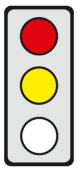
PRIVACY AND ELECTRONIC COMMUNICATIONS

cep**PolicyBrief** No. 2017-16

KEY ISSUES

Objective of the Regulation: The Commission wants to protect the confidentiality of electronic communications and the related end-user data more effectively and at the same time ensure their freedom of movement.

Affected parties: End-users and providers of electronic communication services, manufacturers of software giving access to the internet, persons who store information in, or collect it from, the terminal equipment of end-users, providers of public directories.



Pro: Uniform rules protecting the confidentiality of electronic communications that are also applicable to OTT services create a level playing field EU wide.

Contra: (1) The numerous ambiguities in the Regulation make its uniform application virtually impracticable. This results in legal uncertainty which weakens the EU as a location for the data economy.

(2) The envisaged coherence between the Regulation and the GDPR has not been achieved. The Regulation must be fundamentally revised.

CONTENT

Title

Proposal COM(2017) 10 of 10.01.2017 for a **Regulation** of the European Parliament and of the Council **concerning the respect for private life and the protection of personal data in electronic communications** and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Brief Summary

- **Context and objectives**
  - Following the reform of the protection of personal data by the General Data Protection Regulation [(EU) 2016/679, see cep**PolicyBrief**] the Commission now wants to replace the Data Protection Directive 2002/58/EC for electronic communications ("E-Privacy Directive") with a Regulation.
  - The Regulation will "particularise and complement" the General Data Protection Regulation (GDPR) and not lower its level of protection and will apply contemporaneously with the latter as from 25 May 2018 (Recital 5, Art. 29).
  - The aim of the Regulation is (Explanatory Memorandum, p. 2-6 and 8),
    - to safeguard the end-users' fundamental rights to privacy and confidentiality of communications and the protection of their personal data when using electronic communications,
    - to ensure the free movement of communications data, equipment and services in the EU,
    - to extend existing rules on new types of communications services such as Whatsapp or Skype (over-the-top or OTT services) in order to create a level playing field,
    - to ensure coherence with the GDPR and create legal certainty.
- **Scope and Definitions**
  - The Regulation applies to the processing of electronic communications data when providing and using electronic communications services (ECSs). It also protects all "information relating to the terminal equipment of the end-users". [Art. 2 (1)]
  - It protects both natural and legal persons [Art. 1 (1) and (2)].
  - ECSs are (Art. 4 (1) (b), (2) in conjunction with Art. 2 No. 4 and 5 COM(2016) 590, see cep**PolicyBrief**)
    - internet access services,
    - services consisting mainly in the conveyance of signals, e.g. fixed and mobile telephony services and machine-to-machine communication (M2M) and
    - interpersonal communications services (ICSs) which allow the interpersonal exchange of information, e.g. webmail services, internet telephony services, messenger services and chat functions.
  - "Electronic communications data" are [Art. 4 (3) (a) - (c)]:
    - communications content - e.g. texts, videos - which are transmitted by way of ECSs and
    - metadata which has to be processed in electronic communications networks in order for the transmission or exchange of content to take place at all, e.g. locational data and time of communication.
  - Terminal equipment refers to PCs, tablets, smart phones and satellite earth station equipment [Art. 4 (1) (c)].
  - The Regulation applies to (Art. 3 (1) (a) - (c) and Recital 9)
    - all operators who "provide" ECSs to end-users in the EU even if provision takes place from outside the EU or the communications data is not processed in the EU,
    - all "users" of these services and
    - the terminal equipment of end-users located in the EU.
- **Confidentiality of electronic communications data**

  Electronic communications data is confidential. Listening, storing, scanning or other kinds of interception, surveillance or processing of such data by other persons than the end-user is generally prohibited. (Art. 5)

Authors: Dr. Anja Hoffmann, LL.M. (Eur.) and Philipp Eckhardt, | mailto:hoffmann@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Telephone +49 (0)761 38693-107 | www.cep.eu

