1). This means that cookies may be installed on terminal equipment if:
- the user/subscriber agrees with such installation
- all necessary information relating processing of data were offered prior of such installation.
- the information should be given in clear and comprehensive manner. In this regard the ECA-1 refers to the Personal Data Protection Act, which provides further guidance on how the consent of the user can be given and on the elements of the notice given by data controller.

However, the consent of the user can be given also implicitly (art. 157(3)). The ECA-1 allows that consent may be given by the settings of a browser or other applications, but only if it is technically possible. According to the Guidelines on cookies, issued by the Information Commissioner ([https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/](https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/)), currently no browser or application is sufficiently advanced to allow such implicit consent, because they are all using opt-out regimes (page 14).

b. The ECA-1 applies equally to all cookies or any other technologies that enable data storage or gaining of access to information stored in the terminal equipment of a subscriber/user. In this
regard, there is no difference between certain types of cookies or between terminal equipment on which they are stored. However, the law distinguishes between cookies where the prior consent is necessary and those where it is not. Article 157(2) provides two exceptions from obtaining user’s consent prior to installation of cookies:

1) cookies that are needed solely for the transfer of communication on an electronic communications network, and
2) cookies, which are necessary to ensure the information society service, which has been explicitly requested by the subscriber/user.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

**Slovenia:**
As already described above, when it comes to consent, the ECA-1 in art. 157(1) refers to the Personal Data Protection Act. In this respect two provisions of the Personal Data Protection Act are relevant:

<table>
<thead>
<tr>
<th>Article</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td>Personal consent of an individual – is a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and this is given on the basis of information that must be provided to such individual by the data controller pursuant to this Act; personal consent of an individual may be written, oral or some other appropriate consent of the individual.</td>
</tr>
<tr>
<td>15.</td>
<td>Written consent of the individual - is the signed consent of the individual having the form of a document, the provision of a contract, the provision of an order, an appendix to an application or other form in accordance with statute; a signature shall also mean on the basis of a statute a form equivalent to a signature given by means of telecommunication and a form equivalent by statute to a signature given by an individual who does not know how to write or is unable to write.</td>
</tr>
<tr>
<td>16.</td>
<td>Oral or other appropriate consent of the individual - is consent given orally or by means of telecommunication or other appropriate means or in some other appropriate manner from which it can be concluded unambiguously that the individual has given his consent.</td>
</tr>
</tbody>
</table>

Article 19 provides obligations on the data controller regarding the information which needs to be communicated to user/subscriber before obtaining his consent:

1. If personal data are collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information, if the individual is not yet acquainted with them:
   - data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),
   - the purpose of the processing of personal data.

It needs to be mentioned that the consent is not perpetual. According to the Guidelines on cookies, subscriber/user should always have an option to withdraw the given consent (p.18).

**Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)?**

Law does not explicitly require use of pop-up screens or consent bars for providing information to the user prior to obtaining his consent. However, it is not enough to provide information implicitly...
(e.g. somewhere in the Privacy Policy or in General Terms) or to assume that the user has got the information simply because he visited a particular web page. Information on cookies should be presented to user in the visible spot, for example where he is asked for his consent. In Guidelines on cookies (p. 16) Information Commissioner recommends pop-ups, consent bars or other similar techniques (e.g. splash screens) as one of the most suitable options. Additional guidance on how to present the information is published in Information Commissioner Guidelines (https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/).

**How are the rules applied in relation to mobile devices? Does this depend on cookie types?**
There are no special rules regarding the device type. The law does not distinguish between installation of cookies on mobile devices and on other devices.

**Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?**
A cookie may be loaded on user’s terminal equipment only after his/her consent has been given. Without the consent only cookies that fall under exceptions (e.g. session cookies) can be installed.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g., language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

**Slovenia:**

ECA-1 in art. 157(2) entirely follows the provisions of ePrivacy Directive regarding the exceptions to the consent rule:

> (2) Without prejudice to the provisions of the preceding paragraph, the technical retention of information or access to this data may be permitted exclusively for the purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

The first exception relates only to cookies necessary for transmitting a message (i.e., without which the message in a communications network would not be transferred). This exception should be interpreted narrowly: cookies which only allow a faster transmission of message or better management of the transmission do not fall under this exception.

The second exception relates to cookies without which the user would not be able to receive a service he/she explicitly requested. The term "necessary" is again to be interpreted narrowly – without the installation of such cookie, the requested service cannot be performed. The argument that the cookie ensures better performance of certain features of the site or that a cookie is "very important" is not enough. The exception is only allowed if (i) user actively requested certain service (e.g., by clicking on a certain location, a certain selection, setup, etc.) and (ii) the cookie is necessary in order to carry out his request.

The ECA-1 does not define in detail what type of cookies satisfies the above exceptions. In practice, the Guidelines on cookies and the opinion of the WP 29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf) are used in this manner. According to above mentioned Information Commissioner’s Guidelines the following cookies fall under the consent exemption:
- cookies which are used to ensure that the website remembers user input in web forms, online shopping etc. (shopping cart cookies)
- cookies for authentication of the user, by example in connection with online banking services where the user enters his username and password (authentication cookies)
- cookies which ensure the proper flow of information between servers and endpoints (load balancing).
- cookies which allow playback of multimedia content and are necessary in order to play video or audio content on the web (flash cookies)
- cookies which allow different Websites to integrate products of social networks into their content (social plug-in content sharing cookies)

It seems that the Guidelines on cookies are more in favor of exceptions in the case of cookies with a
shorter durability (e.g. session cookies). For permanent cookies or cookies with longer durability, additional justification is required to prove the existence of exemption. It is also easier to allow the consent exception if the 1st party cookies are in question than in case of cookies of third parties.

Finally, if the website analyzes behavior with their own cookies, such analytical cookies do not constitute a disproportionate interference with the privacy of users. The same goes if the website uses cookies of a contract partner who does not use the collected data for his own purpose (Opinion of the Information Commissioner, no. 0000 from 19.04.2013)
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?
Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?
Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

Slovenia:

Compliance and enforcement of provisions on cookies is the competence of the Information Commissioner.

Enforcement of the cookie provision only began in June 2013 when the ECA-1 came into force. By the end of 2013 the Information Commissioner received complaints against a high number of websites (141), mostly due to inadequate or missing notifications on the use of cookies. In most instances the operators acted in line with the guidelines and remedied the situation after being notified by the Commissioner.


No infringement decisions have been issued yet. The websites providers have been cooperative in most of the cases; a number of procedures are still ongoing.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

<table>
<thead>
<tr>
<th>a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. national courts through rendering of case law</td>
</tr>
</tbody>
</table>

**Slovenia:**

a. As the Information Commissioner is the competent authority for supervision of the implementation of article 157 ECA-1, it is the sole authority which adopts guidelines and opinions on cookies.

So far, the Information Commissioner has adopted following guidelines which are connected to cookies:


Regarding the implementation of legislation, there are also several opinions available, which were adopted by the Information Commissioner (in Slovenian language only):

1. Predlog implementacije piškotkov SOZ - MOSS (no. 0712-1/2013/3578 from 27.09.2013)
2. Piškotki, privolitev (no. 0712-1/2012/1925 from 24.05.2013)
3. Implementacija pravil glede piškotkov na spletnih straneh (no. 0712-1/2013/1562 from 23.04.2013)
4. Nova zakonodaja o piškotkih (no. 0000 from 19.04.2013)
5. Stališče Informacijskega pooblaščenca glede uvajanja nove opredelitve psevdonimnih podatkov v predlagani reformi varstva osebnih podatkov v EU (no. 007-17/2013 from 05.03.2013)

b. There aren’t any court decisions interpreting legal provisions regarding the cookies and applying them to concrete situations.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

Although the provision has been criticized by businesses for imposing an additional burden and impeding smooth online transactions, there is a general consensus that the new rules on cookies have enhanced the privacy of users/subscribers. However, the Chamber of Commerce published some statistics that after new rules on cookies have been implemented the visit of webpages decreased by 15% and the revenues from online shopping has fallen for 10% (http://www.gzs.si/slo/skupne_naloge/stalisca_in_komentari/stalisca_gzs/61958).

