EUROPEAN COMMISSION

Brussels, 20.10.2017
C(2017) 6935 final

Dear President,

The Commission would like to thank the Bundesrat for its Opinion on the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications {COM(2017) 10 final} ("ePrivacy Regulation").

The Commission is confident that the proposal would enhance the privacy protection of end-users, increase trust in digital services and allow businesses to fully participate in, and profit from, the Digital Single Market.

The Commission is pleased that the Bundesrat agrees with the aim of the proposal to ensure end-users' privacy in electronic communications and equal competition conditions for all equivalent services. It also duly notes the observations made by the Bundesrat.

The Commission values the Bundesrat's questions and comments. The Commission is pleased to have this opportunity to provide a number of clarifications regarding its proposal and trusts that these will allay the Bundesrat's concerns.

In response to the specific questions and comments in the Opinion, the Commission would like to refer the Bundesrat to the attached annex.

The points made in this reply are based on the initial proposal presented by the Commission, which is currently in the legislative process involving the European Parliament and the Council.

The Commission hopes that the clarifications provided address the issues raised by the Bundesrat and looks forward to continuing the political dialogue in the future.

Yours faithfully,

Frans Timmermans
First Vice-President

Andrus Ansip
Vice-President

Ms Malu DREYER
President of the Bundesrat
Leipziger Straße 3 - 4
D – 10117 BERLIN

ANNEX

The Commission has carefully considered the issues raised by the Bundesrat in its Opinion and would like to offer the following observations grouped by topic.

1. *The relationship between the proposal for an ePrivacy Regulation and the General Data Protection Regulation*

The Bundesrat requests that the relationship between the proposed provisions and the provisions of the General Data Protection Regulation[1] are defined more precisely. One of the main objectives of the review of the ePrivacy Directive[2] is to ensure a high level of protection of consumers throughout the Union, as announced in the Digital Single Market Strategy, and to create a coherent data protection framework. As set out in its Article 1(3), the proposed Regulation is lex specialis to the General Data Protection Regulation and will particularise and complement it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the General Data Protection Regulation.

Chapter II of the proposal provides inter alia for permitted processing of electronic communications data under Article 6; exceptions to the prohibition to make use of processing and storage capabilities of terminal equipment and to collect information from end-users' terminal equipment under Article 8(1); and exceptions to the prohibition to collect information emitted by terminal equipment under Article 8(3). In practice, this means that the provisions of this Regulation would prevail in these specific circumstances over the general legal grounds to process personal data provided by the General Data Protection Regulation.[3] Conversely, the other provisions remain applicable for data that qualifies as personal data, such as the right to be forgotten, the right to access to, erasure and rectification of data and the rules on transfers of data to third countries. Due attention will be paid during the legislative process to creating a clear legal framework and to avoiding legal uncertainty.

2. *Confidentiality of electronic communications data: scope of application*

The Bundesrat questions whether all services providing location services, such as mapping services, and thus processing location data, are treated equally to electronic communications services that process location data.

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

3 Recital 5 of the proposed Regulation states that: "Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation." (*emphasis added*)

The proposal provides for confidentiality of communications for natural and legal persons, as does the current ePrivacy Directive. This is in line with Article 7 of the Charter of Fundamental Rights of the European Union, which grants the right to respect for private life and communication both to private and legal persons. Under the proposal, electronic communications services are required to delete metadata, including location data, unless the processing is permitted under Article 6 of the proposed Regulation. The reason for this is that communications metadata can reveal a person's habits in life, such as one's movements, activities and social relationship.

A mobile phone connects to the cell tower non-stop and provides location data to the electronic communications service. Switching off the electronic communication service is not possible, otherwise one loses connectivity and thereby the ability to call and to be called. This is different for some other services processing location data. Some services rely on GPS-location data. A user may decide to switch off his or her GPS signal and thereby decide not to reveal his or her geographical location to the respective service. This data is protected by the General Data Protection Regulation.[4]

The processing of location data that is not related to a communication may be needed in a variety of circumstances and is covered by the General Data Protection Regulation ; for example an employer needing to know which employees are in the building by using a badge system or a taxi service that needs to locate its taxis. In some cases, consent of the individual may be needed under the General Data Protection Regulation, but not necessarily. For example in an employment context, the employer cannot rely on consent as a legal ground to process location data because the worker is in theory able to refuse consent, but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid.[5]

The different circumstances in which the General Data Protection Regulation applies illustrate the need for different legal grounds to process location data that is not related to a communication. However, in the case at hand, electronic communication services present a specific, known circumstance outlined above, justifying a specific regime.

Furthermore, the Bundesrat questions whether the transmission of machine to machine communications data should be included in the scope of the Regulation or if this would hamper innovation. The proposed ePrivacy Regulation would cover the transmission of machine to machine communications data when carried out by an electronic communications service, just like the ePrivacy Directive currently does. The reason for this is that machine to machine communications data may relate to a natural person or may constitute business information, just like communications exchanged by natural persons or legal persons. If the transmission of machine to machine data were not required to be confidential, such a

---

4 In addition, if the GPS location data is obtained from the terminal equipment, this would entail the use of the processing capabilities of the terminal equipment and thus consent would be needed under Article 8 (1) of the proposed ePrivacy Regulation.

