Position Paper – ePrivacy Regulation

Bitkom views concerning the first Finnish Presidency´s Discussion Paper 10753/19

01/07/2019

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

The Finnish Presidency of the Council of the European Union recently published its first Presidency Discussion Paper (10753/19) regarding the ePrivacy Regulation (ePR).

Bitkom welcomes the steps already taken on the text of the ePrivacy Regulation but thinks there are still many unresolved areas and the file needs further work and in depth discussion. A clear, coherent and future-proof text is needed to move on to trilogue discussions. We therefore welcomed the Presidency´s working plan and the objective to continue the negotiations on the ePrivacy proposal and further the discussions as far as possible with the aim to ensure high quality of the legislation.

The state of the discussion on the proposal has been recently summarized in the progress report by the Romanian presidency (9351/19). Considering the report and also the reflections and discussions on certain aspects of the proposal, it is clear that further discussion is still needed. In their first Presidency Paper on the ePrivacy proposal, the Finnish Presidency invited the Member States to express their views on the next steps to be taken and the following questions:

1) The main objective of the proposed regulation is to protect the fundamental right of private life and confidentiality of the communications. To this end, which parts of the proposed regulation could be considered as the most essential?

2) On which parts of the text more discussion is still needed? As the text stands now we would like to especially have your views on:

- which parts are the most problematic and how can those problems be concretely solved?

- can some parts be identified where no changes are necessary ?
- Are there some parts of the text you consider unnecessary and which should be deleted?

3) Some delegations have indicated that further alignment with the General Data Protection Regulation and ePrivacy rules would be needed. In this regard, what kind of specific changes to the text would be needed?

4) What should be the next steps to be taken to continue the negotiations in the Council?

As Bitkom has always provided comments and industry insights on several questions regarding the ePR, we would like to use this opportunity to comment on the latest developments as well.

1. Core Aspects and essential Parts

Question 1: The main objective of the proposed regulation is to protect the fundamental right of private life and confidentiality of the communications. To this end, which parts of the proposed regulation could be considered as the most essential?

As the GDPR already introduces a very high level of protection of personal data, the rules on ePrivacy compliment with regard to the confidentiality of communications. Therefore, any remaining open aspects should be based on a coherent and clear text before entering in the trilogue phase. Where the EU Electronic Communications Codex (EECC) already introduced new rules, an assessment should take place on parallel rules in the ePrivacy Regulation.

While the protection of confidentiality of communications is of course an important objective of the proposed regulation, one of the main issue with the draft remains that it does not distinguish between the confidentiality of communications and a ban / overly strict rules on data processing. The scope of application is still unclear, which will create considerable legal uncertainty, as providers cannot assess when the communication and transmission process ends and from which point in the process the GDPR rules can be applied. Recital 12 in the current text does not provide enough clarity on the question, when the transmission process is concluded and the application process begins. This distinction, however, is crucial to assess whether the rules of the ePrivacy Regulation apply or those of the GDPR. Furthermore, the interplay of the ePrivacy rules with the GDPR provisions on consent, processing and anonymization is still unclear (as the scope includes legal persons and non-personal data) as well as correlations to the EECC. Where the ePrivacy rules go beyond what is provided in the EECC and overlap with GDPR provisions, providers need certainty on which rules apply (and which authority is competent).

2. Further Discussions

Question 2: On which parts of the text more discussion is still needed? As the text stands now we would like to especially have your views on:

- *which parts are the most problematic and how can those problems be concretely solved?*
- *can some parts be identified where no changes are necessary ?*
- *Are there some parts of the text you consider unnecessary and which should be deleted?*

Question 3: Some delegations have indicated that further alignment with the General Data Protection Regulation and ePrivacy rules would be needed. In this regard, what kind of specific changes to the text would be needed?

Question 4: What should be the next steps to be taken to continue the negotiations in the Council?

As one of the core aspects needing further discussion is the alignment with the GDPR and the scope of the ePrivacy Regulation and the aspects still to be discussed are, in our opinion, the starting point for all further discussions and next steps to be taken in the Council Questions 2, 3 and 4 will be answered conjointly in this part of our Position Paper. We summarized the core aspects (see para 2.1) and provide comments and suggestions on specific parts of the Proposal (see paras 2.2 to 2.8).

