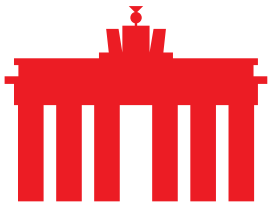

WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

POSITION PAPER

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

Berlin/Brussels, 28 February 2017

On 10 January 2017 the European Commission presented its draft proposal for a regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (COM(2017)10 final) (ePrivacy Regulation). The Commission intends the regulation to govern the confidentiality of electronic communication and to establish rules for the transfer of data and its storage. The ePrivacy regulation is intended as *Lex Specialis* to the EU General Data Protection Regulation (hereafter GDPR), according to the EU Commissioner Věra Jourová. This means that the regulation would have precedence over the GDPR.

In its strategy for the Digital Single Market in 2015, the European Commission decided that the ePrivacy Directive 2002/58/EC, which is currently in force, should be examined in order to ensure that it harmonises with the General Data Protection Regulation. The result, a new ePrivacy Regulation, by far overshoots this goal. eco has previously called for a regulatory framework for data protection to be created which is as uniform as possible and applies across sectors of the economy.

General Comments

Data protection in the Digital Single Market should be subject to general uniform and universal standards. Sector-specific regulations – for example, as is the case for electronic communication – should concentrate on a clearly defined area. Such a precise regulatory environment offers all participants in the digital society – from providers of electronic communication services to website owners and Internet users – legal and planning certainty. With its draft ePrivacy Regulation the Commission by far overshoots the goal of just examining the existing directive. The ePrivacy Regulation restricts digital business models and makes the development of a European data economy more difficult with restrictive regulations and excessive extension of the regulatory field.

Since the directive will immediately become law in all Member States, it creates the need for adaptation to and implementation in the German telecommunications and

telemedia law. At the same time, there are particular challenges for the Internet industry; both due to the Commission choosing to propose a regulation and due to the contents of the regulation.

- **Extension of regulatory field through the ePrivacy Regulation**

The ePrivacy Regulation refers to the two central regulatory frameworks for the Internet industry: the European Electronic Communications Code (EECC) and the GDPR. At the same time, the ePrivacy Regulation introduces new definitions in reference to the GDPR and expands on existing definitions included in the EECC.

This extends the application of the regulation to services that are explicitly not included in the EECC. The additional definitions in the area of data protection extend the provisions of the GDPR to all and any electronic communication – also to communication that is not between persons. This extension is contrary to the aims the EU Commission states in its communication "Building a European Data Economy" as part of the Digital Single Market strategy and to enable framework conditions for Big Data offers and the free flow of data traffic in Europe. In just the last few years, businesses have started which provide specialised services – also for traditional industries – and are active in a highly specialised competitive environment.

- **Fragmentation of data protection regulation**

It is unclear which relationship individual aspects of the ePrivacy Regulation have to the GDPR. This is the case with Article 6 of the ePrivacy Regulation, which does not address the further processing of data. The GDPR enables further processing of data with some limitations. To what extent these limitations can be exploited is not clear in the draft regulation, as it only places restrictions on data processing itself. The reference to several articles of the GDPR (Articles 18ff) is also an issue, as these could be substantially changed during the further legislative process. This will result in data protection regulation becoming even more fragmented, thanks to the ePrivacy Regulation.

A further difficulty is that delegated and implementing acts may be created for the GDPR which further define the implementation rules for the GDPR. These could conflict with the ePrivacy Regulation, for which delegated and implementing acts may also be developed.

The proposed regulation does not provide legal certainty, but rather ambiguity. Further fragmentation of the regulation through national statutes which can all be interpreted differently will only compound this problematic situation.

- **The regulatory framework between the EECC, GDPR and the ePrivacy Regulation is becoming increasingly inconsistent**

Although it is often reiterated that the ePrivacy Regulation is only intended to a specific part as a *Lex Specialis* to the GDPR, the aspects addressed above show that this delineation is not successful.

It is also unclear what the relationship is to the EECC. The original intention of the EU Commission has been lost; to present a clear GDPR which proscribes a high level of uniform data protection for all market participants and to offer a telecommunications framework with the EECC and further define corresponding rules to regulate the telecommunications market. The ePrivacy Regulation lays claim to a new and separate area of application, which distorts the standards of relevant European legislation and makes them inconsistent.

