European Commission

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

**FINAL REPORT – EXECUTIVE SUMMARY**

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



*Digital Agenda for Europe*

**This study was carried out for the European Commission by:**



## 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.

ISBN 978-92-79-48918-1

doi:10.2759/419180

# 1. Executive summary

## 1.1 Introduction

Directive 2002/58/EC – hereafter "the ePrivacy Directive" – aims to protect the privacy and regulate the processing of personal data in the electronic communications sector. As such the Directive complements the Data Protection Directive 95/46/EC. Inter alia, the ePrivacy Directive specifies how some of the principles of Directive 95/46/EC apply to the electronic communications sector.

The ePrivacy Directive is on the other hand part of the Regulatory Framework for Electronic Communications. The Framework was last amended in 2009 and the deadline for transposition of the 2009 amendments was 25 May 2011. By January 2013, all Member States had notified the necessary measures to implement the revised ePrivacy Directive into their national laws.

On 25th January 2012, the Commission adopted a proposal for a reform of the EU legal framework on the protection of personal data. The reform includes a Regulation which lays down a new EU framework for data protection (replacing Directive 95/46/EC). The proposed Regulation also makes a limited number of technical adjustments to the ePrivacy Directive to take account of the transformation of Directive 95/46/EC into a Regulation. The Communication that accompanies the proposed Regulation explains that the substantive legal consequences of the new Regulation and of the new Directive for the ePrivacy Directive will be the object, in due course, of a review by the Commission, taking into account the result of the negotiations on the current proposals with the European Parliament and the Council.

The first objective of this report is to provide evidence on the transposition of the ePrivacy Directive, but also on the effective implementation and enforcement of key provisions of this Directive in the Member States. A second objective is to assess whether the ePrivacy Directive appears to be achieving its intended effects, by identifying and discussing possible gaps, overlaps and diverging transpositions in the Member States, taking into account, in particular, the need to ensure a single market and free movement by avoiding fragmentation along national boundaries. Last but not least, the report addresses the interaction between the ePrivacy Directive and the proposed Data Protection Regulation in order to assess how the two instruments will operate together.

The report does not deal with the entire ePrivacy Directive but is focused on five topics: (i) Articles 1 to 3 regarding the geographical and material scope of application;

(ii) Article 5(1) on confidentiality of communications; (iii) Article 5(3) on cookies, spyware and similar techniques; (iv) Articles 6 and 9 on traffic and location data respectively; (v) Article 13 on unsolicited commercial communications. Topics such as security (Art. 4), itemized billing (Art. 7), calling and connecting line identification (Art. 8 and 10), automatic call forwarding (Art. 11) and subscriber directories (Art. 12) are thus outside the scope of this report.

## 1.2 Scope of application

The Regulatory Framework for Electronic Communications to which the ePrivacy Directive belongs, applies to providers of "electronic communications networks and services" as defined in Art. 2 of Directive 2002/21/EC (the Framework Directive). More precisely, according to Art. 3 of the ePrivacy Directive, the provisions of this Directive are applicable "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community". Consequently only services consisting wholly or mainly in the conveyance of signals – as opposed to e.g. the provision of content – are within the scope of the Directive. However convergence sometimes results in services that are very similar from a functional perspective remaining subject to different legal regimes depending on whether they are provided in the form of an electronic communications service, an information society service, or an audiovisual service. Well-known examples are internet telephony and webmail.

Our survey of the transposition of the ePrivacy Directive into the national legislation of the Member States has demonstrated that the provisions of the Directive are not always transposed in the context of the national legal framework applicable to the electronic communications sector. Several provisions of the Directive have been transposed by Member States in the context of another legal framework, such as the legislative instrument applicable to information society services, the general personal data protection law or the legal framework for consumer protection. As a result, the scope of the national provisions on topics such as cookies, traffic and location data, or unsolicited direct marketing communications, adopted pursuant the ePrivacy Directive, frequently have a different scope of application than the one defined by Art. 3 of the ePrivacy Directive.