From the perspective of legal certainty, one would expect to have more explicit rules set in the law. As we described above, many provisions (e.g. Consent exemptions) can be implemented only through “soft law” of the Information Commissioner which gives further guidance on e.g. types of cookies.
C. Traffic data

<table>
<thead>
<tr>
<th>1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slovenia:</td>
</tr>
<tr>
<td>Rules regarding traffic data are transposed in the ECA-1 (art. 151)</td>
</tr>
<tr>
<td>The term “traffic data” is defined in art. 3, para. 45, which provides that the term shall mean “…any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.”</td>
</tr>
<tr>
<td>In this respect, national legislation entirely follows provisions of art. 2 of the ePrivacy Directive.</td>
</tr>
</tbody>
</table>
2. What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects

<table>
<thead>
<tr>
<th>Slovenia:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ECA-1 (Art. 151) provides the following rules:</td>
</tr>
<tr>
<td>(1) Traffic data relating to subscribers and users processed and retained by an operator must be erased or made anonymous as soon as it is no longer needed for the purpose of the transmission of a communication, except in the cases of data for which a longer period of retention is defined under this Act with regard to internal procedures (Article 149), the supply of traffic and location data for the protection of life and limb (Article 153), the tracing of malicious or nuisance calls (Article 155), the lawful interception of communications (fifth paragraph of Article 160) and obligations ensuing from the chapter of this Act on the retention of data (Articles 162 to 168).</td>
</tr>
<tr>
<td>(2) Without prejudice to the provision of the preceding paragraph, an operator may, until complete payment for a service is made but no later than by the expiry of the limitation period, retain and process traffic data required for the purposes of calculation and of payment relating to interconnection.</td>
</tr>
<tr>
<td>(3) For the purpose of marketing electronic communications services or for the provision of value-added services, the provider of a publicly available electronic communications service may process the data referred to in the first paragraph of this Article to the extent and for the duration necessary for such services or marketing, but only if the subscriber or user to whom the data relates has given his prior consent. Subscribers or users must be informed, prior to giving consent, of the types of traffic data which are processed and of the purpose and duration of such processing. A user or subscriber shall have the right to withdraw their consent at any time.</td>
</tr>
<tr>
<td>(4) For the purposes referred to in the second paragraph of this Article, and in order to inform subscribers and users, a service provider must state in the general terms and conditions which traffic data will be processed and the duration of that processing.</td>
</tr>
<tr>
<td>(5) Traffic data may only be processed under the previous paragraphs of this Article by persons acting under the authority of an operator and handling billing or traffic management, responding to customer enquiries, detecting fraud, marketing electronic communications services or providing a value-added service, where this processing must be restricted to what is necessary for the purposes of such activities.</td>
</tr>
<tr>
<td>(6) Without prejudice to the provisions of the first, second, third and fifth paragraphs of this Article, an operator shall send traffic data to the Agency or a competent body if they so request in order to settle disputes, in particular interconnection or billing disputes, in accordance with the applicable legislation.</td>
</tr>
</tbody>
</table>

According to above described rules, traffic data may be processed (beside being processed for the purposes required by the law such as lawful interception or data retention) only for the purpose of:
1. billing and interconnection payments
2. marketing of electronic communication services or value added services

**Legal requirements:**
AD1 Operator (i.e. service provider or/and network operator) may process traffic data only until the complete payment of a service but no later than by the expiry of the period during which the bill
may lawfully be challenged. Additionally, the user/subscriber should be informed which traffic data will be processed and the duration of that processing (this information should be provided through the General Terms of operator/service provider). However, no consent of user/subscriber is needed.

AD2 Service provider may process traffic data only to the extent and for the duration necessary for providing VAS services or marketing of electronic communication services. The service provider should obtain prior consent of the user/subscriber and should have right to withdraw it at any time. The user/subscriber should be informed, prior to giving consent, of the types of traffic data which are processed and of the purpose and duration of such processing.

However, the operator or service provider should also respect any other provisions provided in national legislation (such as those provided in the general data protection legislation etc.).

Provisions of the ECA-1 are following those provided in the ePrivacy Directive. The only difference is that Slovenian law requires that the information on processing of traffic data regarding the billing should be stated in the General Terms of a service provider (there is no such requirement in the ePrivacy Directive).

3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>Slovenia:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ECA-1 requires that traffic data relating to subscribers and users processed and retained by an operator must be erased or made anonymous as soon as it is no longer needed for the purpose of the transmission of a communication (art. 151 (1)).</td>
</tr>
</tbody>
</table>
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

We are not familiar with any such cases in Slovenia.
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

Slovenia:
There have been no significant problems on implementation of rules regarding traffic data in practice so far. It seems that the rules are sufficiently clear and logical.

For clarity and legal certainty reasons it would be recommendable that art. 151(2) ECA-1 would refer to an exhaustive list of traffic data which can be processed by operators\(^7\). However, one must understand that due to constant technological development/improvement such list could be soon out of date. That’s probably why this definition is left to the service providers who determine which traffic data to be processed and for how long.

From the most recent decision of the Constitutional Court, which annulled national rules on data retention (art. 162-168 of the ECA-1) and ordered operators to erase all the data, questions have been raised whether law enforcement agencies could have access to traffic data gathered for billing purposes. The ECA-1 does not explicitly prohibit such access, although this might infringe the general data protection rules, which stipulate that data obtained for a certain purpose may not be further processed in any manner incompatible with that purpose. In this respect, one would expect more clear legal provisions.

---

\(^7\) The law provides:

(2) Without prejudice to the provision of the preceding paragraph, an operator may, until complete payment for a service is made but no later than by the expiry of the limitation period, retain and process traffic data required for the purposes of calculation and of payment relating to interconnection.
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

| Slovenia: |
| Rules regarding location data traffic are transposed in the ECA-1 (art. 152). |

The term location data is defined in art. 3, para. 44, which provides that the term shall mean “…any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service.”

In this regard, Slovenian legislation entirely follows the provisions of art. 2 of the ePrivacy Directive.

Besides and in addition to the rules of the ePrivacy Directive, the ECA-1 in art. 153 requires that the operator should supply certain data to the authorities in case of missing persons. In this context, the law refers to data which is necessary to establish the most recent location of a mobile communications device. This data is defined in a following way: “…data on the location codes (Cell ID) at the start of the communication and data determining the geographical location of cells, with an indication of their location codes (Cell ID), during the period for which it is retained, data on the communication, and other data processed by the operator in personal and other databases and enabling a more precise determination of the most recent whereabouts of an individual’s mobile communications device.” (art. 153, para 3)
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Slovenia:
The ECA-1 (Art. 152) is worded as follows:

(1) Location data other than traffic data relating to users or subscribers may only be processed when it is made anonymous, or with the prior consent of the users or subscribers, to the extent and for the duration necessary for the purposes of providing the value-added service. A user or subscriber may withdraw this consent at any time.
(2) A user or subscriber must be informed, prior to issuing the data processing consent referred to in the preceding paragraph, of:
1. the possibility of refusing consent;
2. the type of data to be processed;
3. the purpose and duration of processing;
4. the possibility of the transmission of this location data to a third party for the purpose of providing the value-added service.
(3) A user or subscriber that has consented to the processing of the data referred to in the first paragraph of this Article shall have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.
(4) The data referred to in the first paragraph of this Article may only be processed under the previous paragraphs of this Article by persons acting under the authority of an operator or by a third party providing the value-added service, where this processing must be restricted to what is necessary for the purposes of providing the value-added service.
(5) In accordance with the third paragraph of Article 134 of this Act, an operator must supply the location data referred to in the first paragraph of this Article to the competent body in relation to calls to the single European emergency call number ‘112’ and the police number ‘113’ even where a user or subscriber has temporarily refused the processing of the data referred to in the first paragraph of this Article or has not given his consent to its processing.
(6) The provisions of the first to fourth paragraphs of this Article shall not be applied to location data other than traffic data for which this Act stipulates mandatory retention.

Above provisions of the ECA-1 almost entirely correspond to art. 9 of the ePrivacy Directive.

However, the law has an additional provision, which requires that the operator (i.e. service provider and/or network operator) provides location data of user’s equipment to the authorities in case of emergency phone calls (112) or phone calls to the police (113). There is also a provision suspending the rules in case of mandatory data retention: in such case location data may be processed without requirements provided by the art 152, but should follow the rules regarding data retention instead.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

<table>
<thead>
<tr>
<th>Slovenia:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In principle, location data should always be made anonymous, except in case of (i) a consent given by the user regarding the provision of VAS or (ii) when law requires/allows processing of such data for lawful purposes (e.g. data retention)</td>
</tr>
</tbody>
</table>

There is no legal requirement to delete location data in the ECA-1. The data should only be made anonymous.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)
b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

a. So far, AKOS has not adopted any guidelines/recommendations, opinions or decisions regarding the interpretation of location data.

There are some opinions of the Information Commissioner available which refer to location data:
1. Lokacijski podatki zavarovanca, ki jih od mobilnega operaterja želi pridobiti zavarovalnica (no. 0712-7/2007/2 form 19.1.2007)

In both opinions the Information Commissioner provided additional guidance on which data may be considered as a location data (e.g. the direction of travel, geographical altitude, etc.). The Information Commissioner mainly follows the wording of preamble to the ePrivacy Directive, which lists location data.

b. We are not aware of any court cases with regard to application of location data in practice.
5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

In the past there has been a lot of criticism that rules regarding location data has been too strict (e.g. in case of missing person it was not possible to get information on location of the user although there was an emergency situation). With the amendments to ECA in 2007 (now art. 153) this obstacle has been removed and rules on supplying data to the police in the emergency situation have been introduced.

For the purpose of legal certainty, it would be advisable to specify which types of (location) data fall under the provisions of art. 152.
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:
   a. the scope and substance of your national implementation
   b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

Slovenia:

a. Provisions of art. 13 of the ePrivacy Directive have been transposed to Slovenian legislation by the ECA-1. Article 158 provides as follows:

(1) The use of automated calling and communication systems to make calls to subscribers’ telephone numbers without human intervention (e.g. automatic calling machines, SMS, MMS), facsimile machines or electronic mail for the purposes of direct marketing shall be allowed only on the basis of a subscriber’s or user’s prior consent.