- **The ePrivacy Regulation must be thoroughly revised**

The ePrivacy Regulation draft gives rise to numerous, fundamental regulatory questions in relation to the regulatory framework and the compatibility of existing regulations such as, e.g., the GDPR. These questions must be answered. The ePrivacy Regulation must be harmonized with the GDPR and superfluous sections must be removed. The Commission has repeatedly stressed that the ePrivacy Regulation is to come into force simultaneously with the GDPR on 25 May 2018. This is problematic for two reasons. Firstly, the legislative process for the ePrivacy Regulation will most likely drag out until the end of 2017. Secondly, the contents of the draft show that there is much need for intensive and fundamental examination and discussion.

When the interaction between the ePrivacy Regulation and the GDPR is examined, then it is clear that it will not be possible for the Internet industry to implement both regulations within the specified timeframe. The deadline must be extended. A further difficulty is that the EECC – a second reference point – has not yet been passed. The annexes of the EECC and the regulation establishing the Body of European Regulators for Electronic Communications (BEREC) may also affect the ePrivacy Regulation. Passing the ePrivacy Regulation too quickly with references to these regulations is something that should be avoided.

There is also an urgent need to closely examine the necessity and scope of the individual articles, as well as their interplay with existing legislation. This will lead to comprehensive consultations with the Internet industry, civil society and politics. These should be fully exploited in order to jointly identify regulatory gaps and how to address these.

1. Comments on the individual Articles

- **Article 1 “Subject matter”**

Article 1 is a modified version of Article 1 GDPR. However, in comparison to the GDPR, it expands the circle of those affected to include legal persons (Art. 1 (1)). This de facto extends data protection to data above and beyond personal data. This has a corresponding impact on other economic sectors in which data is transmitted and processed electronically. This is particularly problematic in the field of machine-to-machine (M2M) communication. There, for example, personal data may not be

even affected – in the fields of goods production, inventory management, or logistics. In the upcoming discussions, it would make sense to carefully examine whether this material extension of the application of the ePrivacy Regulation is actually expedient, or whether already existing and established practices are thus undermined and innovation hindered.

- **Article 4 "Definitions"**

Article 4 of the Regulation refers to the two most relevant laws of the European Commission: the EECC and the GDPR. It is positive that the legislator pays tribute to these laws and the terms they use. However, the adoption of the definitions in the EECC (Art. 4 (1b) and (2)) is one of the central problems of the ePrivacy Regulation: The extension of the term "interpersonal communication services" to include such services which enable interpersonal communication being "ancillary to another service" (see Recital 11). This delineation is difficult as a result. The EU Commission itself specified in its presentation on 10 January 2017 in relation to social networks that only the messaging function of the platforms or services are affected by the Regulation. This led to further questioning by civil rights organisations who had interpreted the Regulation differently. What this made clear is that the current definition is very problematic and must be re-examined.

The debate shows that the provisions of the ePrivacy Regulation are unclear, for example, whether only personal communication is protected on larger platforms or whether other aspects of these platforms are also affected.

The two terms introduced in Art. 4 (3), these being the breakdown of "electronic communications data" into "electronic communications content" and "electronic communications metadata", are vague. This has led to debates about in which cases, for example, location data can be processed by whom. The definition, which was intended by the EU to be open and technology neutral, just results in lack of clarity (see Recital 14). The definition also leads to the massive problem that what the GDPR seeks to protect – personal data – has been extended to all possible forms of electronic exchange of data. It is not helpful to include the communication between two devices in the protection of privacy.

This results in a lack of clarity when it comes to dealing with electronic communication in the business and technical fields when it is between different end devices; something that was supposed to have been explicitly excluded, according to Recital 12.

This stipulation urgently needs to be re-examined and corrected in terms of its scope.

- **Article 5 "Confidentiality of electronic communications data"**

Article 5 states that "electronic communications data", as defined in Article 4, are to be treated as confidential. It greatly restricts the processing of all electronic communications data, unless permitted by the Regulation. This provision is meant to

protect “electronic communications data” as defined in Article 4 from access by persons or organisations other than the participants in communication. This approach is problematic. New, innovative ways of processing data are thereby forbidden and restricted for companies and market participants, or at least harder to implement, as consent must be sought.

eco recommends that this article is harmonised with the GDPR and examined as to whether there is even a need to specially regulate confidentiality when dealing with electronic communications data.

