Position Paper – ePrivacy Regulation

Bitkom views concerning the Presidency´s Discussion Paper 10975/18

17/08/2018

The Austrian Presidency of the Council of the European Union recently published its first Discussion Paper (10975/18) regarding the ePrivacy Regulation (ePR). The document deals with Art. 6, 8 and 10 and their related Recitals.

Bitkom welcomes the new approach of the Austrian Presidency, especially because many questions are still open and even though the previous Presidency successfully specified and clarified some aspects, a full analysis with regard to legal certainty, practicability and the necessary alignment with the GDPR was not yet achieved. 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.

Introduction

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. Especially Art. 6, 8 and 10 are rather complex and raised a number of concerns. In our view, the ePR needs to take future business models and key technologies such as Artificial Intelligence, Machine Learning and IoT into account and secure the European competitiveness in this regard. We therefore highly appreciate the reference made in section II. of the Presidency Paper and the introduction of a possibility for further compatible processing of electronic communications metadata in the new Art. 6(2a) and would like to provide some input on the Presidency´s request to indicate examples of the use of further compatible processing in practice and would also like to comment on other issues regarding the current state of the ePR and its Art. 6, 8 and 10 and their related Recitals.

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of 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. Artificial Intelligence and the ePR – Article 6

Artificial intelligence (AI) is the concept used to describe computer systems that are able to learn from their own experiences and solve complex problems in different situations. Without data, in many cases personal data, the systems are not able to learn and become intelligent. The same applies to Machine and Deep Learning.

AI and further processing

AI and ML are used in a variety of situations. Research in the context of health applications shows great promise for AI systems for better diagnose or recognition software that diagnoses cancer in tumors. ML can also be used to build models that identify the risk of tax or social fraud. Image and voice recognition software can help built better smart assistants used to facilitate easier ways to plan schedules or perform translations in real time. Car to x communications can take autonomous decisions with regard to street quality, obstacles, weather conditions etc. The basis for such technologies is data. But data has to be collected for a specific purpose. The purpose and potential of processing communication data sometimes changes, depending how the ML system develops and learns. Data collected to e.g. analyse a tumor structure could be used – if the ML would discover a pattern for example – to help prevent liver failure. Also, if electronic communications metadata was collected to provide and maintain the service, it could not later be used to improve the service (if the ML analyzed that data and discovered a need for change in functionalities for instance). Such a procedure would encompass a change in purposes for the processing. GDPR allows such a change under specific circumstances in Art. 6(4), which enables processing without prior consent if considered compatible with the initial processing purpose.

But ePrivacy does not provide for a legal basis for processing for compatible purposes – if the provider falls within the definitions of electronic communications service he could not further use the data from the communication process for ML and AI techniques, as ePR does only provide for legal grounds for the initial processing in very narrow circumstances. The scope of the ePR does explicitly encompass services used for the conveyance of signals such as transmission services used for the provision of M2M services, which would encompass many M2M and IoT-platforms. Their AI programs and research would basically always fall under ePR instead of GDPR and hamper all AI and ML research and development.

Also, everyday uses might be endangered as well. If a company wants to develop automating aspects of its services it already offers to its customers, it would have to, under ePR, ask for consent every time the company wants to add new functions such as new recommendations to the customers use of service.

ML processing regularly forms a secondary purpose for using the data originally processed for e.g. contract performance. For these cases, Art. 6(4) GDPR) provides a frame that can enable such processing: it establishes further compatible processing as a mechanism for ECSPs to reuse personal data for a new purpose other than the

one which they've initially collected the data for, on the condition that this new purpose is compatible with the initial one. To assess compatibility, the GDPR provides for a number of factors, for instance the use of pseudonymisation as an appropriate safeguard, the consequences of such processing and the link between the two purposes or the context in which the personal data has been collected (e.g.: existing relationship between data subject and data controller). If compatibility is given, no new legal basis separate from the one that allowed the original collection of personal data is required for the processing (see also Recital 50 GDPR).