(2) Without prejudice to the provisions of the preceding paragraph, a natural person or legal entity that obtains from a purchaser of its products or services their electronic mail address may use that address for the direct marketing of its own similar products or services, on condition it gives that customers the clear and distinct opportunity to refuse, free of charge and straightforwardly, the use of their electronic mail address at the time of the collection of these contact details, and on the occasion of every message in the event that the customer has not initially refused such use.

(3) The use of means of direct marketing using electronic communications (e.g. voice calls) other than those laid down in the previous two paragraphs of this Article shall be permitted only with the consent of the subscriber or user. The refusal of consent must be free of charge for a subscriber or user.

(4) The first and third paragraphs of this Article shall be applied to subscribers that are natural persons.

(5) The sending of electronic mail for the purposes of direct marketing which, contrary to the act governing electronic commerce in the market, disguises or conceals the identity of the sender on whose behalf the message is sent, or without a valid address to which the recipient may send a request that such direct marketing cease, shall be prohibited. The sending of electronic mail for the purposes of direct marketing that invites recipients to visit websites that contravene the above-mentioned act shall also be prohibited.

(6) The provisions of this Act shall be applied in cases where commercial communications are sent by electronic mail contrary to the provisions of this Article and they also constitute unsolicited electronic mail under the act governing consumer protection. The provisions of this Act shall also be applied in cases where commercial communications are sent by electronic mail contrary to the provisions of this Article and they also constitute unsolicited electronic mail under the act governing electronic commerce in the market.

(7) Without prejudice to any supervisory procedure occasioned by a breach of the provisions of this Article, any natural person or legal entity that has suffered damage by the breach, as well as any service provider seeking to protect its business interests and the interests of its customers, shall have a legal interest in filing a civil action or interim order against the person committing a breach of the provisions of this Article.
The ECA-1 mainly follows the wording of the ePrivacy Directive. In article 158(1) the law prohibits use of any kind of automated systems, FAX or email for the purpose of direct marketing, without obtaining the consent of user/subscriber (opt-in regime). As it comes to already established commercial contacts with user/subscriber, the ECA-1 allows use of email for direct marketing without prior consent of user/subscriber, but only for other similar products or services. Nevertheless, user/subscriber should have an option to reject such email at any time and free of charge (art. 158/2).

Regarding the unsolicited communications other than those from article 1 and 2 of the ePrivacy Directive, the ECA-1 provides opt-in regime. Such communication is permitted only with the consent of the user/subscriber.

Regarding the beneficiaries, the ECA-1 in article 158(3) follows the wording of ePrivacy Directive, limiting the scope of legislation only to natural persons. From the “commitment” perspective, obligations provided in article 158 should refer to any natural or legal person who performs direct marketing and not only to network operators or providers of electronic communication services.

In relation to other legislation, the ECA-1 in article 158(6) provides supremacy over the act governing consumer protection and the act governing electronic commerce in the market. In case an email is sent contrary to the provisions of these two acts and at the same time also contrary to the provisions of the ECA-1, the provisions of the ECA-1 shall apply.

When it comes to the provision of article 13(5) of the ePrivacy Directive, it seems that ECA-1 lacks the specific rules that would protect the legitimate interests of subscribers other than natural persons with regard to unsolicited communications. There are also no provisions on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of provisions of the ECA-1 regarding the unsolicited communications.

Regarding unsolicited direct marketing, the ECA-1 in part where it deals with directories (art. 150, para. 3) provides an additional option for a subscriber to prohibit certain phone calls by putting a mark in a directory (some sort of “Do not call” list):

“(3) Subscribers must be given the opportunity to prohibit the use of their personal data for calls with a commercial or research purpose. A subscriber may prohibit the use of his personal data for both or one of the above purposes upon entry in the directory or at any time subsequently. The issuer of a directory must clearly mark the prohibition applying to the use of a subscriber’s personal data for a particular purpose in the directory...”
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

**Slovenia:**
For the purposes of direct marketing, the use of:
- automated calling and communication systems without human intervention (e.g. automatic calling machines, SMS, MMS),
- facsimile machines or
- electronic mail
is allowed only on the basis of a subscriber’s or user’s **prior consent**. The same requirement is prescribed also for any other means of communication as Slovenian legislator decided to implement provisions of art. 13(3) of the ePrivacy Directive in such way that opt-in regime is required. The law further provides that the refusal of such consent must be free of charge for a subscriber/user.

The only exception to the above described rules is provided in article 158(2) od the ECA-1: the law allows sending commercial emails without the consent of the user if the address has been obtained in previous business contact and if it is used for marketing similar products and services.

In case of emails, the law requires transparent and fair treatment. In this sense, an email which (i) disguises or conceals the identity of the sender on whose behalf the message is sent or (ii) does not have a valid address to which the recipient may send a request that such direct marketing cease, is prohibited. The sending of electronic mail for the purposes of direct marketing that invites recipients to visit websites that contravene the above-mentioned act is also prohibited (see article 158(5) of the ECA-1).

Regarding the phone calls with commercial and research purposes: such calls are only allowed to the phone numbers of those subscribers who haven’t put a limitation in the public directory (art. 150(3) of the ECA-1). However, in practice there may be confusion as several versions of the directory exist which are not updated simultaneously.
3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

**Slovenia:**
The only exception to opt-in regime is provided for in paragraph 2 of article 158 ECA-1:

The email for the purpose of direct marketing may be sent if the sender:
- has obtained user’s/subscriber’s electronic mail address through previous commercial/business relations (for example user has purchased a product or service)
- uses email for offering similar products or services to those already purchased,
- gives user/subscriber an option to refuse, in a simple way and free of charge, the use of his electronic mail address. This option should be given at (i) the time of the collection of contact details, and (ii) in any email the user/subscriber receives.

It should be stressed that these rules refer only to email and not to any other means of direct marketing (such as automated calling and communication systems without human intervention or fax machines).
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

Generally, the ECA-1 (nor any other law) does not distinguish between different communication channels. In case of each of above mentioned communication channels, two conditions should be met to consider such communication lawful:
- the sender must obtain the prior consent of each recipient,
- the recipient should have the right to withdraw the given consent at any time.

However, three things should be brought to attention:
- for emails sent in the context of already established business contact the law does not require consent (see answer to q. 3)
- the law prohibits phone calls which have commercial or research purpose, if a subscriber has put a “do not call” mark in phone directory (ECA-1, art. 150, para. 3)
- in case of any communication channels other than those provided for in art. 158, para. 1 (i.e. automated calling and communication systems to make calls to subscribers’ telephone numbers without human intervention (e.g. automatic calling machines, SMS, MMS), facsimile machines or electronic mail) the law explicitly provides, that the withdrawal of the consent should be free of charge (ECA-1, art. 158, para. 3)
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

Slovenia:

a. AKOS has adopted several decisions regarding unsolicited direct marketing communications. In most cases the plaintiffs argued that the sender of email/SMS did not get their prior consent, which eventually proved not to be true and the cases were dismissed. Therefore, no guidance on application of the law was given in these cases. Neither has AKOS adopted any recommendations or opinions regarding the interpretation of unsolicited direct marketing communications.

The Ministry for education, science, culture and sport of the Republic of Slovenia on 10.9.2013 adopted a non-binding opinion no. 029-44/2010/169 in which it interpreted the scope of beneficiaries under the provisions of article 158 ECA-1. The Ministry is of the opinion that natural persons, who perform a business activity (a sole trader) and receives a commercial email within his/her business activity, does not enjoy the protection provided for in article 158.

On the other hand, there are numerous opinions of the Information Commissioner which refer to the different aspects of direct marketing communications. It should be mentioned that the Information Commissioner deals with unsolicited communication only from the general data protection perspective. Opinions (in Slovenian language only) are available on its webpage (https://www.ip-rs.si/hc/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odloche-in-mnenja-varstvo-osebnih-podatkov/):

In some of its opinions (e.g. Izvajanje raziskav in neposredno trženje po elektronski pošti) the Information Commissioner explicitly stressed the difference between commercial emails and email which are unsolicited, but have no commercial purpose. As for the latter, they only fall under the provisions of article 72 of Personal Data Protection Act, which requires lawful consent for the processing of personal data: if data controller has processed address of the user without consent, such processing is considered as an infringement of PDPA. There are also opinions on conditions which need to be met for the lawfulness of the consent (eg. Mnenje glede veljavnih oblik privolitve).

The Information Commissioner in its opinions made clear that the provisions of the ECA-1 regarding the unsolicited communication are applicable only in case of natural persons. It is therefore not contrary to the law if the email address of a legal person/private company has been used for direct marketing (e.g. Neposredno trženje po elektronski pošti).

There is also a case reported in which a private company had been sending commercial SMSs to users without having their prior consent. The Information Commissioner issued a supervisory decision in which the offender was ordered to erase from his database all phone numbers obtained without the consent of subscribers (eg. SMS za neposredno trženje).

b. No such case law is available at the moment.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

**Slovenia:**

The rules on unsolicited communications are fragmented. Although the majority of rules are provided in the ECA-1, three additional acts are also applicable: the Electronic Commerce Act, the Personal Data protection Act and the Consumer Protection Act. In practice there has been some confusion in application of the provisions. In many events more than one authority seemed to be competent to handle the case.