5 WP29 Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185).

situation may lead to an interference with the right to respect for private life and communications of the natural or legal person the data relates to.

3. Confidentiality of terminal equipment

With regard to the proposed provision on the protection of confidentiality of terminal equipment, the Bundesrat considers that Article 8(1)(d) of the proposal is inappropriate.

The Commission recalls that Article 8(1)(d) allows usage of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment without consent from the end-user concerned if it is necessary for web audience measuring, and provided that such measurement is carried out by the provider of the information society service. Web audience measurement carried out by the providers of the information society services itself is considered to have no or limited privacy impact. Such an exception receives support from the European Data Protection Supervisor and the Article 29 Working Party, provided that certain safeguards are in place.[6]

On the possibility under Article 9(2) of the proposal to provide consent via appropriate technical settings, the Commission would like to stress that consent needs to be in accordance with the conditions set out under Article 4(11), Article 7 and recital 42 of the General Data Protection Regulation. Consent needs to be freely given, with specific, informed and unambiguous indication of the data subject's wishes, by a clear affirmative action. To this end, recital 24 encourages web browsers to allow the user to make exceptions for or to whitelist certain websites, or to specify for which websites (third) party cookies are always or never allowed. If technical settings do not allow for consent to be given in accordance with the conditions of the General Data Protection Regulation, the technical settings may deem to be inappropriate to provide for consent.

4. Obligations placed upon software permitting electronic communications

The Bundesrat asks for clarification on which actors would be covered by Article 10 of the proposed Regulation. The requirement to offer the option to prevent other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment is put on software permitting electronic communications. This applies to browsers, but also other kinds of software such as applications that permit calling and messaging or provide route guidance, as explained in recital 22. Operating systems that permit electronic communications also qualify as the software concerned, as suggested by the Bundesrat. Hardware does not fall within the scope of the proposed Regulation. However, the Radio Equipment Directive requires equipment to be constructed so as to ensure personal data and privacy of the user and of the subscriber are protected.[7]

---

6 EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation); WP29 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP247); WP29 Opinion 04/2012 on the Cookie Consent Exemption (WP194).

7 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance (OJ L 153, 22.5.2014, p. 62–106).

Article 10(1) of the proposal requires software to have a specific setting available, to prevent anyone from storing or processing information already stored in the terminal equipment. This does not prevent software from developing additional settings, such as 'always accept cookies' or 'only accept first party cookies', as explained in recital 23. The requirement under Article 10(1) ensures that technical settings are available to make the prohibition enshrined in Article 8(1) effective. Article 8(1) prohibits making use of processing and storage capabilities of terminal equipment and collecting information from end-users' terminal equipment, unless one of the situations described under Article 8(1) (a) to (d) applies. This prohibition corresponds with the aim of protecting the integrity of the terminal equipment. Given that current tracking techniques entail the use of processing and storage capabilities of terminal equipment, Article 10(1) aims to achieve the same result with the required setting as Do-Not-Track settings would, namely to prevent tracking. The aim of Article 10 (1) is illustrated in recitals 22 to 24 of the proposal.

5. *Collection of data emitted by the device (offline tracking)*

The proposal contains rules on the collection of data emitted by the device in its article 8(2). The Bundesrat is concerned that the proposal would lower the level of protection. The Commission would like to stress that the proposal does not intend to lower the level of protection.

The proposal is meant to cover a specific situation: counting individuals, without the collection of any other additional information, as explained in recital 25. For other more intrusive purposes, including merging the collected data with personal data, providing information may not be sufficient and an additional legal ground under the General Data Protection Regulation may be needed.

6. *Restrictions of rights and obligations under the proposed ePrivacy Regulation*

The Bundesrat expresses its concerns regarding the balance between, on the one hand, the necessary protection measures to ensure the protection of communications data and on the other hand, the need to effectively combat terrorism and crime. To this end, the Bundesrat asks clarification on the relationship between Article 2(2)(d) which provides that the Regulation does not apply to "activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security", and Article 11 that allows for restrictions.

Article 2(2)(d) of the proposal places the activities carried out by competent authorities for the stated purposes outside the scope of the proposed Regulation[8]. Article 11, on the other hand, refers to other actors, such as providers of electronic communications services, and

[8] These activities may fall within the scope of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

allows Member States' law or Union law to introduce restrictions to the scope of their rights and obligations under this Regulation.

The Bundesrat believes that requirements are needed for Member States to work together to combat cyber dangers. The Commission recognizes the need for cooperation between Member States on cyber security and notes that the Union legislator has addressed this need in Directive (EU) 2016/1148 on security of network and information systems ("NIS Directive"). The Directive establishes mechanisms enhancing cooperation, both strategic and technical cooperation, between Member States, with a view to achieving a high common level of cyber-security within the European Union. In order to support strategic cooperation, the Directive establishes the so-called Cooperation Group which aims at facilitating the exchange of information among national competent authorities and developing trust amongst them. The Directive also created a network of Computer Security Incident Response Teams, known as the CSIRTs Network, which is instrumental to swift and effective operational cooperation. This Network allows national experts to share information about possible cybersecurity risks and eases cooperation in case of cyber-incidents.

