DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Committees on IT-Law and Surveillance

Council mandate on the proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) dated 10 February 2021

Position Paper No.: 28/2021

Berlin/Brussels, April 2021

Members of the IT-Law Committee

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Chair)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Köln
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf (Rapporteur)
- Rechtsanwältin Birgit Roth-Neuschild, Karlsruhe
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

In charge in the Berlin office

- Rechtsanwältin Nicole Narewski

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparency Register ID number:
87980341522-66

www.anwaltverein.de

Members of the Surveillance Committee

- Rechtsanwältin Lea Voigt, Bremen (Chair)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin (Rapporteur)
- Rechtsanwalt Dr. Eren Basar, Düsseldorf
- Rechtsanwältin Prof. Dr. Annika Dießner, Berlin
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Prof. Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt
- Rechtsanwalt Prof. Dr. Mark A. Zöller, München
- Prof. Dr. Annika Dießner, Berlin (permanent guest member of the Committee)
- Prof. Dr. Mark A. Zöller, München (permanent guest member of the Committee)

In charge in the Berlin office

- Rechtsanwältin Uta Katharina Schmidt
- Rechtsanwalt Max Gröning

In charge in the Brussels office:

- Anja Wyrobek
- Rechtsanwältin Eva Schriever, LL.M.

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 62.000 German lawyers and lawyer-notaries in 252 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level.

Brief summary

Four years ago, the German Bar Association (DAV) already commented on the proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (see DAV-Position Paper 29/2017). The relationship between the General Data Protection Regulation (EU 2016/679), hereinafter GDPR, and the ePrivacy Directive 2002/58/EC has been unclear since the GDPR already entered into force in May 2018.

On 10 February 2021, the Council adopted its mandate for negotiations with the European Parliament on the ePrivacy Regulation (hereinafter: Council mandate)[1], which heavily modifies the Commission's proposal dated 10 January 2017 (hereinafter: COM proposal)[2] and the EU-Parliament's mandate dated 20 October 2017 (hereinafter: EP mandate)[3] in some respects. As regards the forthcoming trilogue negotiations the German Bar Association would like to comment on Council mandate and point out some of the added value in the mandate as well as raise some concerns.
The German Bar Association is concerned that the new draft enables Member States to introduce provisions on data retention by creating an opening clause. The provisions in Art. 6(1) and Art. 7(4) Council mandate do not respect relevant case law on data

[1] Council mandate on the proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Doc. No. 6087/21
[2] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final
[3] Report on the proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017

retention by the CJEU, let alone because no exceptions are provided for professional secrecy holders.

Furthermore, the German Bar Association welcomes the clarification regarding the territorial scope of application to users located in the EU, but criticises that the material scope of application remains unclear with regard to free services. The DAV also underlines the importance of browser configurations - and thus the user's wishes – which is not taken into account accordingly. Moreover, the DAV calls for a strengthening of the provisions on the withdrawal of consent. Furthermore, we suggest to refrain from creating a new terminology in the context of consent to tracking and maintaining the current wording of the GDPR in order to streamline both Regulations. Furthermore, we advocate to refrain from unnecessarily restricting the handling of metadata in view of the economic consequences, in the case of no special need for protection. Concerning cookie walls, we suggest to enable end users to choose whether they want to pay with money or with data to get access to content, in order to prevent monopoly providers from a de facto enforcement of disclosure of data. Finally, the German Bar Association sees an erosion of the privacy-by-design principle in the current Council mandate.

Material scope of application of the regulation is partly unclear

The scope of application of the Regulation has been redefined in Art. 2(1)(a) Council mandate. It now covers: "*The processing of electronic communications content and of electronic communications metadata carried out in connection with the provision and the use of electronic communications services*".

Compared to earlier proposals, the focus is now on "*electronic communications content and electronic communications metadata*" instead of "*electronic communications data*". This amendment makes no sense and is even superfluous because "*electronic communications data*" is legally defined as "*electronic communications content and electronic communications metadata*", see. Art. 4(3)(a) Council mandate.

The clarification in Art. 2(1)(a) EP-Mandate, according to which the Regulation also covers communications data when using free services, was removed. This also applies to Recital 10 and Art. 3(1)(a) Council mandate. In this respect, it is unclear whether free communication services should no longer fall within the scope of the regulation. There is an urgent need for clarification on this question.

The material scope of application and applicability also remain open for services where the user does not make a monetary payment to the service provider, but transmits data to the service provider that is not necessary for the functioning of the service - i.e. the payment is provided with the user's own data. Here, too, clarification is needed.
In addition, the applicability of the Regulation with regard to the end-user's terminal equipment has been somewhat restricted (see. Art. 2 (1)(b) Council mandate). Now only "*end-users' terminal equipment information*" is covered. Whereas the previous wording of the EP-Mandate regulated a broader scope of application: "*the processing of information related to or processed by the terminal equipment of end-users*". This restriction appears to do no harm, because the information about the terminal equipment is to be regarded as less worthy of protection.