There have been proposals to the Ministry from AKOS, the IP and Market Inspectorate to codify all the rules in one single act, but so far unsuccessfully. It seems that the problem lies in the fact that the above mentioned acts are implementing different directives (besides ePrivacy Directive also e-Commerce Directive and Data Protection Directive) each one with its special provisions.

Provisions on fines (art. 235(14) are not precise enough as they refer only to subscriber and not to subscriber and user: “...use electronic communications for direct marketing without the subscriber’s prior consent (first or third paragraph of Article 158)*;” In case the receiving party of unsolicited communication is a user (and not subscriber) such inconsistency would probably prevent imposing fines on the sender.

*please note that unofficial English translation of the ECA-1 wrongly uses word “user” instead of a “subscriber”*
For the Study

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Under the assignment of the European Commission

Directorate General CONNECT

SMART 2013/0071

By: Ian Lloyd, Ian Lloyd Legal Services Ltd.

Date: 17 August 2014
Contents

Part 1: Management summary ........................................................................................................3
Part 2: Answers to the questionnaire .............................................................................................4
Part 1: Management summary

**Management Summary for the United Kingdom**

- The e-Privacy Directive has been transposed into UK Law principally through the Privacy and Electronic Communications (EC Directive) 2003. These were modified in 2011 to take account of changes to European legislation adopted in 2009. Also very relevant are provisions of the Communications Act 2003 that contains definitions of key concepts such as traffic and location data and the Electronic Commerce Act 2000. All sectoral legislation has also to be read in conjunction with the general rules established under the Data protection Act 1998.

- Responsibility for enforcement of the legislation lies principally with the Information Commissioner. Under the terms of a memorandum of an agreement between OFCOM and the Information Commissioner, OFCOM’s role is limited to providing technical assistance when this is sought by the Information Commissioner in the course of specific investigations. A number of other regulators have a more peripheral impact on the topics. The Financial Conduct Authority, for example, can impose financial penalties on financial organisations which make fraudulent use of SMS to sell financial products.

- The United Kingdom has transposed all the specified articles of the Directive into domestic law. In many respects it has expanded definitions although this appears to give specific examples of activities that are covered by the more general definitions adopted in the Directive. One consequence is that the United Kingdom implementing legislation is significantly longer than the text of the Directive. In one area there does appear to be some uncertainty regarding conformity with the Directive. Following a judicial decision it appears that monetary penalties may be imposed on organisations whose infringing conduct causes ‘substantial damage or distress’ to those receiving unsolicited commercial communications. This appears a higher threshold for liability than that set out in Directive 95/46.

- A problematic area of application concerns the application of the legislation to cookies and similar devices. A number of criticisms have been expressed centring on the notion of consent and the extent to which this can be a viable proposition especially in the context of what might be regarded as legacy websites. There is concern that the Directive attempts to retrofit data protection measures into a technical environment where they may not be effective.

- In respect of the handling of traffic and location data the legislation seems to be working reasonably well but there is a tension between the periods of time for which retention of this data might be permitted under data protection principles and the retention requirements introduced under the data retention Directive and now continued in the United Kingdom by the Data retention and Investigatory Powers Act 2014.
Part 2: Answers to the questionnaire

A. Implementing legislation: identification of the laws and their scope

1. Through which legislation was the ePrivacy Directive transposed in your national legislation? Please provide a short history of the transposition, indicating:

- the full title of the law in English
- the short title of the law in English
- the URL linking to the text of the implementing legislation (if available)

Please also fill out the concordance table indicating for each relevant provision of the Directive the corresponding national transposition. Where necessary, please subdivide per subject (as done in the case of Belgium below)

Directive 2002/58/EC was transposed into UK Law by the Privacy and Electronic Communications (EC Directive) Regulations 2003. These entered into force on 11 December 2003. These apply to all parts of the United Kingdom. Following changes introduced in the 2009 EU reforms, the 2003 Regulations were amended by the Privacy and Electronic Communications (EC Directive) (Amendment ) Regulations 2011. These entered into force on 26 May 2011.

In addition to these specific regulations, there is always also the requirement to comply with the provisions of the general Data Protection Act 1998, in particular the requirements that processing be fair and lawful. The Electronic Commerce (EC Directive) Regulations 2002 also contain provisions relating to unsolicited electronic communications.

Concordance table

<table>
<thead>
<tr>
<th>ePrivacy Directive</th>
<th>Transposed into national law by:</th>
<th>URL</th>
</tr>
</thead>
</table>

utm_source=eshot&utm_medium=email&utm_campaign=Regulations%20on%20
<table>
<thead>
<tr>
<th>Article</th>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
</table>
Electronic Communications (EC Directive)(Amendment) Regulations 2011 | website%20cookies


|-----------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------|

2. Which enforcement authority (ies) is/are responsible for supervision of the national provisions transposing the ePrivacy Directive? (e.g. the national telecoms regulator, the national data protection authority, the ombudsman, etc.)

For each authority please provide in the table below:

- a. the full name in your national language
- b. the English translation of the short name
- c. the part or the provision(s) of the ePrivacy Directive it supervises
- d. URL link to website

<table>
<thead>
<tr>
<th>Full name of the authority</th>
<th>English translation of the short name</th>
<th>The part or provision(s) it supervises</th>
<th>URL link to website</th>
</tr>
</thead>
</table>

6
<table>
<thead>
<tr>
<th>The Office of the Information Commissioner</th>
<th>ICO</th>
<th>All</th>
<th><a href="http://www.ico.gov.uk">www.ico.gov.uk</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Office of Communications</td>
<td>OFCOM</td>
<td>All</td>
<td><a href="http://www.ofcom.org.uk">www.ofcom.org.uk</a></td>
</tr>
<tr>
<td>The Financial Conduct Authority</td>
<td>FCA</td>
<td>Regulation 13</td>
<td><a href="http://www.fca.org.uk/">http://www.fca.org.uk/</a></td>
</tr>
</tbody>
</table>

Explanation:

Under UK statutes, the Information Commissioner and the Office of Communications have equal responsibilities for enforcement of the e-privacy legislation. By virtue of a memorandum of understanding between the regulators it has been determined that the Information Commissioner – who has responsibility for enforcement of the Data Protection Act 1998 - will assume prime responsibility for the enforcement of the legislation whilst OFCOM will provide any necessary technical assistance within the telecommunications sector.

Ofcom is the independent regulator of the UK communications industries. It is responsible for, among other things, regulating advertising and programme content on television and in on-demand services falling under UK jurisdiction. These services include those receivable in other Member States of the European Union. Co-regulators have been designated by Ofcom for the regulation of advertising on television and in on-demand services (the Advertising Standards Authority), for example, will regulate that sector of activity and programme content in on-demand services (the Authority for Television on Demand).

In areas not subject to co-regulation, Ofcom itself handles complaints about television services which fall under UK jurisdiction (and therefore hold a licence granted by Ofcom) but which are receivable in other Member States of the European Union.

In addition to actions that may be taken by the Information Commissioner, a range of sectoral statutory and non-statutory agencies may also have significant roles to play. The Financial Conduct Authority (http://www.fca.org.uk/) is the supervisory agency for that sector and it, and its predecessor, the Financial Services Authority, have levied very significant fines on companies that
have been found to breach data security requirements.

The FCA is also empowered to act if an SMS is sent to a consumer offering debt management services.

A further cause of problems in the UK has been the use of SMS by claims management companies seeking to persuade recipients to use their services in order to claim (frequently fraudulently) compensation following a road accident. Where such an SMS is sent concerning an accident claim, a report may be made to the Ministry of Justice’s Claims Management Regulator. They will also need to know the date, time, message and the number it was sent from. The website can be found at https://www.claimsregulation.gov.uk/index.aspx.

Subscribers and users of electronic communications services and networks can also address complaints to the Ombudsman for Telecommunications (www.ombudstelecom.be).
3. How does the implementing legislation define the networks, services and providers which fall within its scope? Is the scope of the legislation different from the ePrivacy Directive, and if so, how?

The 2003 Regulations adopt without modification the definitions of electronic communications networks and services found in the Communications Act 2003. This defines them in section 32 in the following terms:

“(1) In this Act “electronic communications network” means—

(a) a transmission system for the conveyance, by the use of electrical, magnetic or electromagnetic energy, of signals of any description; and

(b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—

(i) apparatus comprised in the system;

(ii) apparatus used for the switching or routing of the signals; and

(iii) software and stored data.”

This definition differs in terminology and structure from that found in the Authorisation Directive in particular by not giving the specific examples found in the Directive, such as the explicit statement that Internet traffic is covered. By providing that the definition extends to the transmission ‘of signals of any description’, it does seem that it will produce the same effect in practice.

In respect of electronic communications services, the UK Communications Act provides, again in section 32, that:

“(2) In this Act “electronic communications service” means a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service.”