Furthermore, the definition of the scope of application of the ePrivacy Directive is ambiguous. The provision refers to "the provision of publicly available electronic communications services in public communications networks" and, according to Art. 2(c) of the Framework Directive the notion of "electronic communications service" does not include information society services, as defined in Article 1 of Directive

98/34/EC and which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

On the other hand, it seems incontestable that certain provisions of the ePrivacy Directive are nevertheless applicable to providers of information society services. The most obvious example is Art. 5(3) dealing with the use of cookies and similar techniques.[1] For other provisions, such as Art. 9 – regulating the processing of location data other than traffic data – the extension of the scope of application to information society service providers is most often excluded.[2] Art. 13 regulating unsolicited direct marketing communications is generally interpreted as being exclusively applicable to messages transmitted via electronic communications.[3]

Moreover, for certain provisions, such as Art. 6 – relating to the processing of traffic data – or Art. 9 – on location data other than traffic data – the narrow scope leads to unacceptable situations of unequal treatment. It is difficult to justify why traffic or location data should receive different legal protection if they are processed in the context of very similar services from a functional perspective. The same observation is valid for the provision of Art. 13(1), prohibiting the use of e-mail without prior consent of the recipient only for messages transmitted via electronic communications and not for messages exchanged via information society services such as social media platforms.

In order to remedy this situation we recommend amending Art. 3 of the ePrivacy Directive to make its provisions applicable to the protection of privacy and the processing of personal data "in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union". The amendment would put an end to the discussion about the applicability of the provisions of the ePrivacy Directive to information society services and other value-added services provided via public electronic communications networks. In addition it would extend the scope of the Directive to private networks that are intentionally made accessible to the public. Such extension has also been suggested by

[1] See e.g. the Article 29 Opinion 2/2010 on online behavioural advertising, p. 9: "The Working Party has already pointed out in WP 29 Opinion 1/2008 that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used".

[2] See e.g. the Article 29 Opinion 13/2011 on geolocation services on smart mobile devices, p. 9: ""The e-Privacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network".

[3] See e.g. the Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines, WP 148 (2008), p. 4: .

the EDPS in his second opinion of 9 January 2009 on the review of Directive 2002/58/EC.[4]

In the longer term, further convergence will probably trigger a broader debate about the opportunity of a more in-depth revision of the current structure of the European regulatory framework for the online environment. Maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services will most probably become less and less relevant in the future. For the time being however, an explicit widening of the scope of application of the ePrivacy Directive can solve, to a large extent, the most urgent issues.

## 1.3 Confidentiality

Article 5(1) of the ePrivacy Directive protects the confidentiality of communications and the related traffic data. The provision states that "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation" and that "in particular, they (Member States) shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users".

It is evident that, at the moment of the adoption of this provision in 2002, all Member States had already long since introduced legislation protecting the confidentiality of private communications. The transposition of Art. 5.1 did not have a harmonizing effect on these existing national legal provisions. The legal protection of confidentiality of communications in the Member States remains therefore diverse. The diversity is mainly related to definitions, conditions and other modalities but, evidently, also to the exceptions. This is due to the fact that Art. 15.1 of the ePrivacy Directive states that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".

As a consequence rules with regard to e.g. wiretapping for law enforcement purposes or monitoring electronic communications in an employment context are not harmonized at the European level. This situation will not fundamentally change after

[4] O.J. C 128 of 6 June 2009, p. 36.

the transposition by the Member States of the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (so-called "Law Enforcement Directive"). The scope of this proposed Directive is restricted to the processing of personal data by law enforcement authorities and doesn't deal with topics such as the interception of electronic communications. Further harmonisation of the rules with regard to these topics would also be difficult to achieve in the short term since they are, in most of the Member States, part of the national criminal procedure rules.

In order to bring the text of Art. 5.1 into line with the proposed widening of the scope of the ePrivacy Directive, we suggest amending it and making it applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible private communications network". It is further evident that confidentiality of electronic communications should also be protected against "automatic" intrusions without human intervention. This clarification could be added in a Recital to the Directive, noting that automated intrusions are of course always initiated and/or controlled by one or more persons. Finally, the exception of Art. 5(1) for "technical storage which is necessary for the conveyance of a communication" should probably be broadened to "storage as far as necessary for ensuring the functioning of the network or the provision of the service on that network". Such amendment would be a logical consequence of the extension of the scope of Art. 5.1 to e.g. information society services.