Clear territorial scope of the regulation to be welcomed

Compared to the previous proposals, the Regulation shall only apply to electronic communications of end users located in the EU, (see Art. 3 Council mandate). Thus, the Regulation does not apply to services offered from the territory of the EU and used only by end-users outside the EU, as stated in Art. 3(1)(b) EP-Mandate. The wording "*end-users who are in the union*" also creates a parallel with Art. 3(2) GDPR, which according to the prevailing opinion is based on the actual residence of the person. It also continues to be harmless for the applicability of the ePrivacy-Regulation that a provider is not located in the EU.
The focus on the end user and the narrowing of the geographical scope of application to the Union is to be welcomed. Otherwise, EU-based providers of electronic communications would be at a competitive disadvantage when operating in non-EU countries. European companies, in contrast to local providers, would be subject to the stricter rules of the ePrivacy-Regulation. Also, the link to the actual habitual residence of the end-user in Union territory is easier to establish and requires less effort than focusing on the nationality of the end-user.

The wording of “Consent” and limited appreciation of browser preferences

With regard to Art. 4a(2) Council mandate, reference can first be made to the German Bar Association’s Position Paper No. 29/2017 (page 26 f.). As previously submitted the customary term "browser" should be used instead of "*software placed on the market*

permitting electronic communications, including the retrieval and presentation of information on the internet.".

It is unclear why rules on withdrawal of consent have been removed from the enacting part of the Regulation and why the reference is now limited to the recitals (in particular recital 34 Council mandate).

The significance of the browser settings with regard to a general rejection of cookies or the use of a cookie whitelist is also reduced. Thus, Art. 4a(2aa) Council mandate harbours the risk that, despite corresponding clear browser settings, the impression is created among users that they would have to express their opinion on the storage and processing of cookies again. Thus, the browser settings do not lead to noticeable changes. On the contrary, in particular website operators could repeatedly or aggressively ask the end user for consent, even though the end user had previously consciously decided against consent in the browser. These "pushy" website operators would then have an advantage over "upright" operators who respect the relevant browser settings.

According to Art. 4a(3) Council mandate, the user is to be regularly reminded of his or her right to withdraw consent, which the user can, however, waive. The obligation to remind users is to be welcomed. However, the scenario that users will be encouraged to waive the obligation to be reminded of their consent at the time of consent is quite likely. With the result that Art. 4a(3) Council mandate would be rendered meaningless. In its current form, the reminder obligation is therefore not very practical.

Art. 10 COM proposal has been removed. The EP-Mandate provided, among other things, for data protection-friendly default settings in applications as well as information obligations about the data protection settings. This removal would lead to an indirect reduction of the data protection level. This is because, as a rule, it is mainly uninformed users who use the default settings of software such as the web browser. Also, only a few users change the data protection settings of their browser, for example out of fear that certain websites would then no longer be fully accessible. Therefore, the provision in the wording of Art. 10 EP-Mandate should remain in place.

"Consent" is better than "accept"

Recital 21b Council mandate introduces a new term according to which tracking by media websites that are financed by advertising should also be possible, under the condition that the end user "*has been provided with clear, precise and user-friendly*

information about the purposes of the cookies or similar techniques used has accepted such use".

It would be advantageous to use the term "consent" here. This is because according to Art. 4a(1) Council mandate, the provisions of the GDPR apply to consent. These provisions under the GDPR include, for example, the transparency requirement under Art. 5(1) GDPR and also the requirements for informed consent under Art. 7 GDPR ("*intelligible and easily accessible form, using clear and plain language*"). It is unclear why a new category is created, thus deviating from the previous differentiated consent system for no reason.

Lack of certainty in Art. 6c Council mandate

Requirements are set for the transfer of data to third parties if the network operators originally collected the metadata for another purpose, see recital 17aa, Art. 6c (3) Council mandate. Overall, Art. 6c Council mandate substantiates the well-known data protection principle of purpose limitation.