The term ‘content service’ is defined in the following terms:

“In subsection (2) “a content service” means so much of any service as consists in one or both of the following—

(a) the provision of material with a view to its being comprised in signals conveyed by means of an electronic communications network;

(b) the exercise of editorial control over the contents of signals conveyed by means of a such a network.”
This definition also differs from that found in the Directive. It is very much shorter and in some respects broader. It does not, for example provide that services be normally provided for remuneration. The major reason for the variations is that the Communications Act, unlike the relevant Directives, does regulate significant elements of broadcasting and content.
There has been considerable interest regarding the treatment of over the top services such as VOIP. In December 2007 OFCOM published a statement <http://stakeholders.ofcom.org.uk/binaries/consultations/voip/statement/voipstatement.pdf> setting out aspects of its policy towards the regulation of VOIP services and in particular the requirement that users be allowed to access the emergency services. These will be subject to regulation subject to the following conditions:

1.25 Firstly, we have excluded “Click to Call” services. They are a form of VoIP service that may be selected on a web-site or other application by a user and connect the user only to a number or a limited set of numbers pre-selected by the provider or a user.

1.26 Secondly, the requirement now relates to services that allow calls to national numbers (and not national and international numbers). That means it covers services that allow calls to national or to national and international numbers, to ensure that services that allow calls to national numbers only are caught by the requirement and to exclude services that allow calls to international numbers only.

One of the major contents of the regulation is that users are to be made aware of the fact that access to emergency services may not be available in the event of a power failure. Whilst any network may suffer from outages, the General Conditions of Entitlement that apply to more traditional networks require that services should be maintained in the event of a failure in the public electricity supply.

In 2004 a code of practice regarding the use of location data was introduced by the mobile network operators. The current version was adopted in 2006 (>http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf<) It defines location services as either ‘active’ or ‘passive’. Active services are initiated by the user – for example a request for directions to the nearest cash machine. Passive services are more contentious and relates to the location of a mobile user by a third party. An example might be a parent seeking to locate a mobile phone. This imposes restrictions on the uses that may be made of location data by mobile services although there is no formal legal document that specifies these. The key element is a requirement that the user should consent on an ongoing basis to the tracking of the mobile device. This raises some difficult issues in the increasingly common situation where children have mobile phones. It is not clear when and to what extent children may give valid consent to such actions.

There are no specific provisions relating to the use of webmail services although these did attract considerable publicity in a case where is was alleged that a Government minister was using such
services to communicate with his advisers so as to bypass normal rules relating to Ministerial communications and also the requirements of freedom of information legislation (allowing individuals to obtain copies of official communications) (See <http://www.theregister.co.uk/2011/09/29/does_gove_email_policy_breach_data_protection_act/>).
5. How is the territorial scope of the implementing legislation defined? How does national law deal with cross-border situations (ex. a breach from an entity established in your country that affects individuals residing in different Member States or the other way around)? Specifically, are there circumstances where the legislation can affect operators outside of the national territory, and are there any examples where the law has been applied to foreign entities?

By way of example: have there been cases where your national law has been applied to a foreign entity?

Any network operators seeking to provide services to UK customers will be liable to notify details of their operations to OFCOM. They will inevitably be required to have physical assets in the United Kingdom and will be subject to the jurisdiction of the regulators.

The situation is more complex when electronic communications service providers are involved. There will not be the same need to have physical assets in the United Kingdom and the implementing regulations make no mention of jurisdictional issues. It is made clear in regulation 4 that the regulations do not impact upon a party’s responsibility to comply with the general Data Protection Act.

6. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on the (scoping of) definitions mentioned in this section:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law

a. The Communications Act provides in section 33 that

“(1) A person shall not—
(a) provide a designated electronic communications network,
(b) provide a designated electronic communications service, or
(c) make available a designated associated facility,

unless, before beginning to provide it or to make it available, he has given a notification to OFCOM of his intention to provide that network or service, or to make that facility available.”
An electronic communications network, electronic communications service or associated facility is designated for the purposes of this section if it is of a description of networks, services or facilities that is for the time being designated by OFCOM as a description of networks, services or facilities for which notification under this section is required”.

The General Conditions of Entitlement issued and maintained by OFCOM specify all requirements that must be met by any party providing a publicly available communications network or service (as defined in the Communications Act and restated in the general conditions.). There has been discussion regarding the situation where services can be considered to be made available to the public. An example given concerns the provision of communications services within a closed environment such as a prison.

- a) the provision of electronic communication services to third parties;
- b) the provision of electronic communication networks, electronic communication services and network access to communication providers;
- or
- c) the making available of associated facilities to communication providers.

The concept of designated operator is essentially linked to the requirement to pay administrative charges (the successor to licence fees) to OFCOM in respect of the costs incurred in regulating the sector. The current designation is found in an OFCOM <http://stakeholders.ofcom.org.uk/binaries/consultations/designation/statement/statement.pdf>. This provides that notification requirements will be imposed on any:

- any Electronic Communications Network, Electronic Communications Service or Associated Facility where the person providing that Network or Service, or making available that Associated Facility had a Relevant Turnover from Relevant Activities of £5 million or more in the last but one calendar year prior to the charging year in question.

b. There have not been any court decisions relating to these definitions.
7. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<table>
<thead>
<tr>
<th>a.</th>
<th>There do not appear to have been significant regulatory issues with the definitions and no significant privacy implications have been identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>The distinction between public electronic communications networks and information society services is becoming blurred with, for example, Internet based services offering ‘click to connect’ services where a user who clicks on a marked button will establish a VOIP connection. The issue is more one for communications regulation generally than privacy in particular, but it might be appropriate to align more closely electronic communications definitions and those relating to information society services.</td>
</tr>
</tbody>
</table>
B. Confidentiality obligations

1. How was the principle of confidentiality of communications and the related traffic data (article 5.1 of the ePrivacy Directive) implemented? Please identify the relevant laws and their general scope. Is there a definition of ‘communications’ under this legislation? If so, how is it formulated?

The relevant UK legislation in this field is the Regulation of Investigatory Powers Act 2000. This Act draws a distinction between the interception of content data and traffic data. This has become contentious in the context of recent revelations about the scale of on-line monitoring undertaken by national security agencies as the safeguards relating to the nature and extent of obtaining traffic data are significantly less stringent than those applying to content data.

(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—

... (b) a public telecommunication system.

Breach of the provision constitutes a criminal offence that can be punished with a term of imprisonment of up to 2 years. As indicated above, the offence is committed only when a party acts intentionally.

Issues have arisen when messages are in the course of communication over a public telecommunications system. It has been held, for example, that interception between a wireless telephone handset and its base station do not fall within this definition.

The term ‘communication’ is defined in section 81 of the Act as including ‘anything comprising speech, music, sounds, visual images or data of any description;’. Also included are ‘signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus’. This would encompass all elements of a communication including traffic data.

2. Article 5.2 of the ePrivacy Directive states that the provision of Art. 5.1 doesn't affect “legally authorised recording of communications and the related traffic data when carried out in the
course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.” Please describe the transposition and substance of this exception in your national legislations

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 were enacted to permit conduct that would otherwise have been prohibited under the Regulation of Investigatory Powers Act 2000. This statute is currently the major UK statute providing for the lawful interception of communications. The regulations provide that:

“3. (1) For the purpose of section 1(5)(a) of the Act (providing for regulations to be made specifying circumstances under which interception of communications will be authorised), conduct is authorised, subject to paragraphs (2) and (3) below, if it consists of interception of a communication, in the course of its transmission by means of a telecommunication system, which is effected by or with the express or implied consent of the system controller for the purpose of—

(a) monitoring or keeping a record of communications—

(i) in order to—

(aa) establish the existence of facts, or

(bb) ascertain compliance with regulatory or self-regulatory practices or procedures which are—

• applicable to the system controller in the carrying on of his business or

• applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures, or

(cc) ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties, or

(ii) in the interests of national security, or

(iii) for the purpose of preventing or detecting crime, or

(iv) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system, or

(v) where that is undertaken—

(aa) in order to secure, or

(bb) as an inherent part of,
the effective operation of the system (including any monitoring or keeping of a record which would be authorised by section 3(3) of the Act if the conditions in paragraphs (a) and (b) thereof were satisfied); or

(b) monitoring communications for the purpose of determining whether they are communications relevant to the system controller’s business which fall within regulation 2(b)(i) above; or

(c) monitoring communications made to a confidential voice-telephony counselling or support service which is free of charge (other than the cost, if any, of making a telephone call) and operated in such a way that users may remain anonymous if they so choose.

(2) Conduct is authorised by paragraph (1) of this regulation only if—

(a) the interception in question is effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller’s business;

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business;

(c) the system controller has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted; and

(d) in a case falling within—

(i) paragraph (1)(a)(ii) above, the person by or on whose behalf the interception is effected is a person specified in section 6(2)(a) to (i) of the Act;

(ii) paragraph (1)(b) above, the communication is one which is intended to be received (whether or not it has been actually received) by a person using the telecommunication system in question.

(3) Conduct falling within paragraph (1)(a)(i) above is authorised only to the extent that Article 5 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(4) so permits. “
3. Does any legislation or known case law in your country define other exceptions to the confidentiality principle, particularly in light of Article 15(1) of the ePrivacy Directive? Please identify the relevant laws and describe their general scope.