Article 5.2 of the ePrivacy Directive stipulates that the protection of confidentiality "shall not affect any 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". This provision – often designated as the "business exception" - has been interpreted and transposed by Member States in very different ways. National legislators in some of the Member States have restricted the scope of Art. 5.2 to the electronic communications sector. In other Member States the provision is applied to all sectors and is aimed at giving employers some margin to register telephone conversations conducted by employees in the context of, for instance, a call centre. We suggest therefore clarification of the scope of Art. 5.2 in order to obtain a uniform transposition and implementation of this provision throughout the Union. The currrent restriction to "the provision of evidence of a commercial transaction or of any other business transaction" could be widened to other situations in which recording of communications in an employment context seems to be justified, such as quality control or legitimate supervision of work performance. A harmonised legal basis for monitoring communications of employees for such legitimate reasons, and under the

condition to respect general data protection rules, is currently missing on the European level. A careful assessment of the impact of such change on stakeholders would be needed to assess its feasibility, taking into account the diversity of rules currently applicable to the processing of personal data in the employment context.

## 1.4 Cookies and Similar Techniques

Article 5.3 requests the Member States to "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 (…)". Recital (24) explains that "so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned".

The requirement to collect the users' prior consent in the context of Art. 5.3 is the result of an amendment adopted in 2009 in the context of the Citizen's Rights Directive. Recital (66) of the Citizens' Rights Directive states 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". This part of Recital (66) has been integrated into the text of the law by about ten Member States, including e.g. France, Ireland, Luxembourg, Greece, Poland, Slovakia, Slovenia, Spain and the UK, In other Member States Recital (66) of the Citizen's Rights Directive is referred to in guidance documents issued by national data protection commissioners.

The possibility to express consent via the configuration of browser settings has initially led to uncertainty. The Article 29 Working Party has therefore elaborated the conditions for browser settings to be able to deliver valid and effective consent in its Opinion 2/2010. Several major web browsers, whose default settings often allow all kinds of cookies, do not currently fulfil these conditions. As a consequence – and this should preferably be clearly stated in a Recital of the ePrivacy Directive – only browsers or other applications which by default reject 3d party cookies and which require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites are able to deliver valid and effective consent.

It is further difficult to deny that the introduction of the consent rule in Art. 5.3 did not entirely reach its objective. This is largely due to the fact that the user is currently

receiving a warning message with regard to the use of cookies on almost every web site. Obviously the effect of such warning messages would substantially increase if they would only appear if the web site contains 3d party cookies, cookies used for direct marketing purposes and, more generally, all cookies that are not related to the purpose for which the user is navigating on the site.

Article 5.3 currently contains two exceptions where prior consent of the user is not needed: a) for the technical storage of, or the gaining access to information for the sole purpose of carrying out the transmission of a communication over an electronic communications network and b) for the provision of an information society service that is explicitly requested by the subscriber or the user, when the storing of or the gaining access to information is strictly necessary for the provider. These exceptions should preferably receive a slightly broader formulation, for example, by deleting the condition stating that "the storing of or the gaining access to information (should be) strictly necessary for the provider". In addition we recommend the insertion of additional exceptions, e.g. for cookies which are exclusively used for web site usage statistics. Finally we propose the explicit request of specific, active and prior consent in all cases where cookies or similar techniques are used for direct marketing purposes.

Last but not least, while the current discussion mainly deals with the issue of *how* consent should be given and *how* the relevant information should be furnished to the user or the subscriber, it should also be examined *whether* the choice to make the ePrivacy Directive allow the use of cookies (and similar techniques) based only on the consent of the user or the subscriber is effective and logically plausible. Does the consent of the user justify unlimited tracking of that user's behaviour in the online environment, given the known weaknesses of consent as a mechanism for ensuring legitimacy? This question inevitably leads us to the issue of "profiling", and any solution should take into account the outcome of the discussion in the framework of the proposed general Data Protection Regulation on this very issue.