- **Permitted processing of electronic communications data**
  - As an exceptional case, electronic communications data - both communication content and metadata - can be processed, e.g. stored, if and insofar as this is necessary to
    - achieve the transmission of the communication [Art. 6 (1) (a)],
    - to maintain the security of ECSs and networks or to detect faults [Art. 6 (1) (b)].
  - In addition, electronic communications metadata can only be processed [Art. 6(2)],
    - if the end-user "concerned" has consented to its being processed for specific purposes, e.g. in order to receive additional services, insofar as these purposes cannot be achieved if the data is made anonymous,
    - in order to meet quality requirements under EU law – e.g. the ability to cope with jitter – or
    - in order to bill for services or to combat their abusive use.
  - In addition, electronic communications content can only be processed
    - for the sole purpose of providing a specific service "to an end-user" which cannot be provided without the processing of this content and "the end-user or end-users concerned" have consented [Art. 6 (3) (a)], or
    - for other purposes that cannot be achieved where information is made anonymous, if "all end-users concerned" have given their consent; in addition the operator must consult the supervisory authority and comply with its recommendations (Art. 6 (3) (b), Art. 36 GDPR).
  - As soon as the electronic communications data is no longer needed for the permitted purposes, the processing permission ceases to apply and the operator must delete them or make them anonymous [Art. 7 (1)–(3)].
  - The end-user's consent must comply with the conditions of the GDPR: it must be a freely given, with knowledge of the situation ("informed"), unmistakeably intended for a specific case and it must be capable of withdrawal at any time [Art. 9 (1) in conjunction with Art. 4 and 7 GDPR].
- **Protection of "information related to end-users' terminal equipment"**
  - In principle, other persons than the end-user are not permitted to use the "processing and storage capabilities" of end-users' terminal equipment – e.g. in order to store cookies – or to collect information from this terminal equipment, e.g. stored photos or contact details (Art. 8 (1)).
  - Exceptions are permitted if the end-user gives consent or the use or collection is necessary
    - for transmitting the communication or
    - for the provision of an "information society service" requested by the end-user, such as where cookies are necessary to authenticate the end-user in an online shop; in this case, the intrusion of privacy must only be very limited (Recital 21); or
    - for web audience measuring, provided that such measurement is carried out by the provider of the information society service itself – and not by a third party.
  - Consent may be issued or refused by way of the software enabling information to be downloaded from the internet, such as via web-browsers and apps [Art. 9 (2))]. Suppliers must configure their software so that upon installation or update, end users have to choose "binding" privacy settings which are "enforceable" against third parties (Art. 10, Recital 22).
  - In principle, it is not permitted to collect any information sent by terminal equipment to enable it to connect to another device or network, e.g. equipment identities, bluetooth or wireless signals (Art. 8 (2), Recital 25). By way of an exception, such "offline tracking" is permitted
    - if and insofar as it is necessary in order to establish a connection, or
    - where the collector takes appropriate data security measures and the end-users are informed in a "prominent notice" inter alia of the purpose of the collection and of the possibility of stopping it.
- **Protection from unsolicited direct marketing**
  - All types of direct marketing, including election canvassing, can only be sent by ECS to natural persons who have given consent ("opt-in", Art. 16 (1), Recital 32). Member States can provide for a right to object in respect of personal marketing calls ["opt-out", Art. 16 (4)].
  - In the context of existing customers, advertising emails for one's "own similar products or services" are permitted if the customer has not objected ["opt-out", Art. 16 (2)].
- **Restriction and enforcement of the Regulation, compensation**
  - Member State law may restrict confidentiality by law in order to protect important interests (Art. 11).
  - Compliance with the Regulation will be monitored by the independent national supervisory authorities responsible for the GDPR (Art. 18). These have the powers set out in the GDPR and where appropriate can impose fines running into the millions [Art. 23 (1) - (3) in conjunction with Art. 58 (2) (i) GDPR].
  - End-users can claim compensation for damages and - with the exception of class actions - have the same remedies and rights of recourse as under the GDPR (Art. 21 and 22).

