Position Paper

Bitkom views regarding Presidency Discussion Paper and Doc. 5165/18

29/01/2018
Page 1

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. Introduction

Bitkom welcomes the opportunity to comment on the outlined guiding principles and options raised by the Presidency.

The European industry places a high value on privacy and confidentiality, but the proposal for an ePrivacy Regulation (ePR) puts the progress that was achieved through the balanced provisions of the GDPR at risk. Without amendments, the ePR will make it exceedingly difficult for European companies to innovate and transform digitally. Furthermore, many current business models would be put at risk and user experience for most information society services would suffer unduly. Therefore, we appreciate the Presidency´s view on some points of the ePR, especially the willingness to look into the issue of Art. 6(2) and the possible alignment with Art. 6(4) of the General Data Protection Regulation (GDPR), as Bitkom has consistently advocated for such an alignment.

We would like to highlight the following aspects first and then go into more detail below:

(1) **Scope**

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)). M2M communication should be removed explicitly from the scope of the Regulation altogether.

The rules regarding the applicability of the e-Privacy Regulation need to be strictly limited to the transmission of communications data only and clear in scope to ensure that companies can assess which framework applies when.

(2) **General approach**

The ePR needs to ensure flexibility for future business models. It therefore has to be technology neutral and should implement the well-proven risk based approach. Processing personal data must not only depend solely on consent but 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.

To ensure a balance between protecting personal data, confidentiality of communications and processing data to facilitate innovative business models, we would like you to consider the following points and arguments regarding the options outlined in doc. 5165/18:

2. Link to General Data Protection Regulation (GDPR) and clarification on where the e-PR complements and where particularizes it, with a focus on Articles 5,6,7,8, and 10

We strongly agree that the relationship between GDPR and ePR need clarification. Clarity is needed in order to avoid legal uncertainty due to possible duplications and contradictions between the frameworks. The ePR brings challenges that will be equally large if not much larger than the GDPR as its vague provisions and unclear relation and scope due to overlapping provisions will add to the legal uncertainty and slow down the data protection implementation process in the Member States. The Council should work on a streamlined approach and only add regulation where it is absolutely necessary. The drafting of the GDPR took years and European legislators were finally able to create a balanced regime for the whole of Europe. This balance should not be thwarted by another Regulation that excludes too many business and data processing operations from the scope of the GDPR.

3. Issues related to scope of the ePrivacy Regulation and the alignment with the proposal for a Directive establishing a European Electronic Communications Code (EECC)

3.1 Machine-to-Machine (M2M) communications (Articles 2, 3 and 5)

The Presidency states that under the EECC compromise proposal the transmission services used for the provision of machine-to-machine services constitute an electronic communications service and such should be covered by the ePR for the purpose of ensuring their confidentiality. However, the application layer of such machine-to-machine services, which does not normally constitute an electronic communications service, is not covered by the EECC/ePR. In view of the presidency, this follows the scope of the current ePrivacy Directive.

With its connection to basically any electronic communications data, even in the communications between machines, the ePR extends the scope of application far beyond the protection of personal data. Machine-to-machine communication processes are essential for a functioning digital industry. Stringent rules on all M2M communications is excessive and will discourage digitization of industry as it narrows the scope for innovation in the area of Industry

4.0 and the Internet of Things. M2M communication processes should therefore not be covered by the restrictive rules on processing on (personal) electronic communication Data and should be explicitly removed from the scope of the proposal.

3.2 Machine-to-Machine – Option 2

We therefore support the view of the Presidency given on page 9 of the document. There the Presidency states that as M2M communications are carried out with limited or without human intervention at all, communicating end users should not have a right to confidentiality of the information transferred this way.