Such processing under GDPR adequately protects the interests, rights and freedoms of the individual. Implemented in the ePR, such a provision would provide for transparency and choice. It is a concept that allows – if certain conditions are fulfilled – ECSPs to re-use data that they have already lawfully processed based on one of the other initial legal bases (e.g. billing purpose or technical transmission of the network). To address any concerns about this concept in relation to communications metadata, it is recognized that the approach taken by the Austrian presidency clearly goes beyond Art. 6(4) GDPR, as it foresees a set of compulsory safeguards (pseudonymization, no profiling) for the further processing of metadata. In addition, the GDPR principles (purpose limitation, data minimization, storage limitation, integrity of the data) and end-user rights (rights to erasure, to access, to rectification, to object) continue to apply – just as they would apply to Art. 6(4) GDPR. In support of and trusting in the principles promoted by GDPR, many companies have invested heavily in privacy by design measures such as pseudonymization and therefore welcome a risk-based approach that would enable a more flexible approach towards data processing, as long as risks can be mitigated through appropriate safeguards.

Further processing of content data

In addition, in order to further align the ePrivacy Regulation with the provisions of the GDPR, we suggest another amendment: Enable further processing of e-communications content data.

Compatible further processing of electronic communications content data enables innovative digital technologies to be developed and refined in Europe and provides industries, in particular small and medium enterprises (SMEs), with the opportunity to compete on a level playing within an increasingly competitive global market.
Several examples can be drawn of the benefits of such processing, in particular with relation to enabling accelerated machine-learning in the cloud. These benefits can relate to private life, home, environment, etc. For example, it allows for the deployment of applications that enable voice-controlled and hands-free operation of technology, the categorization of correspondence based on content, translation of material to and from a foreign language, the enhancement of the consumer experience in the retail environment through the input of product preferences by the end-user, accurate indexing of content data such as photos which could be used for national security purposes, and others.

The ePR so far has ignored both the concept of compatible further processing as well as the legal base of legitimate interest and allows ML only to the extent contractually required or consented to. And because ePR may prevail over the GDPR for the processing of data on all connected devices such as IoT, the privacy by design related investment that was made based on the trust built upon GDPR principles holding true is at risk.

The new approach taken by the Austrian Presidency (introduction of compatible further processing of metadata alongside compulsory safeguards to address potential risks) is therefore highly welcomed.

Additionally, we suggest a thorough analysis whether legitimate interests as a legal ground for processing could be added as well.

In the context of Art. 6, it is also vital to clarify, that the 'end-user' in a business context – i.e. where no private information of individuals is communicated – must be the legal entity which is (contractually) related to the communication process (see also below).

Data Protection Impact Assessment

Contrary to Recital 17 of the proposal, the new Recital 17aa stipulates that prior consultation of the supervisory authority needs to take place each time that metadata is being further processed for compatible purposes. This requirement would thus set forth a presumption that the processing of metadata will always result in high risks to the rights and freedoms of natural persons, and that these risks cannot be mitigated. We believe that for metadata processing, an obligation for a compulsory Data Protection Impact Assessment (DPIA) would be a more justified and a more reasonable approach. Art. 36(1) GDPR foresees prior consultation of a DPA only in those cases, where the impact assessment did not lead to the successful mitigation of risks, see also Art. 35(7) GDPR. Therefore, a compulsory prior consultation would deviate from the principles laid out by the GDPR and likely would overburden the data protection authorities. Only in the case that the identified risks could not be mitigated, a consultation of the DPA should be required, see Art. 36(1) GDPR.

Harmonization

Additionally, in contradiction to GDPR principles Art. 6(2)(f) allows for the processing of electronic communications metadata it is necessary for statistical counting, or for scientific research purposes, provided it is based on Union or Member State law. By giving the member States room for maneuver for providing national laws on the further processing of communications metadata the proposal jeopardizes the already achieved harmonization data protection rules by the GDPR and perpetuates the fragmentation of data protection and ePrivacy laws in the European Union. Therefore further processing of electronic communications metadata necessary for statistical

counting, or for scientific research purposes should be considered compatible in accordance with Art. 5(1)(b) GDPR without leaving room for national laws.