Main Changes to the Status Quo

- In future the rules will be contained in a Regulation rather than, as previously, in a Directive.
- Until now, the rules only applied to conventional ECSs services; in future they will also apply to OTT services.
- The existing opt-in requirement for cookies will be extended into a general protection for information in terminal equipment. By contrast, "offline tracking" will be permitted without consent.
- New: in future all software which enables access to the internet (browsers, apps) must require the end-user to select binding privacy settings upon installation.

- Until now, various authorities monitored compliance with the Regulation in the Member States; in future, the national authorities responsible for the GDPR must also do this. Fines will be increased.

Statement on Subsidiarity by the Commission

In the transnational electronic communications market, only action at Union level can provide uniform EU-wide protection of fundamental rights, the free movement of data and a level playing field.

Policy Context

Within the framework of its Digital Single Market Strategy [COM(2015) 192, see cepPolicyBrief], the Commission also wants to reform the rules protecting the privacy of users of ECSs.

Legislative Procedure

10 January 2017	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content & Technology (leading)
Committees of the European Parliament:	Civil Liberties, Justice and Home Affairs (leading), Rapporteur: Marju Lauristin (S&D)
Federal Ministries:	Federal Ministry of Economics (leading)
Committees of the German Bundestag:	Economic Affairs (leading);
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Legislative competence:	Art. 16 (2) TFEU (Data Protection), TFEU (Internal Market)
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Ordoliberal Assessment

Uniform provisions protecting privacy and **the confidentiality of electronic communications that are also applicable to OTT services** strengthen the internal market because they result in lower costs for data-processing companies and **create a level playing field EU wide.** The latter is also achieved by the fact that, in future, not only traditional but also new types of electronic communications services (OTT services) will have to meet the requirements.

The Commission proposal contains serious flaws however. Firstly, the relationship to the General Data Protection Regulation (GDPR) is unclear in many respects. Secondly, the proposal contains numerous vague provisions (see Legal Assessment). This **results in significant legal uncertainty which** has the effect of inhibiting investment and **weakens the EU as a location for the data economy. The Regulation** must therefore be rejected in its current form. It **must be fundamentally revised**, even if this means that its entry into force will not be contemporaneous with that of the GDPR.

Legal Assessment

Legislative Competency

This is unproblematic; the Regulation is correctly based on the data protection competence (Art. 16 (2) TFEU) and on the internal market competence (Art. 114 TFEU).

Subsidiarity

The confidentiality of borderless communication can be better protected by the EU than by the Member States.

Proportionality with respect to Member States

Uniform, EU-wide protection which is consistent with the GDPR can only be provided by way of a Regulation because this avoids any diverging implementation under national law. However, **the Regulation fails to provide the clarity of wording required for directly applicable law and is** therefore disproportionate and **thus unlawful. Numerous ambiguities make its uniform application virtually impracticable.** This concerns e.g. unclear definitions by references to the "European Electronic Communications Code" [COM(2016) 590], which has not yet been adopted, vague exception rules – e.g. which "concerned" end-user must consent? –, a non-transparent fusion of data protection and confidentiality rules – the Regulation protects the confidentiality of the communication irrespective of any reference to a person, but wants to ensure the "protection of personal data" –, and a lack of differentiation from the GDPR (see below). All of the main terms must be defined in the Regulation. It must be made clear which rules bind which addressees.

The obligation of Member States to monitor compliance with the Regulation by way of its independent data protection authorities, is a disproportionate intervention in the organisation of national authorities. The EU

Charter of Fundamental Rights (CFR) stipulates monitoring by an independent authority only for compliance with provisions on the protection of personal data, but not for the protection of communications. An obligation for the existing authorities to cooperate effectively with the data protection authorities would therefore be less interventionist.