2.1 Summary of the core aspects needing further discussion

From our point of view, certain aspects need further discussion:

- The relationship between the GDPR and the ePrivacy Regulation must be clarified and coherence established.
- Software updates must not be subject to new consent requirements and questions regarding the "end-user" characteristic must be clarified; it must be possible for legal entities to give consent for employees working in the company within the framework of business use. Furthermore, we need clarification that software updates fall under Article 8 para 1 lit. c.
- The potential for innovation must be preserved, particularly opportunities in the field of AI, autonomous driving and developments of IoT platforms must not be obstructed; this requires above all the further processing of data for compatible purposes and coherent

rules for M2M-communications. With regard to end-users being legal persons, it should be clarified that the basis for processing may take the form of a contract.

- As the GDPR already introduces a very high level of protection of personal data, the rules on ePrivacy compliment with regard to the confidentiality of communications. Therefore, any remaining open aspects should be based on a coherent and clear text before entering in the trilogue phase. To date, the ePrivacy Regulation also still lacks clarification as to who is an "end-user" and thus, for example, is able to give consent. With regard to Article 4a para 1 and 1a we need clarification that the contractual relationship between a legal person (f.i. the employer) and a service provider (contractual partner) is a valid basis for processing electronic communications data. In line with GDPR requirements, the current provisions should be amended to allow for the distinction between consent and contractual basis. The question is particularly important in the business context, as it is absolutely necessary for companies/legal entities to be able to decide, e.g. on updates or the use of (new) software in the company. It is therefore necessary to expressly allow the permission (in the form of the contract) to process the relevant data being given by the contractual partner of the software provider: the company. It should be clearly stated that the legal entity is the 'end-user' in case that electronic communication services and terminal equipment are used for business purposes. We suggest introducing that if a legal person subscribes to business-related electronic communications services or network, consent may be obtained from the legal person concerned, and not necessarily from the individual user. If terminal equipment of the legal person is used in the business-related context by a natural person, consent must be obtained from the legal person as the end-user. The legal person shall respect the rights of those other end-users in accordance with Regulation (EU) 2016/679, employment and other applicable laws.

2.2 Comments on Article 4a

To date, the ePrivacy Regulation also still lacks clarification as to who is an "end-user" and thus, for example, is able to give consent. With regard to Article 4a para 1 and 1a we need clarification that the contractual relationship between a legal person (f.i. the employer) and a service provider (contractual partner) is a valid basis for processing electronic communications data. In line with GDPR requirements, the current provisions should be amended to allow for the distinction between consent and contractual basis. The question is particularly important in the business context, as it is absolutely necessary for companies/legal entities to be able to decide, e.g. on updates or the use of (new) software in the company. It is therefore necessary to expressly allow the permission (in the form of the contract) to process the relevant data being given by the contractual partner of the software provider: the company. It should be clearly stated that the legal entity is the 'end-user' in case that electronic communication services and terminal equipment are used for business purposes. We suggest introducing that if a legal person subscribes to business-related electronic

communications services or network, consent may be obtained from the legal person concerned, and not necessarily from the individual user. If terminal equipment of the legal person is used in the business-related context by a natural person, consent must be obtained from the legal person as the end-user. The legal person shall respect the rights of those other end-users in accordance with Regulation (EU) 2016/679, employment and other applicable laws.

2.3 Comments and suggestions on Article 6

The enormous innovation potential of new technologies must be preserved. Especially opportunities in the field of AI and data analytics must not be obstructed. The further processing of data for compatible purposes is above all necessary in order to promote and maintain this potential; technical safeguards such as pseudonymisation offer suitable protection mechanisms in line with GDPR and its risk-based approach. We therefore welcome all the work that has been done with regard to Article 6 and the processing of communications metadata. We especially recognise the improvements made in Article 6 para 2 lit a with regard to the principle further compatible processing and, more in general, to the whole structure of Article 6 governing the processing of electronic communications data.