- **Article 6 “Permitted processing of electronic communications data”**

Article 6 formulates the exceptions mentioned in Article 5 that allow the processing of electronic communications data. The remaining spectrum for data processing is problematic. The stipulations for the processing of metadata (Art. 6 (2)) are too strict. They could also apply to the providers of other services, such as checking the quality of service.

The requirement of explicit consent for the processing of data for specified purposes (Art. 6 (2) and (3b)) is problematic, as it is too narrow. For further forms of processing in the context of communications services this would require new consent from the user.

The requirement to anonymise data in Art. 6 (3b) de facto goes beyond the GDPR, which requires data to be pseudonymised. Neither the GDPR and the ePrivacy Regulation define the term anonymisation, so this is an unspecified legal term.

eco calls for Article 6 to be examined in relation to how the consent requirements can be harmonised with the GDPR and how the GDPR’s requirement for pseudonymisation meet the requirement of anonymisation. With this in mind, it is worth exploring whether Article 6 should be substantially rewritten and whether the regulatory approach in conjunction with Article 5 – a blank ban with individual exceptions – should be changed. In its current wording, these few, narrow and ambiguously worded exceptions form a barrier to the European data economy.

- **Article 7 “Storage and erasure of electronic communications data”**

Article 7 requires that electronic communications content is to be deleted or anonymised by the provider (Art. 7 (1)) once the recipient has received it. This also applies to the metadata related to such communication (Art. 7 (2)). Both aspects are difficult. The deletion and anonymisation of communications content corresponds to our criticism that the term anonymisation (as opposed to pseudonymisation) is not clearly defined in Article 6. There are also worries that the planned requirement to anonymise or delete communications metadata will cause great difficulty for services currently offered by telecommunications service providers, such as the creation of heat maps to track network usage or malfunctions. Recital 17, however, considers the creation of such heat maps to be relevant and specifies that location data is not considered to be metadata in this context.

These points show that the stipulations of the ePrivacy Regulation are formulated too broadly and too generally, and are not suited to building up a European data economy. They even risk undermining existing practices that could be useful for expanding broadband provision and, later, for traffic planning. Article 7 should be based on Articles 5 to 11 GDPR when it comes to the storage and processing of electronic communications data. It should restrict data protection explicitly to personal data and the processing thereof, where necessary enabling further processing within the limits set by GDPR.

- **Article 8 "Protection of information stored in and related to end-users' terminal equipment"**

Article 8 regulates how the communication with end-user devices is dealt with. It also extends the protection of confidential information to areas that go far beyond the protection of personal data (see Recital 20).

A positive aspect is that the Article is formulated in such a way that it does not in general exclude business models for refinancing free services, and, e.g., allows the use of cookies to improve an offer. At the same time, the wording is vague, so that it is unclear whether certain analytical tools may be used (Art. 8 (1d)). Thus, the Regulation is unclear as to whether the analytical tools of third-party providers may be used. When presenting the ePrivacy Regulation, the Commission did explain that "analytics" is still basically possible, however this is not mirrored in the current wording.

The requirement for consent for third-party cookies is also risky, as it requires the consent of the user. Companies which offer users such products must first get numerous statements of consent. This runs counter to the needs of providers of services and products that are explicitly focused on "analytics" or on distributing advertising. A difficult aspect in regard to cookies is the interaction between the ePrivacy Regulation and the GDPR. The earlier is referring in its Article 4ff to the latter, which explicitly mentions cookies in its Recital 30. In order to avoid double regulation, only the GDPR and its delegated and implementing acts should govern how cookies and end devices are dealt with, rather than having additional regulation in the ePrivacy Regulation.

- **Article 9 "Consent"**

Consent is a central aspect of European data protection. For this reason, we welcome the ePrivacy Regulation orienting itself on the definitions presented in the GDPR. It remains unclear, though, whether the regulations in Article 9 (2) actually meet the requirements of Articles 7 and 8 of the GDPR. Should delegated or implementing acts be based on these two GDPR articles, it is unclear how they will interact with the ePrivacy Regulation.

The interplay with Article 9 (3) is also out of place. The obligation to remind end users every 6 months will result in users being flooded with requests. Whether such a reminder is in the users' interests is doubtful.