The main exceptions to the confidentiality principle are found in the Regulation of Investigatory Powers Act and also to some extent the provisions of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 described above.

The Regulation of Investigatory Powers Act provides in section 2 that:

“Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which, or which that person has reasonable grounds for believing, is both—

(a) a communication sent by a person who has consented to the interception; and

(b) a communication the intended recipient of which has so consented.”

It continues to provide that interception of communications is legitimate where it is authorised by the operator of a communications network and is conducted:

“for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.”

Section 2 also sanctions interception where this takes place in connection with attempts to detect and prevent unauthorised use of wireless telegraphy.

The Act also contains provisions in section 5 whereby a warrant may be issued by the Secretary of State authorising interception where this is considered to be necessary:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting serious crime;

(c) for the purpose of safeguarding the economic well-being of the United Kingdom;
4.

a. How does your legislation address automated breaches of confidentiality without human involvement, and specifically:

- Whether the interception of MAC addresses would entail breach of confidentiality;
- Whether the non-consent based capturing of payload (content) data from unencrypted Wi-Fi networks would constitute a breach of confidentiality;
- Does your national law distinguish between the protection of content of the communications and other data relating to communications (i.e. traffic data)?

b. Is there any other important legislation with regard to the protection of private electronic communications?

a. This form of conduct will principally be dealt with under the terms of the Computer Misuse Act 1990. This provides in section 1 that is an offence (punishable by up to 5 years imprisonment) to programs or data held on any computer system. Also relevant are the provisions of section 125 of the Communications Act 2003 that criminalise the dishonest obtaining of access to an electronic communications system with the intent to avoid charges that would normally be payable. The requirement that there be an intent to avoid payment will limit the scope of this provision but prosecutions have successfully been brought against persons who have sought to make unauthorised use of Wi-Fi networks.

As indicated above, the legal protection afforded to content data is significantly greater than that applying to traffic data. Interception of content data requires the approval of a judge whereas consent to the accessing of traffic data may be granted by a senior police officer.

b. Amendments were made to the Regulation of Investigatory Powers Act 2000 following the decision of the European Court of Human Rights in the case of Halford v. UK. This held that a breach of Article 8 rights had been committed when a police authority intercepted telephone calls made by one of its staff using an internal telecommunications network. The Act now provides in section 2 that:

> Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either—

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private
telecommunication system.”
5. As to cookies and spyware as mentioned in article 5.3 of the Directive, please describe:

a. the scope and substance of your national implementation

b. whether your legislation makes any distinction between types of cookies (e.g. first party - third party; persistent cookies - flash cookies - supercookies - evercookies - etc), and/or between the type of device (e.g. general computers, mobile phones, tablets)?

a. Regulation 6 of the Privacy and Electronic Communications (EC Directive) 2003 as amended in 2011 provides that:

“1) Subject to paragraph (4), a person shall not [store or] gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment—

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

[(b) has given his or her consent].

(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.

[(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.]

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information—

(a) for the sole purpose of carrying out . . . the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.”

The Information Commissioner has published an extensive guidance note on the operation of the new provisions. The major problem area, it suggests, is to modify existing systems to cope with the new requirements:

Implementing these rules requires considerable work in the short term but compliance
will get significantly easier with time. The initial effort is where the challenge lies—
auditing of cookies, resolving problems with reliance on cookies built into existing systems
and websites, making sure the information provided to users is clear and putting in place
specific measures to obtain consent. This work takes place in the context of limited
consumer awareness and understanding of what cookies do. In time a number of factors
are likely to make compliance much more straightforward. New sites and systems and
upgrades to existing systems can be designed to facilitate compliance with the rules,
those operating websites will be more aware about how they choose to use cookies and
enhanced browser options will increasingly allow websites to rely on browser settings to
help to satisfy themselves they have consent to set cookies.²

While the Commissioner indicates that obtaining explicit consent to the use of cookies from users
would secure “regulatory certainty” the guidance note states:

“Early reporting on the new rule led some to believe that an explicit, opt-in style
consent would be required for every cookie each time it was set. The Information
Commissioner’s guidance made it clear that although an explicit opt-in mechanism
might provide regulatory certainty it was not the only means of gaining consent. In
some circumstances those seeking consent might consider implied consent as an
option that was perhaps more practical than the explicit opt-in model.

... consent (whether it is implied or express) has to be a freely given, specific and
informed indication of the individual’s wishes. For implied consent to work there has
to be some action taken by the consenting individual from which their consent can be
inferred. This might for example be visiting a website, moving from one page to
another or clicking on a particular button. The key point, however, is that when taking
this action the individual has to have a reasonable understanding that by doing so
they are agreeing to cookies being set”.³

One approach that is widely used is to display a message on the opening screen of a
website indicating that cookies are being used, giving a general description of their
purpose and indicating that if the user proceeds to use the site further, consent to
their use will be assumed.

b. The legislation does not differentiate between different forms of cookie. In his Guidance,
however, the Information Commissioner states that the nature of a cookie is a factor that will be

² At pp.3–4.
³ At pp.6–7.
taken into account in determining whether an individual has given consent to the use of a cookie or similar device.
6. How is the informed consent rule implemented in national law? Is there a requirement in the law to use e.g. pop-up screens or consent bars? Are there rules or practices on which information needs to be provided (other than the information specified in general data protection law)? How are the rules applied in relation to mobile devices? Does this depend on cookie types? Does the law allow the setting up of cookies before individuals have provided consent (i.e., the cookie is set immediately when loading a page)?

The legislation makes no specific reference to this point. The Information Commissioner has, however, issued guidance in the following terms:

http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx

in the following terms:

“Much of the debate around the so-called “consent for cookies” rule has focussed on the nature of the consent required for compliance. Implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices. While explicit consent might allow for regulatory certainty and might be the most appropriate way to comply in some circumstances this does not mean that implied consent cannot be compliant. Website operators need to remember that where their activities result in the collection of sensitive personal data such as information about an identifiable individual’s health then data protection law might require them to obtain explicit consent.”

Whilst the Commissioner indicates that explicit consent might increase ‘regulatory certainty’, the view is taken that – very much in line with the UK approach under general data protection law – implied, sometimes referred to as opt out consent will suffice subject to the requirement that the individuals concerned are given appropriate notice of the proposal to insert a cookie.
7. How are the exceptions to the informed consent rule implemented in national law? Specifically, the ePrivacy Directive permits Member States not to require consent i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (ii) when strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. How are these exceptions applied with respect to cookies? Are e.g. language cookies, shopping cart cookies, or analytics cookies excluded or treated differently?

Regulation 6(4) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 provides that consent to the use of cookies is not required when they are used:

(a) for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

The use of the words ‘sole’ and ‘strictly’ in the above provisions will limit their applicability. The Information Commissioner has issued the following guidance:

<table>
<thead>
<tr>
<th>Activities likely to fall within the exception</th>
<th>Activities unlikely to fall within the exception</th>
</tr>
</thead>
<tbody>
<tr>
<td>A cookie used to remember the goods a user wishes to buy when they proceed to the checkout or add goods to their shopping basket</td>
<td>Cookies used for analytical purposes to count the number of unique visits to a website for example</td>
</tr>
<tr>
<td>Certain cookies providing security that is essential to comply with the security requirements of the seventh data protection principle for an activity the user has requested – for example in connection with online banking services</td>
<td>First and third party advertising cookies</td>
</tr>
<tr>
<td>Some cookies help ensure that the content of your page loads quickly and effectively by distributing the workload across numerous computers.</td>
<td>Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored</td>
</tr>
</tbody>
</table>
8. How would you assess compliance and enforcement of cookies rules? What are the ways of obtaining consent in practice?

Are there statistics on compliance? Have there been any enforcement actions against violations of the rules (either against individual violations, or through broader enforcement actions)?

Are there any data, statistics or surveys on users’ views (e.g. satisfaction surveys (even simple news, articles, etc.), what percentage of users refuse or accept cookies, once information and choice has been provided?)

The implementation of the new legislation has been complex and rather contentious. The Privacy and Electronic Communications (EC Directive (Amendment) Regulations amended existing rules in order to implement the 2009 Directives but the Information Commissioner indicated that he would not seek to enforce these for 12 months.

A number of studies have been conducted by the consultancy firm KPMG and have been widely reported in the computer press. In the first study conducted in 2011 it was estimated that only 2% of web sites complied with the regulations. By 2013 the figure had risen to 50%.