The new Article 6 para 1 lit c will make machine-to-machine communications and the Internet of Things safer. Electronic communications data can then be processed to protect the devices connected to the network against security threats and attacks, and not only the security of the network as such as per Article 6 para. 1 lit b. We therefore welcome the improvements made in this regard.

Article 6 para 2aa lit. c contains a clarification referring to Article 35-36 GDPR which brings the proposal for further compatible processing more in line with the GDPR's risk-based approach whereby the result of a Data Protection Impact Assessment determines whether a consultation of the DPA is necessary (i.e., the processing would result in a high risk in the absence of measures taken by the provider to mitigate the risk). However, we would like to emphasize some outstanding concerns regarding Article 6 that need to be addressed in the new Presidency proposal:

- Article 6 para 2a, last sentence: The condition that processing be allowed only when it does not lead to user profiling should be complemented as follows: "the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user which produces legal effects concerning him or her or similarly significantly affects him or her". This would further align this restriction to the risk-based approach and the language of Article 22 para 1 GDPR on automated decision-making, to achieve legal certainty and focus on what directly affects the privacy of end-users.

- Article 6 para 2 lit. f: The requirement that processing for statistical purposes is only allowed if based on EU or Member State law risks resulting in a fragmented application of rules, thus jeopardising the harmonised approach of the ePrivacy Regulation. This reference (to EU Member State law) should therefore be deleted. Processing of metadata for statistical purposes should follow the logic of Article 5 para 1 lit. b GDPR, which stipulates that such processing, in accordance with Article 89(1) GDPR (as referenced to by the draft Regulation) should be presumed to be "compatible" with the initial processing purposes.

- Article 6 para 1 lit. c could be complemented with a clarification for IoT services. Because the IoT value chain consists of both ECS providers and non-ECS providers, Articles 6 and 8 need to be aligned in terms of data processing possibilities. Otherwise there will be a disruption for IoT data processing, undermining the services offered (eg connected driving). Within Article 8, also paragraph 2 needs to reflect the contract legal basis in Article 6 para 2 lit. b; particularly since Article 8 para 1 aims mostly at cookies. Information emitted by terminal equipment to enable it to connect to another device (= paragraph 2) will in most cases refer to machine-to-machine communications. In order to futureproof this Regulation for IoT communications, it is proposed to insert this legal basis which could be assimilated to the contractual legal basis under GDPR, thereby providing more consistency, and reflecting Recital 21.

- Article 6 para 1 lit. d: Voluntary scanning for child sexual exploitation and abuse imagery (CSEAI), or potentially even terrorist content, for example, is still potentially prohibited, or, at best, subject to a patchwork of divergent national laws and codes. The introduced processing ground is unclear und will not facilitate what it was introduced to do without further in depth discussions. We propose that this be dealt with explicitly via a specific new carve-out in Article 6 para 1 that excludes specific use-cases but includes a legal base that allows processing to take place "in compliance with a legal obligation"

- Article 6 para 3: Processing of communications content pursuant to Article 6 para 3 for general training and improvement of machine learning algorithms and other innovative features that deploy artificial intelligence remains prohibited absent user consent. Given the nature of these technologies, specificity of consent may not be achievable to enable the full advantages of AI and ML to be realised, even where all appropriate steps are taken to anonymise and minimise data collection and processing. The lack of flexibility in the current Article 6 para 3 wording fails to correspond with stated EU objectives and Member State strategies for AI and should therefore be amended to include additional processing grounds for content that are (i) as a minimum equivalent to those most recently added to the text of Article 6 para 2 for metadata (including "further processing" wording) and (ii) consistent with GDPR.

- Article 6 para 3 lit. b should be amended with regard to the phrase "if all end-users concerned" as the provider will only be able to get consent from his own customers/users.

Articles 6 and 8 should also be discussed again with regard to the influence on M2M communications. Machine-to-machine communications includes a vast array of disparate devices and services, making inflexible rules under the ePR framework particularly difficult to implement. Broadening the scope to a broadly defined M2M could mean that various products and services that contain built-in M2M communication features - like automated supply chains, remote control or distance operation of machines - might be covered by the legislation. This appears inconsistent with the purpose and objective of the ePR and would unnecessarily lead to unworkable situations and potentially render standard processes and developments of Industry 4.0 laborious or impossible.

