Position Paper

Bitkom views concerning the Presidency´s Discussion Papers and the latest developments regarding the ePrivacy Regulation

07/03/2018

Introduction

The Presidency of the Council of the European Union recently published Guidelines and Discussion Papers regarding the ePrivacy Regulation (ePR). The most recent document dealt with questions regarding Articles 2 and 11 of the ePR (07.02.2018, 5827/18), one discussion paper centered around options for Articles 12 to 16 (25.01.2018, 5569/18), and one focused on the Link to the General Data Protection Regulation (GDPR), the alignment with the European Electronic Communications Code (EECC) and questions regarding Articles 6, 7, 8, and 10.

Bitkom has commented on several questions regarding the ePR and on the latest Presidency Papers and would like to use this opportunity to comment on the latest developments as well.

A. Summary

The latest Presidency Papers and developments in the WP TELE and DAPIX meetings regarding the ePrivacy Regulation have shown a need for more discussions on certain aspects of the Proposal. Bitkom welcomes the Presidency´s approach to the issues in considering different options for the relevant provisions.

We would like to comment on the current framework laid out in the latest papers and the discussion in the Council and on a national level. We would like to highlight the following aspects of our Position Paper. All aspects are explained in detail below.

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Managing Director
Law and Security
P +49 30 27576 -223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Scope and Aligment with GDPR and EECC

The e-Privacy Regulation should only complement existing rules and regulatory overlaps should be minimized. Clear rules are necessary to ensure consistency with (especially) the GDPR and the EECC. This consistency is also necessary with regard to definitions. We need clarity on the definitions of the EECC and a clear scope of the ePR. The ePR must contain a very clear distinction between provisions on the confidentiality of communications and provisions regarding the processing of electronic communications data. Where processing of electronic communications data is concerned, we urge the presidency to consider the necessity of providing for additional regulation where the GDPR already provides for a clear and comprehensive data protection framework.

2. M2M Communication

M2M communication should be removed explicitly from the scope of the Regulation with regard to the processing of data. A differentiation is necessary between the necessary confidentiality of the communication process and the processing after the data transmission is concluded, especially where non-personal data is processed.

As Art. 6 stipulates a ban on the processing of data, e. g. location data, this category of data will be subject to stricter rules as provided for in the GDPR, but these stricter requirements will only to "electronic communications services". The processing of communication content between machines would therefore also be subject to the narrow exceptions. What a “machine” or “M2M communication” is and who the operator of the communication service/network is, is not definitively clarified. In the M2M context, it is also often unclear which "end user" could give consent.

3. Article 6 ePR

Regarding permitted processing under Article 6, the Presidency comments on the possibility to include the GDPR legal basis of “legitimate interests” and “further processing” for compatible purposes. We strongly welcome and support discussions on these points, as the range of permitted data processing capabilities in the ePrivacy proposal should be fully aligned with those afforded by Article 6 of the GDPR, also with regards to third parties processing personal (communication) data for a legally justified reason (e.g. to provide cyber security services).

4. Articles 8 and 10 ePR

The inclusion of any form of access to data-related activity in the user’s end device without exception chooses the broadest possible approach with regard to its regulatory scope and assumes that in principle, any data, any hardware component, and any process in the end devices can be a potential infringement of the privacy of end-users. However, not every use of storage capabilities and collection of information is critical and the consent requirements as one-size-fits all approach does not work in practice. We also urge the Presidency to consider workability and technical feasibility of Art. 8 and 10 ePR. Article 10 will especially burden browsers unduly as the provision does neither clarify the technical aspects of the settings to be provided nor clarifies how the options should be designed. Furthermore, the provision will not achieve its objective as there are already methods known

which would not be affected by the browser setting. Implementing the risk-based approach and introducing balanced provisions for processing is necessary to achieve the objective of a safe, user friendly internet while upholding the GDPRs high standard of data protection and enabling companies to use data after conducting risk analyses, pseudonymization and other safeguards. Without amendments, the ePR will burden the software and access providers, reduce the availability of diverse and free content on the Internet, reduce the quality of online content, burden browsers and other software providers as well as content providers and website operators while at the same time impairing the user experience.

5. Article 15 ePR

Article 15 ePR need to be amended to include the phrase *"operators of electronic communication services"* used in Parliament's draft, as the Council's draft of Article 15 ePR contradicts not only the Commission's and Parliament's drafts and, in particular, its intention to include the offers of OTTs, which are not or not necessarily "number-based", to these regulations, but also the wording of its own recital 30.