To date there have not been any enforcement actions brought. A significant issue for the United Kingdom may be the number of foreign web sites (especially from the United States) that are accessed in English by United Kingdom citizens. Except in the situation where these have some physical assets in the United kingdom, they are not subject to action by the UK authorities.
9. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on these questions provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law


Although not legally binding, given that the Information Commissioner is responsible for enforcing the legislation, it is unlikely that an alternative approach would be taken

b. There have been no court cases to date.
10. What is your individual view of:

a. the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

b. possible improvements of the effectiveness of this legal framework.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>The implementation of the legislation has been problematic. A major difficulty is the requirement to obtain consent. In many cases this a false option. If an individual wishes to buy a plane ticket from an airline the choice may well be between accepting a cookie or doing without the flight. It might be argued, of course, that it has always been the case that the individual cannot in practice negotiate terms and conditions with many commercial providers.</td>
</tr>
<tr>
<td>B.</td>
<td>There is perhaps need for greater clarity regarding the nature of the cookies that are to be enabled with users given a choice what level of cookie they wish to accept. Someone wishing to make a casual visit to a site might be willing to accept a sessional or short term cookie rather than one of potentially indeterminate duration. It might also be a requirement to make information readily available to assist users in deleting cookies from their computers.</td>
</tr>
</tbody>
</table>
### C. Traffic data

1. In which legislation is traffic data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

<table>
<thead>
<tr>
<th>The definition is found in the Privacy and Electronic Communications (EC Directive) Regulations 2003. These provide in regulation 2 that traffic data constitutes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>“any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication;”</td>
</tr>
</tbody>
</table>

This definition is rather more expansive than that provided for in the Directive but does not appear to be inconsistent with its provisions.
2. **What are the legal requirements for the lawful processing of traffic data and/or for providing traffic data services? Please indicate whether this is different from the definition provided in the Directive and in what respects**

Under the 2003 Regulations the term ‘traffic data’ is defined as

“...any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication”

In terms of the processing of traffic data, the Information Commissioner has advised [link](http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/traffic_data) Traffic data may be processed only for the restricted purposes outlined in the Regulations.

- **To provide value-added services to the subscriber or user**
  A value-added service means any service that requires the processing of traffic data or ‘location data’ beyond what is necessary to transmit a communication or the billing of that communication – for example, a service that locates the driver of a broken-down vehicle. There is no restriction on the type of service that can be provided, but such processing may only take place with the prior consent of the subscriber or user.

- **To market the service provider’s own electronic communications services**
  Under the Regulations, the service provider must get the consent of the subscriber or user before they can market their own electronic communications services. Such marketing does not necessarily have to be carried out over the phone and might include, for example, an analysis of a subscriber’s usage patterns to provide that subscriber with the best tariff available.

Only the communications provider or a person acting under their authority can carry out this processing. The communications provider has ultimate responsibility for complying with the Regulations about processing traffic data, so they should observe the requirements of the [seventh data protection principle](#) (relating to the requirement that data be held securely). The provisions about contracts are particularly relevant – see the seventh data protection principle. Although the Act applies only to processing personal data, there is nothing to stop service providers imposing such contracts for processing traffic data relating to corporate subscribers.
3. Are there any legal requirements to anonymise or delete traffic data, and if so, under which conditions?

The Data Protection Act requires that personal data shall not be retained for longer than is necessary for the purpose for which it was obtained. Regulation 7 of the Privacy and Electronic Communications (EC Directive provides that:

"7. (1) Subject to paragraphs (2) and (3), traffic data relating to subscribers or users which are processed and stored by a public communications provider shall, when no longer required for the purpose of the transmission of a communication, be—

(a) erased;

(b) in the case of an individual, modified so that they cease to constitute personal data of that subscriber or user; or

(c) in the case of a corporate subscriber, modified so that they cease to be data that would be personal data if that subscriber was an individual.

(2) Traffic data held by a public communications provider for purposes connected with the payment of charges by a subscriber or in respect of interconnection payments may be processed and stored by that provider until the time specified in paragraph (5).

(3) Traffic data relating to a subscriber or user may be processed and stored by a provider of a public electronic communications service if—

(a) such processing and storage are for the purpose of marketing electronic communications services, or for the provision of value added services to that subscriber or user; and

(b) the subscriber or user to whom the traffic data relate has given his consent to such processing or storage; and

(c) such processing and storage are undertaken only for the duration necessary for the purposes specified in subparagraph (a).

(4) Where a user or subscriber has given his consent in accordance with paragraph (3), he shall be able to withdraw it at any time.

(5) The time referred to in paragraph (2) is the end of the period during which legal proceedings may be brought in respect of payments due or alleged to be due or, where such proceedings are brought within that period, the time when those proceedings are
finally determined.

(6) Legal proceedings shall not be taken to be finally determined—

(a) until the conclusion of the ordinary period during which an appeal may be brought by either party (excluding any possibility of an extension of that period, whether by order of a court or otherwise), if no appeal is brought within that period; or

(b) if an appeal is brought, until the conclusion of that appeal.”
4. Are you aware of any cases where traffic data rules have been applied against specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

There have been no cases concerned specifically with traffic data under the e-privacy directive but there have been issues regarding the extent of traffic and, perhaps more significantly location, data that must be supplied in connection with a subject access requests. There is also guidance from the Information Commissioner regarding the length of time for which traffic data may be retained (apart from retention for law enforcement purposes) The advice is

Data required by the communications network or service provider to calculate the subscriber’s bill or for interconnection charges can only be retained until the end of the period during which the bill may lawfully be challenged or payment pursued. In terms of contract law, this would normally mean a limitation period of six years plus appeals applied. However, in the Commissioner’s view, this provision merely permits such data to be kept only when circumstances require it, for example, if the bill is challenged during a period when a communications network or service provider would normally retain the data for their own billing purposes. It does not permit the wholesale retention of such traffic data in every case. <http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/traffic_data>
5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

<table>
<thead>
<tr>
<th>5. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is an uneasy relationship between the general principles of data protection law applying to traffic data and provisions regarding data retention for national security and law enforcement purposes. Following the decision of the European Court of Justice regarding the data retention Directive, the UK adopted (following less than a day’s discussion in Parliament) the Data Retention and Investigatory Powers Act that provides a legal basis for continued retention of communications data.</td>
</tr>
</tbody>
</table>
D. Location data

1. In which legislation is location data defined, and how? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Privacy and Electronic Communications (EC Directive) Regulations define location data as

“any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—

(f) the latitude, longitude or altitude of the terminal equipment;

(g) the direction of travel of the user; or

(h) the time the location information was recorded; “

This appears to be a more detailed formulation than that applied in the Directive but is compatible with its provisions.
2. What are the legal requirements for the lawful processing of location data and/or for providing location data services? Please indicate whether this is different from the definition provided in the Directive and in what respects. Does this provision apply also to third parties which harvest the data from users’ devices, usually when they download applications?

Regulation 14 of the Privacy and Electronic Communications (EC Directive) 2003 provides that:

“(2) Location data relating to a user or subscriber of a public electronic communications network or a public electronic communications service may only be processed—

(a) where that user or subscriber cannot be identified from such data; or
(b) where necessary for the provision of a value added service, with the consent of that user or subscriber.

(3) Prior to obtaining the consent of the user or subscriber under paragraph (2)(b), the public communications provider in question must provide the following information to the user or subscriber to whom the data relate—

(a) the types of location data that will be processed;
(b) the purposes and duration of the processing of those data; and
(c) whether the data will be transmitted to a third party for the purpose of providing the value added service.

(4) A user or subscriber who has given his consent to the processing of data under paragraph (2)(b) shall—

(a) be able to withdraw such consent at any time, and
(b) in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and free of charge.

(5) Processing of location data in accordance with this regulation shall—

(a) only be carried out by—
(i) the public communications provider in question;
(ii) the third party providing the value added service in question; or
(iii) a person acting under the authority of a person falling within (i) or (ii); and
(b) where the processing is carried out for the purposes of the provision of a value added service, be restricted to what is necessary for those purposes.”

As will be seen, third party processing is permitted in connection with the provision of value added services subject to the consent of the subscriber or user. As is frequently the case with implementation of European Directives, the United Kingdom government chose to add some additional elements to the definitions but these do not appear to alter in any way the substance of
the original provisions. This practice has been the cause of criticism from the courts which tend increasingly to rely on the text of Directives rather than UK implementing measures.
3. Are there any legal requirements to anonymise or delete location data, and if so, under which conditions?

There are no specific provisions relating to the anonymisation of location data. The Data Protection Act requires that data shall not be retained for longer than is necessary for the purpose for which it was collected. Subject again to the rules relating to data retention, this would suggest that the period of retention in a form where the subscriber or user can be identified should be short. The Information Commissioner has produced a Code of Practice [http://ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf] on Anonymisation that provides general guidance on practices and procedures in this area.
4. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on ‘location data rules’ provided by:

   a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

   b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

   a. Guidance concerning the requirements relating to the processing of location data has been published by the Information Commissioner <http://ico.org.uk/for_organisations/privacy_and電子通訊/the_guide/location_data>. This focuses on the need to notify the subscriber of the processing that will take place and, especially where it is proposed to transfer the data to a third party, to obtain consent to this

   b. To date there have been no court or tribunal decisions on this aspect of the legislation.
<table>
<thead>
<tr>
<th>5. What is your individual view of: the effectiveness of these rules in practice, i.e. do you consider them to be clear, logically consistent and appropriate to protecting privacy within your country?</th>
</tr>
</thead>
<tbody>
<tr>
<td>In general there have been few issues concerning the application of the rules regarding location data. The emerging issue is the growing use of over the top services such as ‘Find my Friends’. The proliferation of these services raises questions regarding user consent and will also result in a more widespread and possibly less well controlled use of location data.</td>
</tr>
</tbody>
</table>
E. Unsolicited commercial communications

1. As to ‘unsolicited direct marketing communications’ (as dealt with in article 13 of the ePrivacy Directive) please describe:

a. the scope and substance of your national implementation

b. flag up any differences in comparison to the scope and substance thereof in the ePrivacy Directive (if any), e.g.: are the national provisions entirely in line with the Directive? Do they use the same terminology? Are they more or less extensive? Are they more precise on certain points? Etc.

a. The regulation of unsolicited commercial communications have featured in United Kingdom law and practice for many years. In most cases there has been a preference for industry self regulation with systems such as the mailing and telephone preference services that allow users the opportunity to opt out of receiving such communications. Compliance with such schemes has been somewhat patchy. The Privacy and Electronic Communications (EC Directive) put some aspects on a more legalistic footing and contain extensive provisions relating to unsolicited electronic communications whether by way of telephone call, SMS or email.