In this context, Recital 19 needs further work as well and should be amended to include the following: "This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit for the purpose of providing a service, with the informed consent of the end-user who requested that service."

2.4 Comments and suggestions on Article 7

With regard to fraud detection, further discussions are needed on Article 7 para 2. The provision stipulates that metadata need to be erased or made anonymous when no longer needed for the purpose of the transmission of the communication. Exceptions from such obligation are granted for security and technical faults (Article 6 para 1 lit. b), mandatory quality of service (Article 6 para 2 lit. a) and user consent (Article 6 para 2 lit. c). However, if there is a legal ground to use metadata under any of the provisions under Article 6, this should not be superseded by an obligation to delete the content or metadata immediately after transmission. For example, detection of fraudulent use is permitted under Article 6 para 2 lit b., but is not carved out from Article 7 para 2. This would result in the obligation to immediately erase the data after transmission of communication which would hinder providers to successfully detect fraudulent or abusive use. In addition, the GDPR already foresees that personal data can only be used to fulfil the purpose of processing. Once the purpose has ended, personal data can no longer be processed.

2.5 Comments and suggestions on Article 8

There is still work needed with regard to Article 8, especially in the context of software updates and in particular the rules on consent for data processing operations and software updates. We strongly recommend an amendment of the provisions for several reasons. Firstly, Article 8 para 1 lit. e and Recital 21a seem to presume the existence of updates that serve no purpose other than fixing security vulnerabilities. Software updates, however, often also fix other bugs, improve

functionalities or settings etc. This is primarily for the convenience of the user as this reduces update-related service restrictions and downtime. Many of the issues caused by outdated software will not be addressed by security updates alone. Instead, they require updates to address other bugs, performance and design and functionality issues.

From a practical perspective - there are no ´pure´ security related updates and all updates would require consent, even if such updates do in no way alter privacy settings of the installed software. Furthermore, the Recitals reference to consent would mean that software provider have to comply with the requirements of Article 7 GDPR, with all its requirements and documentation obligations, no matter whether the update has any impact on the privacy settings of the software. For example, an update to a software in a car, adding new features to a parking assistant or merely increasing the precision of the assistant, would require consent of the end-user (every single driver using the car?) of the car with all formal requirements under Article 7 GDPR.

Furthermore, a clarification should be introduced that software updates fall in the scope of Article 8 para 1 lit. c. Recital 19b and 21a, however, need to be amended to mirror this provision. Most importantly, it is still unclear how companies would be able to update their computer systems and software if every update needs the consent of the end-user (Recital 19b implies that the individuals consent is needed). The EP assumes that only natural persons are end-users and therefore able to consent which would mean that every single employee has to allow an update for the software used for their work station and that companies may no longer be able to give their own consent as soon as an individual is involved. Every employer would then be dependent on the consent of his employees if an app that is needed in the job is to be updated, new programs are to be installed on end devices, data from tablets have to be queried (GPS data of working machines), or even just the centrally maintained employee contact list that is stored on the mobile phone is updated. This would not only be impractical but also pose a security risk.

With the current text, it is therefore still unclear how software updates will get delivered to the terminal equipment of end users, particularly if they do not contain a security component (also mentioned above, comments on Article 4a and Recital 19b). At the very least, corresponding recitals should be amended to clarify that current software-as-a-service (SaaS) business models – which provide updates beyond and unrelated to data collection - to are not disrupted.

Article 8 para 1 should read: “The use of processing and storage capabilities of terminal equipment and the collection of information from end-users´ terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited except on the following grounds: (e) it is necessary for a ~~security~~ **software** update**s** provided that: (i) ~~security~~ **the** updates ~~are necessary and~~ do not in any way change the privacy settings chosen by the end-user ~~are not changed,~~ **and** (ii) the end-user is informed in advance each time an update **will be** ~~is being~~ installed **except where this is not possible due to limitations in the user interface or lack of a user interface**~~,~~