The Bundesrat also puts forward the need for effective data exchange and cooperation between security agencies. National security is the sole responsibility of each Member State according to Article 4(2) of the Treaty on European Union and therefore the Commission does not foresee an initiative on data exchange and cooperation between security agencies.

The Bundesrat considers it inadequate that the restrictions that Article 11 allows for are accompanied with introductory remarks only and questions whether the second sentence of Article 15 (1) of the ePrivacy Directive should be re-introduced.

The proposed provision maintains the substance of Article 15(1) of the ePrivacy Directive and aligns it with the specific wording of the General Data Protection Regulation by referring to Article 23(1)(a) to (e). It provides grounds for Member States to restrict the scope of the rights and obligations as provided for in specific articles of the ePrivacy Directive. Therefore, Member States can still provide for national data retention frameworks. Such frameworks must comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights. This includes, inter alia, the requirement for retention measures to be targeted.[9] *Therefore, the Commission does not see a legal reason to modify Article 11 in that regard.*

7. <u>Enforcement of the proposed ePrivacy Regulation and remedies</u>

The proposal appoints the independent supervisory authority or authorities responsible for monitoring the application of the General Data Protection Regulation as the responsible authorities for monitoring the application of the proposed Regulation. The Bundesrat is concerned that this would lead to more work for data protection authorities and would prefer more flexibility left to Member States on this matter.

---

[9] See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

The proposal aligns the supervisory regime with the regime of the General Data Protection Regulation to ensure a harmonious framework.

In most cases, the enforcement of the ePrivacy provisions will not only concern privacy matters, but also data protection matters. For this reason, Article 16 of the Treaty on the Functioning of the European Union is one of the legal bases for the proposal. Article 16 introduces a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, by Member States when carrying out activities falling within the scope of Union law, and rules relating to the free movement of such data. Since an electronic communication involving a natural person will normally qualify as personal data, the protection of natural persons with regard to the privacy of communications and processing of such data should be based on Article 16 of the Treaty on the Functioning of the European Union. According to that Article, compliance with these rules shall be subject to the control of independent authorities. Thus, pursuant to Article 16, the authorities supervising the General Data Protection Regulation and the proposed ePrivacy Regulation must be independent. Article 52 of the General Data Protection Regulation sets out the independence requirements the authorities supervising the General Data Protection Regulation must comply with. As for the authorities supervising the General Data Protection Regulation it is already established that they must be independent; hence relying on these authorities for the enforcement of the proposed ePrivacy Regulation will ensure that these enforcement authorities are independent as well.

On top of the required level of independence, it is essential that the authorities competent to enforce the ePrivacy Regulation are the same as the enforcement authorities of the General Data Protection Regulation in order to avoid divergent views on the data protection aspects between the authorities enforcing the General Data Protection Regulation and the authorities enforcing the ePrivacy Regulation. It would also allow the enforcement of the ePrivacy Regulation to benefit from the consistency and one-stop-shop mechanisms established by the General Data Protection Regulation. This is particularly relevant due to the extended scope of the proposed ePrivacy Regulation to over-the-top services. These services by nature offer services across border and therefore the General Data Protection Regulation mechanisms would benefit both the enforcement authorities as well as industry.

If enforcement of the ePrivacy Regulation were to lead to more work for the appointed authority, it is important that this is reflected in the authority's resources. To this end, recital 38 states that: "each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation." The same recital explains that Member States may appoint more than one supervisory authority "to reflect their constitutional, organisational and administrative structure."

Reference is made to a provision on "class action" by the Bundesrat. This point is understood in light of Article 80 of the General Data Protection Regulation. The Commission believes that the proposal provides for the possibility of a class action. Article 21 of the proposal

grants the remedies provided for in Articles 77 to 79 of the General Data Protection Regulation to end-users. No reference is made to Article 80 of the General Data Protection Regulation; however, as the proposed ePrivacy Regulation particularises and complements the General Data Protection Regulation, the right granted under Article 80 of the General Data Protection Regulation shall be applicable to end-users who are natural persons. In line with recital 5, the underlying Regulation does not lower the level of protection enjoyed by natural persons under the General Data Protection Regulation. This could be further clarified in the legal text if deemed necessary. The Commission will continue to pay close attention to the coherence of aforementioned instruments.

The Bundesrat also refers to Article 21(2) of the proposed Regulation and requests clarification for the need of providing for the right for natural and legal persons to start legal proceedings. Article 13(6) of the ePrivacy Directive allows this right already for infringement of the national provisions on unsolicited communications. In practice, this would for example allow service providers to initiate legal action against the senders of direct marketing communications and thereby defend the interest of their customers.[10] This rule is kept and broadened by Article 21 (2) of the proposal to apply to the other provisions of the Regulation as well.

[10] Recital 68 of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) (OJ L 337, 18.12.2009, p. 11–36).