6. Implementation Period

We encourage the Presidency to provide businesses with a reasonable and adequate implementation period of the ePrivacy Regulation. Article 29 should therefore be amended and provide for a 2 year implementation period.

B. Detailed Comments on the Presidency´s Discussion Papers

1. Scope and Aligment with GDPR and EECC – General Approach

The e-Privacy Regulation should only complement existing rules and regulatory overlaps should be minimized. Clear rules are necessary to ensure consistency with (especially) the GDPR and the EECC. This consistency is also necessary with regard to definitions (f.i. the definition of consent under the GDPR and definitions in the European Electronic Communications Code (EECC)).

As context and scope of the ePR are closely linked to the definitions of electronic communications in the EECC, we urge the Presidency to first continue and complete the discussions on the definitions of the EECC to clarify the framework and applicability of the ePR. Without definite definitions in the EECC, the scope of the ePR remains unclear.

The ePR needs to ensure flexibility for future business models, while upholding the confidentiality of communications. It therefore has to be technology neutral and should implement the well-proven risk based approach, when it comes to the processing of data.

The ePR must contain a very clear distinction between provisions on the confidentiality of communications and provisions regarding the processing of electronic communications data. The confidentiality of the communications (i.e. the transmission of data) is a legitimate goal and should be applicable to all electronic communications. Nevertheless, a restriction of processing of personal data should not implemented per se, but only for very limited exceptions and only if personal data is involved to reduce conflicts with GDPR.

We urge the Presidency to clarify the scope of the provisions of the ePR. Furthermore, processing of personal electronic communications data should not only depend on consent, but must be lawful when based on other legal grounds as well, as it is already the case under the GDPR. The risk based approach would allow for a graduated approach to processing personal data and making controllers more responsible in assessing the risks of their processing operations. A broader reflection on the general approach of the ePR might therefore be necessary.

We therefore strongly agree with the Presidency that the relationship between GDPR and ePR and EECC need clarification. Clarity is needed in order to avoid legal uncertainty due to possible duplications and contradictions between the frameworks.

2. M2M Communication

M2M communication should be removed explicitly from the scope of the Regulation with regard to the processing of data. A differentiation is necessary between the necessary confidentiality of the communication process and the processing after the data transmission is concluded.

Confidentiality of communication is, of course, also desired for machine data (confidentiality is already laid down in Art. 5 of the ePrivacy Directive). This, however, should not lead to the general prohibition of the processing of non-personal data, where transmission is facilitated between non-personal communication operation, such as M2M communication. Machine data without personal references (measurement data, latency times etc.), only generate insights and value for the recipient who can assign and decrypt the data have a completely different quality than personal data as such. Only personal data can give rise to the personality right and informational self-determination which data protection aims to protect.

3. Article 6 ePR – Need for Amendments to Align the Provisions with the GDPR

Regarding permitted processing under Article 6, the Presidency comments on the possibility to include the GDPR legal basis of “legitimate interests” and “further processing” for compatible purposes. We strongly welcome and support discussions on these points, as the range of permitted data processing capabilities in the ePrivacy proposal should be fully aligned with those afforded by Article 6 of the GDPR, also with regards to third parties processing personal (communication) data for a legally justified reason (e.g. to provide cyber security services).

3.1. Consent

For content data, in many instances it will not be technically feasible to get the consent of all end-users, i.e. where two individuals exchange emails using different email providers, since the service provider will have a customer relationship with only one of the persons. For metadata, processing large amounts of data - often in real time – for example to optimize infrastructure or traffic management will also not be usable when restricted to purely consent-based solutions, since a critical volume of data is needed to be able to provide meaningful analytics. Such analysis does not depend on the identification of individual persons; however, a full anonymization would delete the unifying identifier (pseudonym) which is needed to get valuable and innovative conclusions. Therefore, the balancing of interests and a further processing for compatible purposes in accordance with Article 6 (4) GDPR should be allowed and pseudonymous solutions should be privileged. The abovementioned risk based approach can be a useful tool in that regard as it enables the processing while always protecting the interests of the data subjects. The protection of the data protection can indeed be considered as being higher than if the processing if (only) based on consent, because the processor then does have to apply certain measures to ensure the processing balances the interests and considers the possible impact on the data subject.