However, Art. 6c(3) Council mandate is incomprehensible and not specific enough.
It is not clear what "*such data*" in Art. 6c(3) Council mandate refers to. Metadata can be personal data, but it does not have to be. However, the discussed provision requires anonymisation of data that was originally collected for a different purpose. Only then may this data be passed on to third parties. However, it is not possible to anonymise metadata that is not personal data. Accordingly, only part of the metadata may be passed on, namely the formerly personal data. There is no reason for this differentiation. It seems that the wording is a drafting error. Since this paragraph would make sense under the condition that the anonymisation of personal data was required and it could then be passed on together with other metadata.
It is also not clear from the wording of Art. 6c(3) Council mandate whether the transfer of data to third parties that is already anonymised resp. not personal data must also be dealt with pursuant to Art. 6c(1) Council mandate. This requirement would be an unnecessary and restriction of business models hampering innovation. Informational self-determination is not affected, as the data is anonymised or not personalised. The protection of communication data resulting from Article 7 of the EU Charter of

Fundamental Rights also does not prevail here. On the one hand, the data in question concerns metadata and not content of communications, and on the other hand, the anonymisation or lack of personal reference do not require special protection that could justify a need for considerations under Art. 6c(1) Council Mandate. However, there would be competitive disadvantages: Companies from third countries are not subject to these restrictions in their markets if they sell metadata to third parties as network operators or if they acquire these metadata as third parties. Thus, foreign companies can pursue a business model that is severely restricted in the EU for no apparent reason.

Facilitated use of data on and of the terminal equipment

Art. 8 Council Mandate regulates the handling of end-users' terminal equipment. The integrity of terminal equipment is now explicitly included as a protection objective in the heading of Chapter II. According to Art. 8(1) Council Mandate "*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*" unless one of the justification grounds then mentioned is relevant. These include, among others:

- „*it is necessary*", see Art. 8(1)(a) Council Mandate in comparison to the Art. 8(1)(a) EP-Mandate which states „*strictly necessary*"
- „*the end-user has given consent*", see Art. 8(1)(b) Council Mandate in comparison to the Art. 8(1)(b) EP-Mandate which states "*specific consent*"
- „*it is strictly necessary for providing a service specifically requested by the end-user*", see Art. 8(1)(c) Council Mandate in comparison to Art 8(1)(c) EP-Mandate which states "*it is strictly technically necessary for providing an information society service specifically requested by the user"*
- As regards the use of processing and storage capabilities of terminal equipment and the collection of information the Art. 8(1)(d) EP-Mandate provided for stricter rules in comparison to Art. 8(1)(d) Council Mandate. The Council Mandate allows for third party tracking without consent.

The prerequisites for the use or collection of information from terminal equipment have thus been eased significantly in the Council Mandate.
Among the newly introduced grounds for justification, Art. 8(1)(g) Council Mandate stands out. If the processing for purpose other than that for which the information has been collected, henceforth considerations have to be taken into account. The processing of data for another purpose was not mentioned in the previous drafts and the clarifying points in Art. 8(1)(g)(i)-(v) Council Mandate are to be welcomed, since they are creating legal certainty.
By analogy, Art. 6c(3) Council Mandate applies to Art. 8(1)(i) Council Mandate which regulates the disclosure of tracking data to third parties. In principle, data may not be passed on to third parties, unless the conditions laid down in Art. 28 of GDPR are met, or data is made anonymous. Above mentioned concerns under heading “**Lack of certainty in Art. 6c Council Mandate**” apply here as well.

Vagueness of the term „statistical purposes”
Art. 8(2) Council Mandate regulates the collection of information of data emitted by the terminal equipment. Here, among other things, a new justification for collection of information is created for "*statistical purpose*" according to Art. 8(2)(c) Council Mandate. However, even in conjunction with Recital 25 of the Council Mandate, this justification is too vague, because it is not clear whether commercial statistical interests, such as market research, are also sufficient. It would be desirable for the term "statistical purpose" to be legally defined and for this definition to also include commercial statistical purposes in order to create legal certainty.

So-called cookie walls are possible
Art. 8 (1a) EP-mandate has not been taken into account. According to this paragraph, it would have been prohibited to deny a user access to a service because he or she did not consent to the processing of his or her personal data or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality. This would have prohibited so-called cookie walls in particular.
From the point of view of the website operators concerned, the lack of this interdiction is certainly to be welcomed, as it means that the widespread financing model can continue, in which the end user does not have to pay money in order to use the website,

while the provider nevertheless generates an income. As compensation, however, the legislators should grant the end user a right to choose between a payment with money and a payment with data. Otherwise, the situation arises that in the modern communication society, important services could, due to their monopoly position, de facto force disclosure of data of a large part of the population.

The obligations to inform the user should be made more specific

When processing and collecting data emitted by the terminal equipment and justified by consent or for statistical purposes, the end user must be informed according to Art. 8(2a) Council Mandate.

However, Art. 8(2a) Council Mandate lacks concrete guidance on how this information must be provided. In view of the different designs currently used, for example on websites, harmonised requirements would be desirable. For example, whether it is allowed to use a colour code of the consent pop-up that might influence the end user (so-called "nudging") or to what extent more effort may be required from the end user for refusal of consent than for consent.