Where the Presidency argues that dis-aligment with the Draft Code should be avoided, is should be considered to also excluded M2M communication from the scope of the EECC. This could also serve to avoid discrepancies between the scope of application and there is no objective reason why this form of communication should be included necessarily in the EECC. Furthermore, the Presidency argues that excluding M2M communication from the scope would lower the current level of protection as it was included in the ePrivacy Directive. But seeing that since the introduction of the (revised) ePrivacy Directive in 2009 M2M communication became more and more important to build and design integrated systems, the importance of such communication should be considered in the drafting of the new regulation. Current technological development should be included in the design of the new Regulation to keep it open for innovation while also securing the necessary confidentiality for other methods of communication.

We therefore support the Option 2, where the transmission services used for the provision of machine-to-machine services are altogether excluded from the scope of the ePR regardless whether they transmit personal information or not. This option is to be preferred as it would be impractical to separate between transmission and application layer in practice and would also be impractical to differentiate between M2M-communication regarding personal data and cases where non-personal data is transmitted (to determine which data is processed, a processing would be necessary as a first step either way). Excluding M2M-communication will create a clear legal situation where processors, users of m2m-communication and integrated systems can rely on distinct legal grounds for their processing. The protection of data subjects seems sufficient under the GDPR and with the additional provisions of the ePR.

4. Article 6: permitted processing of electronic communications data

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).

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. 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. 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 should be allowed and pseudonymous solutions should be privileged.

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.

We therefore recommend supporting Options 2 (legitimate interest) as well as Option 4 (further compatible processing), except the limitation to public interest purposes (point 1). The limitation of a public interest test would exclude a variety of socio-economic data analytics projects (e.g. processing data in smart city projects or reducing ecological footprints) where the public interest is often part of commercial project agreements of both public and private entities.

5. Article 7: Storage and erasure of electronic communications data

The ePR requires communications data to be deleted after transmission, with only a few and limited exceptions. This provision is too wide in scope and does not take the modern communication context into account. Moreover, security issues would arise of the current provision is not amended.

Especially with regard to cloud services, the storage of communications content is an essential part of the service provided (storing content from messaging apps, digital communications such as audio, text and video files for later retrieval by the user). An immediate deletion after transmission would render many useful services unfit and less useful.

Moreover, a service provider may also need to store communications data for later analysis for fraud protection purposes, to assess security threats, and maintain and test his systems. As such practices are logically subject to the GDPR and therefore have to follow the rules on limitations of storage and later use of personal data, there is no reason to introduce a framework that imposes special rules on communication service providers and prohibits practices that are allowed under the GDPR. Storage and later use are thus already and well protected under the GDPR and should not be included in the scope of the ePR. This should be clarified.

Furthermore, as an introduction to both Article 7(1) and (2) we suggest the following: “without prejudice to Article 6” as a whole. If providers are obliged to delete or anonymise data as soon as the communication is conveyed, then any other processing for the other purposes under Article 6(2) can no longer be fulfilled. The very purposes of Article 6(2) requires providers to store the metadata until those purposes are fulfilled.

6. Article 8: Protection of information stored in terminal equipment of end-users and related to or processed or emitted by such equipment

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.

7. Article 10: software privacy settings

Bitkom urges the Presidency to consider facts regarding the technical feasibility of the provisions in the ePR, especially the proposed Art. 10 of the ePR. The current 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 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.

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.

8. implementation period

Last but not least, we encourage the Presidency to provide businesses with a reasonable and adequate implementation period of the ePrivacy Regulation of 2 years.

Bitkom represents more than 2,500 companies of the digital economy, including 1,700 direct members. Through IT- and communication services only, our members generate a domestic turnover of 190 billion Euros per year, including 50 billion Euros in exports. Members of Bitkom employ more than 2 million people in Germany. Among the members are 1,000 small and medium-sized businesses, over 400 startups and nearly all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the sectors of digital media or are in other ways affiliated to the digital economy. 80 percent of the companies' headquarters are located in Germany with an additional 8 percent each in the EU and the USA, as well as 4 percent in other regions. Bitkom supports the digital transformation of the German economy and advocates a broad participation in the digital progression of society. The aim is to establish Germany as globally leading location of the digital economy.