- **Article 10 "Information and options for privacy settings to be provided"**

Article 10 looks at the privacy settings of software placed on the market. We see as positive that there is the possibility to implement this requirement as part of an update cycle, which reduces the burden of implementation. The need for adaptation of the numerous computer programmes and apps that will be affected is enormous. The necessity of this article, given that Article 25 of the GDPR proscribes privacy by design, is questionable. The implementation is impossible, particularly for old and obsolete software which is no longer offered on the market. Article 10 neither considers the demands made on the software nor the reality of networked systems. Article 25 GDPR is sufficient. This Article should be removed.

- **Article 11 "Restrictions"**

Article 11 allows restrictions of Articles 5 to 8 by legislative measures of the Member States of the EU.

This gives rise to the risk that such access requests, based on the establishment of internal procedures for answering requests for access to the electronic communications data of end users (Art. 11 (2)), will lead to double regulation in the area of security by the EU and the national legislation. On the basis of the principle of subsidiarity legal requirements should be regulated on a national level. Double regulation in this sensitive area is not helpful.

There is also good reason to be worried about the "internal procedures" formulated in Art. 11 (2), including transfer interfaces to allow encrypted communication to be read.

With this in mind, it should be carefully considered whether such an article is compatible with confidential communication and with the aim to provide a high level of data protection. There must be clarification that this article does not allow governmental institutions to access data as a rule.

- **Article 12 "Presentation and restriction of calling and connected line identification"**

Article 12 of the ePrivacy Regulation governs the presentation of the identification of communications participants based on Article 107 EECC. It is not clear why this requirement was not included in the EECC and whether it contradicts Article 107 EECC, which gave national authorities this task. During the consultations on the EECC, it would make sense to consider including Article 12 of the ePrivacy Regulation in the EECC and to check whether the wording here is not already covered by the suggestion for Article 107.

- **Article 14 “Incoming call blocking”**

This article regulates the possibility to refuse to accept calls from number-based interpersonal communications services. Recital 30 explains that telephone operators, in particular, should inform customers about the possibility to protect themselves from undesired call and that they should enable this free of charge. Although such a regulation can be derived from the connection to the protection of privacy, as this is regulated by technological means, it does not belong in the ePrivacy Regulation. This could be done in the EECC or as an implementing act for the GDPR. How far the acceptance of such calls is affected by the requirement of Privacy by Design stipulated in Article 25 GDPR should be explored.

- **Article 15 “Publicly available directories”**

This article lays out standards for publishing data in publicly available directories. The EECC has already included rules for these kinds of information media. In order to have a strict and coherent regulation of information media, we would welcome these regulations being brought into line with each other. The standards of the GDPR for consent of the use of personal data must also be considered.

- **Article 17 “Information about detected security risks”**

Article 17 stipulates that operators of electronic communications services must inform their users “in the case of a particular risk that may compromise the security of networks and electronic communications services” and show them ways to help themselves, also providing an indication of any possible resulting costs. We question whether this requirement is even necessary.

On the one hand, the GDPR has rules on dealing with risky data processing (Article 9 in conjunction with Article 35) and the reporting obligation (Article 33). On the other hand, the NIS Directive ((EU) 2016/1148) includes the obligation to report incidents related to the flow of personal data (Art. 14 and 16, NIS Directive).

The system of cooperation between the providers of “digital services” introduced by the NIS Directive is threatened by the draft ePrivacy Regulation. The facultative wording “may compromise” is not helpful here, as it significantly increases the number of cases in which the obligation to inform is triggered. When it comes to communications services, it is also often not clear whether data has actually been exposed.

- **Article 29 “Entry into force and application”**

The article stipulates that the Regulation shall apply from 25 May 2018 and that all of its conditions must be complied with by then. This time frame is too short. This is quite obvious considering that numerous IT products need to be adapted, new reporting lines must be created, and corporate processes need to be reshaped. The few months between the Regulation being actually passed and it coming into force

is not sufficient time for IT companies to adequately fulfil the Regulation's requirements.

A further difficulty is that the EECC, which is referred to in various articles of the ePrivacy Regulation, is not yet passed and that delegated and implementing acts of the GDPR are still being negotiated. In this situation, it should be carefully considered whether it would not make more sense to wait to pass these laws before continuing to work on the ePrivacy Regulation. Perhaps some of the Regulation's requirements will then need to be reconsidered.

About eco

eco – Association of the Internet Industry fosters all companies that create economic value with or in the Internet and represents their interests. The association currently represents more than 1,000 member companies.

These include, among others, ISPs (Internet Service Providers), carriers, hardware and software suppliers, content and service providers, and communication companies. eco is the largest national Internet Service Provider association in Europe.