It should be clarified that consent to the processing of electronic communications data, may be given at the time of subscription with a one-off consent for processing of personal electronic communications data for the duration of the subscription. This is especially relevant for legal persons to ensure that B2B services can be delivered seamlessly and as requested.

3.2. Metadata should not be considered as “Special Categories” of Data

Furthermore, it is important to state that metadata are not sensitive personal data per se. As the CJEU held in its Tele2 judgement (judgement of 22.12.2016) sensitivity depends on scope, context, purposes and (lack of) safeguards of the processing to determine the sensitivity of personal data. Moreover, Art. 9 of the GDPR contains an exhaustive list of special categories of personal data and therefore exhaustively lists the types of data that are sensitive per se. This list, however, does not include metadata. In our view, the assessment that communications data (metadata) constitutes sensitive data per se, is therefore legally and factually incorrect. The special categories of data enumerated in Article 9 have a strong connection to discrimination prevention (health data, data on sexual orientation or political views etc.), which cannot be said for metadata of electronic communications. And while metadata can, under certain circumstances, be used to, inter alia, generate user profiles, this does not justify the conclusion that metadata are sensitive data or have to uphold the higher standards that are provided for special categories of data (nearly all data can be used to generate profiles of users, which is already extensively addressed in the GDPR, but that argument alone does not support the conclusion that the data is sensitive).

3.3. Scope and Relationship between Art. 6 and 8 ePR

Lately there have been some discussions on whether the current version of Art. 8(2)(c) of the Councils Draft already includes processing that would otherwise fall under a “compatible” processing. We would disagree with such an assessment, as the wording of Art. 8(2)(c) and the corresponding Recital 25 suggests that this provision refers only to wifi signals and not to signals for the connection with mobile telephone services. Recital 25 states centers around signals from terminal equipment in clearly defined and confined spaces. Furthermore, the Recital introduces the obligation to use prominent notices to inform the user on the edge of the area. Use Cases such as smart city planning are, however, not confined in space. The provision of Art. 8(2)(c) would not be applicable in our view. And even if it where applicable, it would not be possible or practical to display notices on every street corner or mobile phone zone.

Moreover, if such processing would fall under Art. 8(2), the relationship between Art. 6 and Art. 8 and the scope of both articles becomes even more unclear. This can be seen in Recital 17 (corresponding to Art. 6(2)) where heat maps are mentioned that are built by processing data from mobile telephone services. Mobile phones regularly send signals to connect to the mobile network. This is done in order to ensure general accessibility, but also on a case-by-case basis when a concrete connection to communication is established. Pursuant to Art. 4(3)(c), metadata includes "the data generated in connection with the provision of electronic communications services concerning the location of the device". Recital 17 also includes location data generated for the purpose of maintaining access to the service. Consequently, metadata also includes the signals sent for connection to the mobile network. However, this would mean that, in addition to the requirements of Article 8 (2)(c), the requirements of Article 6(2)(e) would also always have to be met. This cannot be the intention of the legislator or the Commission, especially since the requirements differ. We urge the Presidency to find clarification on that point and include an opening for processing equivalent to Art. 6(4) GDPR in Article 6 of the ePR.

Another point to be considered in that regard is the fact that purely statistical processing is a far too narrow approach and would be restricted further by the restrictive interpretation of statistical purposes provided by Article 89 of the GDPR. Therefore, a reference to a compatible further processing according to Art. 6(4) GDPR (with pseudonymization as a protective measure) is still the most suitable option. We ask the Presidency to keep the dialogue open on that issue to find a suitable solution.

4. Articles 8 and 10 ePR – Further Discussions on Technical Aspects and Practicality

4.1. Article 8 – Amendments Needed to Provide for Necessary Exceptions

The inclusion of any form of access to data-related activity in the user’s end device without exception chooses the broadest possible approach with regard to its regulatory scope and assumes that in principle, any data, any hardware component, and any process in the end devices can be a potential infringement of the privacy of end-users. However, not every use of storage capabilities and collection of information is critical and the consent

requirements as one-size-fits all approach does not work in practice. The Council should allow for more exceptions in Art. 8 and not create barriers to the legitimate use of devices.