The Regulations initially make provision for automated telephone calls:

19.—(1) A person shall neither transmit, nor instigate the transmission of, communications comprising recorded matter for direct marketing purposes by means of an automated calling system except in the circumstances referred to in paragraph (2).

(2) Those circumstances are where the called line is that of a subscriber who has previously notified the caller that for the time being he consents to such communications being sent by, or at the instigation of, the caller on that line.

This provision will be discussed further below. A further issue which is at the interface of the relationship between the role of the Information Commissioner (who has prime responsibility in the field) and OFCOM which is responsible for more technical issues concerns the regulation of silent calls. This refers to the situation where a call centre may generate calls automatically and seek to transfer them to a salesperson when a call is answered. In the event all the staff are engaged on other calls, some users may answer a call to be met by silence from the other end of the line.

OFCOM has published guidelines on the standards expected of such systems.

\[\text{http://stakeholders.ofcom.org.uk/consultations/silent-calls/}\]
b. The UK regulations are rather more detailed than their counterparts in the Directive but do not appear to be inconsistent with its provisions.
2. What are the legal requirements for the lawful sending of unsolicited messages via electronic mail or other means indicated in Article 13(1) and 13(3) of the Directive? Please indicate whether this is different from the definition provided in the Directive and in what respects.

The Privacy and Electronic Communications (EC Directive) Regulations continue to provide for the use of email communications for commercial purposes stating that:

(2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

(3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b) the direct marketing is in respect of that person’s similar products and services only; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

Regulation 23 continues to provide that:

A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail—

(a) where the identity of the person on whose behalf the communication has been sent has been disguised or concealed; or

(b) where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided.

In the context of UK regimes, the treatment of email communications marks something of a change. Whilst the regulations make similar provision for fax messages, the general rule regarding commercial communications has been that they are permitted unless there is an opt out by the subscriber. The mailing and telephone preference services have been established under the Communications Act 2003 and their operation has been contracted by OFCOM to commercial companies [http://www.mpsonline.org.uk/](http://www.mpsonline.org.uk/) [http://www.tpsonline.org.uk/](http://www.tpsonline.org.uk/) respectively. There is no equivalent service for email due to the different nature of the obligations imposed upon senders. In respect of mail and telephone calls (including SMS messages) there is an obligation to consult...
registers maintained by these organisations of consumers who have indicated a desire to opt out of receiving messages. Commercial email messages are prohibited unless the consumer has consented.

### 3. Does the legislation provide any exceptions to the opt-in consent mechanism? If so, which?

Under the Privacy and Electronic Communications (EC Directive) Regulations Organisations cannot send marketing text or email messages without consent unless:

- the sender has obtained the user’s details through a sale or negotiations for a sale;
- the messages are about similar products or services offered by the sender; and
- the consumer is given an opportunity to refuse the texts when your details were collected and, if you did not refuse at that stage is informed of the right to refuse to receive further messages in each subsequent message and offered a free and simple mechanism to do this.
4. Within the context of unsolicited commercial communications, does your national legislation distinguish (posing different requirements for lawfulness) between certain communication channels? E.g. different rules for e-mail, MMS/SMS/text messages, Bluetooth messages, banners, instant messaging, newsfeeds, social media outreach, etc.), and if so, please describe the main differences briefly.

<table>
<thead>
<tr>
<th>The Privacy and Electronic Communications (EC Directive) Regulations provide in regulation 2 that</th>
</tr>
</thead>
<tbody>
<tr>
<td>electronic mail” means any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient’s terminal equipment until it is collected by the recipient and includes messages sent using a short message service;</td>
</tr>
</tbody>
</table>

This is in line with the provisions of the Directive. At this level no distinction is drawn but it does appear that more enforcement actions have been taken against parties sending unsolicited SMS messages than against email senders – perhaps because spam filters are more effective at reducing the volume of commercial emails reaching the consumer’s attention.
5. Please describe and give references to any form of ‘guidance’ on the interpretation and/or application on rules on ‘unsolicited direct marketing communications’ provided by:

a. national enforcement authorities mentioned under section A (either through general guidance documents or through decisions in concrete cases)

b. national courts through rendering of case law on specific providers or sectors (e.g. mobile operators, app providers, online video platforms, advertising services, etc.)?

<table>
<thead>
<tr>
<th>a. The Information Commissioner publishes extensive guidance for both individuals and organisations. Information is also published about enforcement actions that have been taken in respect of alleged breaches of the regulations <a href="http://ico.org.uk/enforcement/notices">http://ico.org.uk/enforcement/notices</a> and <a href="http://ico.org.uk/enforcement/fines">http://ico.org.uk/enforcement/fines</a>. The Commissioner can serve enforcement notices, impose monetary penalty orders or institute a criminal prosecution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Appeals against decisions of the Information Commissioner go to the Information Tribunal. A significant decision is that of Neale v. Information Commissioner <a href="http://www.informationtribunal.gov.uk/DBFiles/Decision/i1106/Niebel,%20Christopher%20EA.2012.0260.pdf">http://www.informationtribunal.gov.uk/DBFiles/Decision/i1106/Niebel,%20Christopher%20EA.2012.0260.pdf</a>. The Information Commissioner had imposed a monetary penalty notice of £300,000 on the company in respect of conduct described by the Tribunal in the following terms.</td>
</tr>
</tbody>
</table>

The material before us demonstrates that Mr Niebel and his company, Tetrus, has been engaged in sending unwanted text messages on an industrial scale. There were hundreds of thousands of them sent from hundreds of unregistered sim cards seeking out potential claims for mis-selling of PPI loans or for accidents. There is certainly no evidence from Mr Niebel to show that he made any effort to make sure that the recipients consented or that he retained any record of consents. He did not even bother to register with the ICO under the Data Protection Act (DPA) as a controller of data.

In spite of these findings, the Tribunal overturned the penalty. The UK Data Protection Act that provides the basis for enforcement proceedings under the Privacy and Electronic Communications (EC Directive) Regulations states that a penalty may be imposed in respect of conduct ‘of a kind likely to cause substantial damage or substantial distress’. Although the conduct would certainly have caused annoyance and possibly distress the statutory threshold was higher.

A further Tribunal decision relating to the definition of commercial communications concerned a political party, the Scottish National Party. In the case of [Scottish National Party v Information Commissioner](http://www.informationtribunal.gov.uk/DBFiles/Decision/i1106/Niebel,%20Christopher%20EA.2012.0260.pdf), the political party in question had made use of automated systems during the course of the 2005 general election campaign. It appears that it was not alone in making use of the technology but was perhaps less careful than others in consulting the registers of those who had
opted out of receiving unsolicited marketing calls and the Commissioner served an enforcement notice requiring it to desist from what he considered to be processing in breach of the Privacy and Electronic Communications Regulations. On appeal to the Information Tribunal, the Scottish National Party argued principally that as a political party, its communications did not fall into the category of “marketing”. The Tribunal disagreed and upheld the enforcement notice. Marketing, it was held, was concerned with seeking to persuade to influence the way people acted and the fact that in the present case there was no commercial motive was of no relevance. The Scottish National Party was seeking to persuade people to vote for it in preference to other political parties and this, it was held, was no different in principle from one manufacturer or retailer seeking to persuade consumers to deal with them rather than a competitor.
6. What is your individual view of the effectiveness of these rules in practice, like do you consider them to be clear, logically consistent and appropriate to protect privacy within your country?

A significant problem for the United Kingdom concerns the volume of unsolicited commercial emails (and to a lesser extent SMS messages or telephone calls) that are in the English language but emanate from other countries. Enforcement of the rules is difficult in such circumstances. A recent report [http://securelist.com/analysis/monthly-spam-reports/58559/spam-report-february-2014/] indicates that the vast majority of unsolicited communications emanate from outside Europe.

The general provisions relating to the regulation of unsolicited commercial communications are in conformity with the provisions of the Directive but it is difficult to state that they have been effective in reducing the volume of spam messages. The decision of the Information Tribunal described in the previous section indicates, in part because of limitations in domestic law, how difficult it is to enforce rules in a practical environment.
European Commission

ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation

Luxembourg, Publications Office of the European Union

2015 – 1178 pages

doi:10.2759/26900