## 1.5 Traffic and Location Data

Although Article 6 of the ePrivacy Directive seems to be more or less correctly transposed by the Member States, there are serious problems with regard to the enforcement of some of its provisions. Most problematic is Art. 6(3) which stipulates: "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 or her prior consent. Users or subscribers shall be given

the possibility to withdraw their consent for the processing of traffic data at any time."

In practice some mobile operators mention the possibility of processing user and traffic data in their general terms and conditions. Some of these terms and conditions grant the operator a right to process the data for a duration of two years after the end of the contract.

Furthermore, the provisions regarding location data are frequently criticised. The ePrivacy Directive regulates only a fraction of location based services, namely those which rely on the processing of location data other than traffic data offered via a public communications network or in a publicly available electronic communications service. Location based services that are offered to members of a private network are not governed by the provisions of Article 9 of the ePrivacy Directive, even though privacy risks may be the same or even greater. For example, Article 9 does not cover location data that are transmitted via enterprise networks aimed at a private user group, or data collected and transmitted via infrared signals or GPS signals in combination with a private secured wireless LAN.

Moreover, in its Opinion 13/2011 dealing with geolocation services on smart mobile devices the Article 29 Working Party, referring to the strict definition of electronic communications service in Art. 2(c) of the Framework Directive, also stated that "the ePrivacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network" (p. 9).

In line with our proposed amendment to Article 3 of the ePrivacy Directive it is sufficient to slightly modify the wording of Art. 6(1) and Art. 9(1) in order to make the rules with regard to the processing of traffic and location data applicable to all services provided via public or publicly available private communications networks that collect and further process traffic and location data. As a result, the processing of location data in the context of information society services provided via all kinds of mobile apps will be subject to the application of Art. 6 and Art. 9, even if the location data are not resulting from the public electronic communication network or service as such, but via other techniques such as wifi network proximity or IP-address databases.

Additionally, efforts are needed at the Union and the national level to ensure correct transposition of the European rules on the processing of traffic and location data and to enforce their implementation in practice.

## 1.6 Unsolicited Direct Marketing Communications

In general, Member States have adequately transposed Article 13(1) of the Directive. Thus, they have introduced national provisions ensuring that the use of automated

calling and communication systems without human intervention, fax and e-mail for direct marketing is prohibited unless prior consent has been obtained. The term "electronic mail" – being defined in Art. 2(h) of the ePrivacy Directive 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" – is generally interpreted as being restricted to e-mail via electronic communications and not applicable to messages exchanged via information society services such as Facebook, LinkedIn, Skype or Twitter, even when the transmission of such messages ultimately occurs over the internet and thus makes use of publicly available electronic communications services provided on public electronic communications networks. This restrictive interpretation seems also be the one adopted by the Article 29 Working Party.

The Directive leaves some discretion to Member States in relation to "other forms of direct marketing", such as person-to-person voice telephony. As they are relatively more costly for direct marketers, Member States are free to choose an opt-in or opt-out consent regime. Some Member States have chosen opt-in, and others opt-out. This distinction is a natural consequence of the margin of policy making left to the national legislators by EU legislation.

In relation to communications made to subscribers who are legal persons, the Directive stops short of specifying what rules should be put in place at Member State level, but provides the broad requirement that the legitimate interests of such subscribers be "sufficiently protected". In general, one of three approaches was adopted in each Member State for this situation: opt-in, opt-out, or no protection for legal persons.

Our main recommendation with regard to Art. 13 is to bring the scope into line with our proposed amendment to Art. 3. This means, in the first place, that the opt-in rule of Art. 13(1) should also apply to e-mail messages transmitted via information society services.

This extension of the scope of Art. 13(1) should not, however, lead to the prohibition without the prior consent of the user of all kinds of personalised online advertising. Therefore the definition of "e-mail" in Art. 2(h) of the Directive needs to be amended.

Article 13(1) would of course only be applicable if e-mail is "used for the purpose of direct marketing". It is irrelevant whether the direct marketing message is part of the message body or attached in a separate document. However direct marketing should be the primary purpose. This is the reason why, for example, a newsletter or a magazine, sent as an attachment to an e-mail will not fall under the scope of Art. 13(1), as long as the newsletter or magazine is primarily sent for a different purpose, other than direct marketing.