Article 8(1) ePR should especially be amended to provide for the following cases:

e) It is necessary for a software license check that a user must perform on the end user's end devices. (Example: Company (user) conducts checks of software products that are subject to licensing on the PCs that are used by employees in the context of their work (end user) in order to prevent license violations)

(f) It is necessary to collect information on the use of the programme in order to assist its users and to improve software products.

4.2. Article 10 –Technical Feasibility stands in Question

Bitkom urges the Presidency to consider facts regarding the technical feasibility of the provisions in the ePR, especially the proposed Art. 10 ePR. The current provision proposes that the user must consent to all storage of information on the terminal equipment of an end-user as well as to the processing of stored information alike, as long as it is not strictly necessary for certain reasons (e.g. the transmission of data). This does refer to all possible storage and processing purposes (e.g. if information needs to be stored and processed on company mobile devices to carry out job-related tasks) on a global scale alike, among others by the restrictive pre-settings when installing not only browser software, but all software and apps enabling electronic communication in any form (Art. 10). This would be a barrier to the usage of mobile devices for job purposes, as new features from third parties (e.g. to analyze machine data to give advice to engineers using tablet devices to carry out complex maintenance tasks in an industry 4.0 environment, security enhancements) must be installed independent of the consent of the employee. Company mobile devices are globally managed, maintained and updated globally, to make sure that employees can work with the latest tools and apps, and that private data and company data is separated, to ensure compliance and private use of mobile devices (if requested by the employee).

Further, the proposed pre-settings would effectively ban content providers and website operators from providing personalized content and marketing especially digital advertising, which is necessary for millions of providers and operators to finance their websites. It is furthermore not clear whether the browser settings would allow for even necessary (f.i.) cookies to be placed on the users terminal equipment and whether web audience measuring could take place if the even if the pre-settings prohibit all storing of information on terminal equipment. The currently discussed solutions such as whitelisting by the browsers, an override function for content providers or consent mechanisms do not address the issue in full and do not provide for a comprehensive solution. There need to be a technical debate on function and practicality with all the relevant stakeholders. Is also has to be clarified how the processors could document the given consent as they do not know which user gives his or her consent (outside of log-in systems).

Furthermore, it is often argued that Art. 10 is only an extension of Art. 25 of the GDPR (Privacy by Design) but Art. 25 provides for rules regarding the controller. Art. 10 ePR however, relates to the software provider or the browser. But the browser is not responsible or in control of processing operations, tracking methods used by the content providers or website operators.

5. Article 15 ePR – European Parliament´s Approach preferred

In our view, Article 15 needs to be amended to match the European Parliament´s proposal. In the Council´s current version of the text, Article 15 states that *"The [providers of publicly available directories] providers of number-based interpersonal communications services shall obtain the consent of give end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data the opportunity to determine per category of personal data whether their personal data are included in the publicly available directory...".*

The wording "providers of number-based interpersonal communications services" restricts the applicability of Art 15 to just these providers, i. e. to classic telecommunications providers whose offers are based on the allocation of classic telephone numbers - in fixed or mobile telephone services. The draft version of the EECC does also include such a restriction. Neither the Commission's original ePrivacy draft nor the Parliament's draft did provide for such a restriction on traditional, solely number-based offers of providers.

The Council's draft of Article 15 thus contradicts not only the Commission's and Parliament's drafts and, in particular, its intention to include the offers of OTTs, which are not or not necessarily "number-based", to these regulations, but also the wording of its own recital 30, which expressly states: "Publicly available directories means any directory or service or service containing categories of end-users information personal data such as name, phone numbers (including mobile phone numbers), email address contact details, home address and includes inquiry services". E-mail addresses and applications are expressly mentioned here as non-number-based services, such as e-Post and De-Mail in Germany. Also, there are already communication services where the search function can be used not only to search for numbers, but in particular for user names (even if the basic service behind it is based on a (still) number-based service, a future-oriented wording of Art 15 must and should be applicable in any case. In addition, it must be expected that future electronic communications services installed will no longer be based on number-based technologies, but will use user names or other systems that should already be covered by the ePR.

For the German directory providers, for example, there was and still is an interest in integrating the offers of the mentioned e-mail service providers into directory services. Art. 15 ePR should therefore be amended to include the phrase *"operators of electronic communication services"* used in Parliament's draft.

6. Implementation Period

Last but not least, we encourage the Presidency to provide businesses with a reasonable and adequate implementation period of the ePrivacy Regulation. Article 29 should therefore be amended and provide for a 2 year implementation period.