Structure

Structurally, Art. 6 is still not coherent: Art. 6(2) mentions "networks" and "services" while Art. 6(2)(a) only refers to "networks" and (b) only concerns "services". Optimization and service management should, however, also be allowed for electronic communication services. We therefore suggest including "services" in Art. 6(2)(a) as well.

2. Definition of the "Electronic Communication Service Provider" versus the Term "Controller" in the GDPR

With regard to the term ´electronic communication service provider´ there are still open questions with regard to the proposed Regulation. E.g. when using predictive maintenance for machines the corresponding sensor data/ user data must be continuously sent to a platform (communication process), which collects and analyses the data in order to design maintenance forecasts and recommendations, which are then transmitted back. In many cases, the provider of such a service will provide both the machine and the transmission option (e.g. SIM card for a certain mobile network, which he can either operate himself or buy from others) including storage, analysis and maintenance. If a provider qualifies as ECSP (because he provides and controls the transmission process) he needs to adhere to the strict rules of ePR and it is not clear, when the application of the ePR would end and processing could be based on GDPR rules. Hence, at the moment it is in our view unclear whether he will be able to process the data upon receipt as ´controller´ under GDPR rules (especially because Art. 7 provides for the obligation to immediately delete the data).

Definitions in the EECC

If the communication process is part of the complete offer, this provider would therefore probably be an electronic communications provider within the meaning of the EECC to which the draft regulation refers. Art. 2(4) EECC provides that ´electronic communications service´ means a service normally provided for remuneration via electronic communications networks, which encompasses internet access service as defined in Art. 2(2) of Regulation 2015/2120; and/or interpersonal communications service[1]; and/or service consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services

[1] Art. 2(5) of the EECC furthermore provides for a definition of ´interpersonal communications service´: it means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s); it does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

and for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.

Under ePR rules, the provider would only be allowed to process the data that has been transmitted and the data on the time/location of transmission e.g. if the end user has consented thereto or if the data is anonymized or pseudonymized for statistical purposes. Such strict requirements make it more difficult to use and further develop such systems and complicate the possibility to offer easy-to-use full-service models.

The Regulation in its current state still ignores the fact that it is increasingly impossible to distinguish between pure access and transmission providers and pure application service providers. We therefore strongly recommend clarification regarding the scope as this unclarity is obviously problematic with regarding to messaging services that are rarely offered alone, but usually in combination with another service. If, for example, a messaging service is offered for the business sector combined with project planning and collaboration tools and messages relevant to a project are automatically recognized and assigned to it with the help of AI, for example, such a tool can only be used if individual consent does not have to be obtained from each user. This would make it difficult to improve and develop the service during operation.

3. Software and the ePR

Recital 21a

The Presidency did not yet change Art. 8(1)(e) and the corresponding Recital 21a, which states that 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, 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. Recital 21a then makes the exception that 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 the consent-exception stated above.

We strongly recommend an amendment of this provision for several reasons. Firstly, Art. 8(1)(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 Art. 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 user (every single driver using the car?) of the car with all formal requirements under Art. 7 GDPR.

End-User

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. It is therefore necessary to expressly allow the consent being given by the contractual partner of the software provider: the company.

Regarding the use of ML and AI for email content - e.g. in the form of translation aids, automatic deadline recognition, SPAM control etc. the current provisions allow such use only in narrow circumstances: Art. 6(3)(aa) “for the purpose of the provision of an explicitly requested services by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interest of another person concerned and does not exceed the duration necessary for the provision of the requested services and is limited to that purpose only.” "For purely individual use" suggests that a company cannot decide on the general use within the company, but that the individual employee must give his or her consent. This also would make the application unattractive and impractical in many cases.