For various reasons we recommend maintaining the possibility for Member States to adopt either an opt-in or an opt-out regime for direct marketing message under Article 13(3).

## 1.7 Relationship with the proposed general Data Protection Regulation

The relationship between the ePrivacy Directive and the proposed general Data Protection Regulation is regulated by Art. 89 of the text proposed by the Commission.

Article 89(1) of the proposed Regulation states that "this Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC". In addition, Recital (135) of the draft Regulation proposed by the Commission states that the Regulation "should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly."

Article 89(2) of the draft Regulation stipulates: "Article 1(2) of Directive 2002/58/EC shall be deleted". Art. 1(2) of the ePrivacy Directive is currently worded as follows: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover they provide for protection of the legitimate interests of subscribers who are legal persons."

The objectives of the proposed Article 89(1), further developed in Recital (135) are to delimit the scope of application of both legislative instruments and to ensure that the modified ePrivacy Directive and the Regulation can work together in the future, after the adoption of the General Data Protection Directive. The proposed Regulation will not be applicable in all cases where the ePrivacy Directive contains specific obligations with the same objective. For the provisions examined in our Study this solution is perfectly possible to implement.

However, if, according to the recommendations formulated in this Study, the scope of application of the ePrivacy Directive were to be modified, the text of Article 89(1) should be amended as well. Currently this text refers to "obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public

communication networks in the Union". This should be changed into "obligations on natural and legal persons in relation to the processing of personal data in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union".

The proposed Art. 89(2) is necessary because a directive cannot "particularise" a regulation. According to Art. 288(2) TFEU a regulation has not only general application but is also binding in its entirety and directly applicable in the whole of the Union. Member States can therefore not be requested in a directive to derogate from rules contained in a regulation.

In our view, the Commission should consider transforming the Directive into a regulation for three reasons. First of all, the relationship between the provisions of the two legislative instruments would be considerably less complex if they are at the same level. This would make the announced revision of the ePrivacy Directive a lot easier.[5] In the second place it may considerably facilitate the application of the entire supervisory and enforcement mechanism introduced by the proposed Data Protection Regulation to the topics currently covered by the ePrivacy Directive. Arguably the adoption of this mechanism will be justified once the scope of the Directive (or of a future regulation) would be widened beyond the borders of the electronic communications sector. Last but not least, it would allow the amendment of Art. 89 of the general Data Protection Regulation (once adopted) if this provision was no longer in line with the final text of a future "ePrivacy Regulation".[6]

If the ePrivacy Directive is not transformed into a regulation and remains a directive, it would be necessary to transform it into a self-standing instrument after the adoption of the General Data Protection Directive, following the example of the proposed Law Enforcement Directive. As a result there would be two instruments containing provisions on personal data protection with mirroring provisions but on different levels. Moreover, if the scope of application of the ePrivacy Directive will be widened and include services which do not belong to the electronic communications sector in the strict sense, the ePrivacy Directive will no longer address a separate sector but the

[5] The revision would be easier because, not only for many current provisions such as Art. 1(3) – the exclusion of the former second and third pillar from the scope of the ePrivacy Directive -, Art. 4(3) – security breach notification - , Art. 15 (1) – allowing Member States to restrict certain provisions of the Directive –, etc. but also for not explictly regulated issues such as the territorial scope, it will suffice to refer to the corresponding provisions of the general Data Protection Regulation. Notice that many current provisions of the ePrivacy Directive are already formulated in a directly binding form (see e.g. Articles 4, 6, 7, 8, 9, 13(1)).

[6] In this hypothesis it is, for example, no longer necessary to delete Art. 1(2) of the ePrivacy Directive because a future ePrivacy Regulation can perfectly particularise and complement the general Data Protection Regulation. Consequently Art. 89(2) would have to be abrogated again.

entire online environment, which is also one of the main targets of the proposed Data Protection Regulation. This overlap will inevitably create a very complex situation.

European Commission

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

Luxembourg, Publications Office of the European Union

2015 – 14 pages

ISBN 978-92-79-48918-1

doi:10.2759/419180

KK-04-15-270-EN-N



doi:10.2759/419180

ISBN 978-92-79-48918-1