Compatibility with EU Law in other respects

The basic ban on processing electronic communications data guarantees, on the one hand, the fundamental right to respect for communication in secondary law but, on the other hand, encroaches on the freedom of ECS providers to conduct a business, protected by Art. 16 CFR. However, reliably specifying the exceptional cases when such data is permitted to be processed, is virtually impossible because the Regulation's provisions on consent are sometimes difficult to distinguish from one another and in some cases contain ambiguous requirements. Which exemption is intended to cover which case; which "concerned end-user" has to give consent and what is the relationship between consent and anonymization, are questions which require clarification. **The fact that the Regulation largely requires the consent of the end-user for data processing, strengthens the protection provided by fundamental rights but the requirement for consent is not practicable in every case**, e.g. for spam and virus protection as well as for M2M communication including driverless vehicles. **Thus additional exemptions must be defined.** The question to be examined is whether processing without consent may be permitted under more flexible conditions, in order to protect a person's vital interests or in specific cases where interference with confidentiality can be minimised by supplementary security measures such as pseudonymisation and/or encoding.

The envisaged coherence between the Regulation and the GDPR has not been achieved even though their respective areas of application overlap. The relationship between the provisions is often unclear. In need of clarification, for example, is the question of when the GDPR applies on its own - e.g. after conclusion of the communication process? –, when provisions of the Regulation "complement" the GDPR – e.g. to what extent its general principles apply here too – and when they "particularise" the provisions of the GDPR, i.e. override them – which means recourse to its exception rules is excluded. Stricter provisions than those of the GDPR are only justified where the specific risks of using electronic communications services require them. In some cases, contrary to the declared intention of the Commission, the Regulation's level of protection is even lower than that of the GDPR. Thus the simple option to reject cookies provides less protection than a software that – in line with the GDPR's principle of "privacy by default" – is already pre-set accordingly. Offline tracking is also allowed simply where there is notification and an opt-out possibility. It would be more consistent if, in principle, consent had to be obtained in this case too, but at the same time tracking were permitted in exceptional cases subject to strict limitations, e.g. to determine user numbers.

The rules on privacy settings are also misguided. The corresponding configuration obligations upon the software manufacturers disproportionately interfere with their entrepreneurial freedom (Art. 16 CFREU) and right of ownership (Art. 18 CFREU). Their purpose of creating user-friendly possibilities for giving consent, is misguided because a "simplified" consent in the settings is often not legally binding. According to the GDPR, the end-user must always be "informed" and give consent "for the specific case". This is not complied with if cookies are generally allowed in the browser settings because it is impossible to anticipate the concrete purpose of all data processing operations on websites which are visited subsequently. Such an "advance blanket consent" does not allow the end-user any possibility for differentiation and also lacks transparency. Although a general rejection of cookies is possible in the settings, the Regulation fails to specify how these settings behave where consent has been given independently. It is also unclear to what extent providers can make their services dependent on consent to data collection by cookies, and in what way cookie opponents may no longer be able to make unlimited use of websites.

Impact on German Law

The directly applicable rules in the Regulation override the sector-specific German rules on telecommunications data protection in Sections 91 et seq. Telecommunications Act (TKG), on secrecy of telecommunications (Section 88 TKG), on data protection for telemedia [Section 11 et seq. Telemedia Act (TMG)] and on direct marketing in Section 7 Unfair Competition Act (UWG). In some cases, they have in any case already been overridden by the GDPR. The provisions should be repealed unless they are allowed under opt-out clauses in the Regulation or otherwise go further than mandatory EU law.

Conclusion

Uniform rules protecting the confidentiality of electronic communications that are also applicable to OTT services create a level playing field EU wide. However, the Regulation fails to provide the clarity of wording required for directly applicable law and is thus unlawful. Numerous ambiguities make its uniform application virtually impracticable. The fact that the Regulation largely requires the consent of the end-user for data processing, strengthens the protection provided by fundamental rights. The requirement for consent is not practicable in every case however. Thus additional exemptions must be defined. The envisaged coherence between the Regulation and the GDPR has not been achieved. The rules on privacy settings are also misguided. All this results in significant legal uncertainty which weakens the EU as a location for the data economy. The Regulation must be fundamentally revised.