4. Consent and the ePR

Consent is a valuable tool for user control, as it signals a specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her. Given the special protection needed for electronic communication, this indication can and should only be used for specific situations and provide for one legal ground for processing of users communication data. But requiring consent should always be a signal that a

particular, an exceptional processing of his/her data would follow. To make sure that the user recognizes this particular situation and to avoid consent fatigue the requirement should not be provided for unnecessarily.

For example, in Art. 6(3)(aa) the Council text requires an additional consent for processing of e-communications content, which is redundant. The consent requirement comes on top of the fact that the service concerned already needs to be specifically requested by the end-user (in a comparable GDPR-situation this would mean requiring consent for a contractually agreed processing).

The requirement "if the requesting end-user has given consent" seems redundant and overly disruptive given that the service has already been explicitly requested by the end-user and such requested processing does not adversely affect fundamental rights and interests of another person concerned (Redundancy) and the end-user will have explicitly and specifically requested the service after having been provided with information about the processing of his or her e-communications content data as per Art. 13 and 14 GDPR (Disruptiveness). Therefore, the end-user will have already expressed his or her understanding that e-communications' content will need to be processed, limited to that purpose only. Otherwise, the explicitly requested service for purely individual use cannot be delivered. Requiring an additional consent at that moment will overly disrupt the user experience, and will undermine meaningful use of consent elsewhere.

5. Article 8

Service provision conditional to consent

As already proposed and formulated in the German Comments of 13. June, Bitkom considers it necessary to have a provision in Art. 8 that ensures that the use of online services that are financed through advertising can be made conditional upon the consent of the end-user to the use of cookies for advertising purposes. The current statements in Recital 20 are not sufficient and are not sufficiently clear either. Currently, Recital 20 provides that access to a specific website content may still be made conditional on the consent to the storage of a cookie or similar identifier´. The provision should be part of Art. 8 and read as follows: "The provision of information society services that are wholly or partly financed by advertising may be made conditional upon the consent of the end-user to the storage and collection of information for advertising purposes, provided that the end-user is informed accordingly."

Another alternative/addition could be the already proposed option in the Councils Discussion Paper 9958/18, where it was considered to amend Recital 20 to ensure that making access to website content conditional to the consent to the use of cookies should only be considered disproportionate for services provided by public authorities. We suggest to further analyse this aspect and the different access and business models.

Audience Measuring

Furthermore, the Council text is not clear enough on whether the use of cookies for ad measurement will be exempt from consent. The Council does not specify in Art. 8(1)(d) whether audience measuring also includes “advertising measurement”, even though that would reflect the considerations of Recital 32. This could lead to great legal uncertainty among advertisers and third party measurement providers regarding the consent requirement. “Advertisement measurement” should be added to Art. 8(1)(d) to avoid legal uncertainty.

— Advertising measurement is necessary for many content providers and essential for a well-functioning European digital economy, regardless of whether the provider is showing targeted or non-targeted advertising. If they cannot measure the impact of the ads being served, advertisers will not spend their marketing budgets on advertising with them. Restricting the use of ad measurement cookies will affect contextual advertising and targeted advertising equally, as they involve the same measurement technology.

Fraud Prevention Clarification

— Regarding Art. 8 or the corresponding Recital 20, we would suggest clarification that the use of processing and storage capabilities of terminal equipment and the collection of information from end-users’ terminal equipment is allowed for fraud prevention and the detection of technical faults, even if they are not linked to the security of the information society service provider himself.

6. Article 10

We welcome the new approach with regard to Art. 10, because all the previous discussions have shown that the technical feasibility of Art. 10 is highly questionable and would not only unduly burden browsers and apps, lead to legal uncertainty with regard to obtained consent (especially if consent is given on a website but the browser setting does not allow for e.g. a cookie to be placed on the device) and also lead to consent fatigue. The provision proposes that the user must consent to all non-strictly necessary tracking (storing information on the terminal equipment of an end-user of processing information already stored on that equipment) on a global scale: the pre-settings when installing their browsers. The proposed 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 and optimize their content. 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 previously 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, secure solution. Deleting Art. 10 is therefore preferable to a provision that raises more questions than it answers.