The mentioned standardised icons in Art. 8(3) and (4) Council Mandate are to be welcomed in view of their easy implementation and standardisation. It is also to be expected that by using these icons instead of detailed text on the first level, users will perceive the information as less intrusive.

Lowering the technical level of protection

The principle of privacy by design as stated in Art. 17(1a) EP-Mandate should be upheld. According to Art. 17 (1a) EP-Mandate, "*providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and integrity of the communication in transmission or stored are also guaranteed by technical measures according to the state of the art, such as cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited. Notwithstanding Articles 11a and 11b of this Regulation, member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the*

confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used."

It is of particular interest to companies that secure communication remains possible, especially with regard to business secrets. In this context, the use of already known services is desirable in order to make the flow of information as uncomplicated as possible. However, such services can only be used if they guarantee a sufficient level of confidentiality and security, for example through end to end encryption.

Neutral supervisory power

In Art. 18(1) Council Mandate the addition has been deleted that the tasks and powers of the supervisory authorities are exercised in relation to the end users. This change is to be welcomed and was already submitted in the DAV Position Paper No. 29/2017 p.34 f.

However, also according to Art. 18 (1) Council Mandate where the supervisory authorities are not the supervisory authorities responsible for monitoring the application of the GDPR, the competent supervisory authority shall cooperate with the latter and, *whenever appropriate*, with national regulatory authorities established pursuant to Directive (EU) 2018/1972 and other relevant authorities. The addition "whenever appropriate" should be deleted (see Position Paper No. 29/2017 p.36 f).

Another attempt to introduce data retention?

According to Art. 6(1)(d) Council Mandate: "*Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:*
it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security."

This is supplemented by Art. 7(4) Council Mandate:

“*Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists.*”

There are already considerable reservations about the idea of regulating the highly controversial and complex issues surrounding the admissibility as well as structure and scope of data retention almost "incidentally" within the framework of the envisaged ePrivacy Regulation. This does not do justice to the significance of this measure for the protection of citizens' fundamental rights and its importance to engage in a political discourse.

Art. 6(1)(d) Council mandate also covers content data in contrast to Art. 7(4) Council Mandate which is limited to metadata.

These two provisions would create leeway to introduce data retention at national or EU level and in this respect act like an opening clause. In their current wording, both norms are unacceptable. They do not even begin to do justice to the differentiated case law developed by the CJEU on data retention and the far-reaching prohibition of the same. On the contrary, a new phase of legal uncertainty is to be expected until the CJEU final rules on the legality or more likely overturns the corresponding provisions.

The important principle of the current CJEU case law, notably that a general and indiscriminate retention of all traffic and location data of all subscribers and registered users for preventive or repressive purposes is contrary to fundamental rights, is being ignored. In its judgment of 6 October 2020 (CJEU C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791), the CJEU most recently set out the limits under which data retention may be used and permitted. According to this, "*a serious threat to national security which is shown to be genuine and present or foreseeable*" is required. Moreover, only the "targeted" storage of traffic and location data is permitted and only to the extent that it is necessary for combating serious crime and preventing serious threats to public security. The provisions in question do not even begin to reflect these restrictions.

The condition outlined in Art. 7(4) Council Mandate that data retention "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society*" is exhausted in a repetition of the minimum standards of fundamental rights the legislator always must observe and is therefore obviously not suitable to ensure the implementation of the CJEU's requirements by the member states.

The discussed provisions are also insufficient with regard to the CJEU's requirement that provisions on data retention must "*ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse*".

According to the CJEU, there is also a need for effective review, either by a court or by an independent administrative body whose decision is binding. The aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists. The discussed provisions do not provide those safeguards, not the necessary review.

Also, the categories of data to be stored and collected and their level for protection, the group of persons, the geographical area or the period of time would have to be considered in a differentiated manner (see CJEU C-203/15, C-698/15, ECLI:EU:C:2016:970 marginal no. 106, 108). Such a differentiation is completely missing in Artt. 6, 7 Council Mandate.

Furthermore, the proposal does not provide for any exceptions for persons with a duty of professional secrecy such as doctors, lawyers, pastors, although this is considered essential by the CJEU (see CJEU C-203/15, C-698/15, ECLI:EU:C:2016:970 marginal no. 105). The sensitive relationship of trust between a person subject to professional secrecy and his or her lawyer is particularly worthy of protection and characterised by confidentiality. Without the possibility of anonymous communication, counselling in

mental or social distress would be problematic and in the case of the lawyer-client relationship even at odds with the Charter of Fundamental Rights and a burden to access to justice. The fear of being recorded could prevent contact, which may be crucial for the person seeking help or justice. Legal advice by a lawyer is also of considerable importance and a pillar of the rule of law, protected by the Charta and therefore particularly worthy of protection.