~~and (iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates.~~

The corresponding Recital 21a needs further work as well and should be amended to include the following: "Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs **or to otherwise update the software (for example, to make legally-required changes, render the software more accessible, add new features or improve performance),** provided that such updates do not in any way change ~~the functionality of the hardware or software or~~ the privacy settings chosen by the end-user ~~and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception.~~

Correspondingly, Article 4a para 1 should be amended to clarify the application of consent "mutatis mutandis" to a legal person: if the end-user is a legal person, the contract with this legal person shall serve as basis for processing. This will be particularly helpful in complex (f.i. IoT value chain) relationships (which are often B2B2C) and where data will need to be processed by both legal entities, and not all have a direct relationship with the end-user to obtain consent (controller and processor concepts are not used in the ePrivacy Regulation). The IoT value chain is complex and multi-layered and this clarification would help in addressing this. Further discussions on Article 4a para 3 are also needed. The requirement in Art 4a para 3 that end-users shall be reminded to withdraw their consent every 6-12 months, unless the end-user requests not to receive such reminders, will contribute to consent fatigue and unnecessarily interrupt user journeys without providing more privacy protection. GDPR gives data subjects the right to withdraw consent at any time, even in the context of processing special categories of data under Article 9 GDPR such as health data. Inconsistency with GDPR will create regulatory uncertainty. In practice, this obligation will also lead to consent-reminder fatigue for the end-users. The reference should therefore be deleted.

With regards cybersecurity, the progress achieved by the Austrian Presidency in Recital 8 and in Article 2 para 2 lit e and f improve the text considerably and address the necessary cybersecurity considerations. However, an additional amendment of Article 8 is necessary to complete the cybersecurity-related work on Article 8 para 1 lit da. We suggest the deletion of the words "of information society services". This change is necessary to enable the intervention on the terminal equipment in order to protect it from malicious software/viruses and other attacks. These threats appear at the terminal device and are not necessarily linked to a particular information society service. For example, they could be related to a supply chain attack (e.g. installation of software or

hardware that is already compromised). This amendment will achieve the same goal like with the inclusion of "information society services" but makes it broader and therefore more technology neutral, more future proof to address other/new threats such as fraudulent use of online services. The proposed change would result to the following wording: "(da) it is necessary to maintain or restore the security ~~of information society services~~, prevent fraud or detect technical faults for the duration necessary for that purpose".

In addition, we suggest amending the provision of Article 8 para 1 lit. d, as it does not mirror the different contractual relationships built for the relevant processes that are run by contracted third parties and not by the service providers themselves.
In our view, the specific reference to Article 28 GDPR ("processors") unnecessarily pre-empts the legal relationship between the service provider and the (audience analytics) provider, who could also be seen as "jointly" controlling the data. Therefore, we suggest the deletion of the reference to Article 28 GDPR.

2.6 Comments and suggestions on Article 11

In our view, much more discussions are needed with regard to Article 11.
In particular, the following areas need to be resolved:

- Data retention: The Austrian Presidency's draft Progress Report flags (at paragraph 9) this issue, but it requires much more discussion and debate in light of the detailed case law (Tele 2, Breyer) on this topic since the ePrivacy Directive came into force.
- Extension of scope: The extended definition of ECS (adopted from the EECC), together with the extra public interest grounds laid down in Article 11, represents a material (yet unclear) possibility for the extension of surveillance powers.
- Interaction with other laws, especially the relationship between Article 11 and the GDPR and Law Enforcement Regulations need clarification.
- Encryption: The European Parliament has shown a clear preference for ECS providers to use state of the art technical measures, including end-to-end encryption of electronic communications data to guarantee the confidentiality and integrity of electronic communications. The inherent tension between this and an extension of surveillance needs to be further discussed and resolved before discussions with Parliament can advance.

2.7 Comments on Article 18

With regard to the competent authority, it is unclear which authority will be competent when the processing relates to both personal and non-personal data.

In this respect, a clarification is necessary as to whether only the supervisory authority competent under the GDPR should be competent or - as para. 2 suggests - two or more supervisory authorities which cooperate should be competent. In our view, a restriction to one competent supervisory authority would be desirable.

2.8 Comments on Article 29

We welcome that Article 29 was amended to allow for a 2 year period between entry into force and application of the new rules.