Furthermore, the GDPR already provides for a right to object in a similar way in Art. 21(5): "In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications."

7. Specific Comments on Recitals

For clarification and an in depth analysis, Bitkom would like to provide additional input with regard to some Recitals:

Recital 15

(15) Electronic communications data should be treated as confidential. This means that any interference ~~with the transmission processing~~ of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of ~~all~~ **users** ~~the communicating parties~~ should be prohibited. ~~The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee~~. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, ~~scans or stores~~ the content of electronic communications, or the associated metadata for purposes other than the **provision of the service requested by the user** ~~exchange of communications~~. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber	1. Gathering consent from "all" "communicating parties" is only feasible for closed services and networks. Service providers cannot gather consent from individuals who are not their users. This requirement would outlaw all open services, i.e. those that allow interoperability with services offered by other providers. 2. Scanning is processing, therefore reference should be deleted to bring it in line with the above changes. Storage should not be considered as "interference". An overwhelming majority of communication services are cloud based, storage is expected by users, who access these services from multiple devices. 3. The scope of the regulation seems broader than just transmission and exchange of communication. If this is the case, the wording here needs to be adjusted.

Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	

Recital 18

End-users may consent to the processing of their metadata to receive specific services ~~such as protection services against fraudulent activities~~ .Communication data may be processed to protect services and users against fraudulent activities. This may require ~~by~~ analysing usage data, location and customer account in real time~~)~~. In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. ~~For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679.~~ Basic broadband internet access and voice communications services are to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. ~~Consent for processing electronic communications data from internet or voice communication usage will not be valid if the data subject end-user has no genuine and free choice, or is unable to refuse or withdraw consent without detriment..~~	1. Fighting fraud should not be dependent on end-users consent – otherwise the criminal´s consent may be needed for fraud prevention or users would not be protected because they did not consent beforehand. 2. GDPR already defines a valid consent. To avoid uncertainty with regard to this important definition, additional explanations should not be part of the ePR.

Recital 19b

(19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal entity having subscribed to the electronic communications service, for instance for the professional communication of employees or for other business-related reasons, may allow a natural person, such as an employee, to make use of the service. In such cases, consent may be obtained from the legal person concerned, and not from the individual user.	If electronic communication services are used to carry out business-related communication, the consent must be obtained by the legal person or a competent individual acting on behalf of the legal entity that is the contractual partner of the provider. This can also be the individual end-user, if the legal person decides to delegate the consent in general, for specific services or in individual cases to a natural person (for example the employee). As a general rule, consent of the employer needs to be sufficient (see above – Software and the ePR). In addition to our comments above we would like to refer to the very narrow interpretation of the WP29 in their Guidelines on consent (WP 259): "An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees, Art. 6(1)(a), due to the nature of the

	relationship between employer and employee." We strongly argued against this assessment (please see our Position Paper on the Guidelines) but as the Guidelines are likely to be the basis for interpreting and assessing the validity of consent, ePR needs to take the practical implications into account.

Recital 23a

Terminal equipment which is used for business reasons, such as computer, laptops, tablet computers or smart phones, for example to control production facilities and machines or to run business software, has to be updated simultaneously or at least in a controlled time frame and fashion. It also need to be maintained and managed to reflect the relevant business needs and to comply with security requirements. In this context, the end-user is the legal person, for example a company, who must give consent to the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment.	To provide a high level of IT security and updated software and apps which reflects the business needs and processes of a company, the consent for data processing with regards to terminal must be obtained by the legal person or a competent individual acting on behalf of the legal entity. This can also be the individual end-user, if the legal person decides to delegate the consent in general, for specific services or in individual cases to a natural person (for example the employee).