DeutscherAnwaltVerein

Position Paper

of the German Bar Association by the Information and Security Law Committees

on the proposal for a regulation of the European Parliament and of the Council on the right to privacy and the protection of personal data in electronic communications and for repealing Directive 2002/58/EG (Directive on Privacy and Electronic Communications)

Position Paper No.: 29/2017 Berlin/Brussels, August 2017

Members of the Committee on Information Law

- Rechtsanwalt Dr. Helmut Redeker, Bonn (chairman, rapporteur)
- Rechtsanwalt Dr. Simon Assion, Frankfurt (rapporteur)
- Rechtsanwältin Dr. Christiane Bierekoven, Nürnberg
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Michael Friedmann, Hannover
- Rechtsanwalt Dr. Malte Grützmacher, LL.M., Hamburg
- Rechtsanwalt Prof. Niko Härting, Berlin (rapporteur)
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Responsible DAV-Director

- Rechtsanwältin Nicole Narewski

Members of the Committee on Security Law

- Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (chairwoman)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwältin Dr. Annika Dießner, Berlin (rapporteur)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln

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
Transparency Register identification number: 87980341522-66

www.anwaltverein.de

- Rechtsanwalt Prof. Dr. Björn Gercke, Köln
- Rechtsanwalt Dr. Stefan König, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt/Main
- Rechtsanwältin Kerstin Oetjen, Freiburg
- Rechtsanwältin Lea Voigt, Bremen

Responsible DAV-Director

- Rechtsanwalt Max Gröning

Contact in Brussels:

- Rechtsanwältin Eva Schriever, LL.M.

Mailing List

Germany

Bundesministerium der Justiz und für Verbraucherschutz

Bundesministerium für Wirtschaft und Energie

Bundesministerium des Innern

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag

Ausschuss für Wirtschaft und Energie im Deutschen Bundestag

Ausschuss Digitale Agenda im Deutschen Bundestag

Innenausschuss

Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien

Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien

Justizministerien und -senatsverwaltungen der Länder

Landesministerien und Senatsverwaltungen des Innern

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Datenschutzbeauftragten der Bundesländer

Innenausschüsse der Landtage

Rechtsausschüsse der Landtage

Europäische Kommission – Vertretung in Deutschland

Bundesrechtsanwaltskammer

Bundesnotarkammer

Bundesverband der Freien Berufe

Deutscher Richterbund

Deutscher Notarverein e.V.

Deutscher Steuerberaterverband

Bundesverband der Deutschen Industrie (BDI)

GRUR

BITKOM

DGRI

Gewerkschaft der Polizei (Bundesvorstand)

Deutsche Polizeigewerkschaft im DBB

Ver.di, Recht und Politik

stiftung neue verantwortung e.V.

Institut für Deutsches und Europäisches Strafprozessrecht und Polizeirecht (ISP) der Universität Trier

DAV-Vorstand und Geschäftsführung

Vorsitzende der DAV-Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Europe

Europäische Kommission

- Generaldirektion Justiz
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament

- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres
- Rechtsausschuss
- Ausschuss für Binnenmarkt und Verbraucherschutz
- Ausschuss für Industrie, Forschung und Energie

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)
Vertreter der Freien Berufe in Brüssel
DIHK Brüssel
BDI Brüssel

Press

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
JurPC

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising more than 65.000 German lawyers. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession.

Executive Summary

The planned regulation COM(2017)10/F1 (hereinafter: ePrivacy Regulation) is to repeal the ePrivacy Directive (Directive 202/58/EG of 12 July 2002 – hereinafter ePrivacy Directive). It complements the General Data Protection Regulation (Regulation (EU) 2016/679 of 27 April 2016, hereinafter GDPR) in terms of data generated in the context of telecommunications services. In this respect, the provision assumes – as does the previous provision – a broader scope: protection is also granted for data relating to legal persons and not limited to data relating to natural persons.

Many parts of the proposed provisions deliberately draw a parallel with the provisions of the General Data Protection Regulation. At some points the GDPR is even referred to. Such parallels are not always justified. On the one hand, this is due to the fact that the content of telecommunications is often very personal in nature and therefore, a high degree of confidentiality is required. Moreover, analyzing metadata can result in very personal insights about individual users – ranging from their political orientation to their sexual preferences. This is why the ECJ has repeatedly emphasized the high significance of protecting such data (most recently, in its judgement of 21 December 2016 (C-203/15 and C 698/15)). As a result, the protection level must basically be higher than that for personal data in general, in particular with regard to potential state intervention. The draft regulation does not consider these differentiations. Articles 5 and 6 of the ePrivacy Regulation should take account of the specific protection requirements of confidentiality of communications and counteract specific communication-related threats and interventions instead of treating communication content like personal data per se.

Moreover, the text of the draft regulation is unclear in some points. The European legislator, however, should also consider the principle of normative clarity.

Choosing the legal instrument of a “regulation“, effective date

Suggestion:

- The design as a regulation and the effective date of 25 May 2018 should be adhered to.
- The wording should provide as much normative clarity and accuracy as required for directly applicable law.

Reason:

The Expert Committee advocates the EU Commission’s proposal for a legal regulation and its intent to synchronize the effective date with that of the GDPR. This avoids ambiguities in the relationship between the GDPR and the ePrivacy Directive which would trigger negative consequences on the legal practice and consequently on parties concerned as well as the economy.

By bringing the ePrivacy Regulation and the GDPR to the same level, it becomes clear that neither of the two legislative acts takes absolute precedence over the other. This corresponds to actual interests because the ePrivacy Regulation, as an expression of the secrecy of telecommunications, implies and must imply a different scope and protective character than the GDPR. Keeping the ePrivacy Regulation at the level of a directive would suggest that the data protection law takes precedence over the secrecy of telecommunications, which is not actually the case and is furthermore not appropriate. However, for clarifying the (equal) ranking of the GDPR and the ePrivacy Regulation, more clarification is needed (see below, section “Relationship with the GDPR“).

The synchronized effective date avoids the overlapping of the transition periods. Otherwise, companies would only have a period of a few months, in which the GDPR is already in force, but at the same time, the old provisions of the ePrivacy Directive and as a result, national data protection law would have been applicable. These provisions lack coherence (see section “Relationship with the GDPR“). In addition, synchronization provides the great advantage that companies are able to coordinate their implementation efforts by working towards a consistent implementation date for both legislative acts which are closely related.

The ePrivacy Regulation will replace the prevailing provisions of the German Telecommunications Act, in particular in terms of Telecommunications Data Protection (§§ 91 et seq. of the German Telecommunications Act) and Secrecy of Telecommunications (§ 88 of the German Telecommunications Act). The same applies to the provisions relating to the protection of data as laid down by the Telemedia Act (§§ 11 of the German Telemedia Act). From the perspective of German users of law, the ePrivacy Regulation will only result in an improvement if the ePrivacy Regulation reaches the same standard of normative clarity as existing law. The current draft does not meet this requirement. It should – especially from the point of view of practical handling and applicability – be revised. In this context, the following specific suggestions are provided.

Relationship with the GDPR

Suggestion:

- Art. 95 of the GDPR should be replaced by the following text: “Within its scope, the [ePrivacy Regulation] takes precedence over (EU) 2016/679.”
- Art. 21 Para. 5 of the GDPR should be removed upon the effective date of the ePrivacy Regulation. Instead, Art. 9 Para. 2 of the ePrivacy Regulation should stipulate that the right of objection can be exercised by configuring browser settings.

Reason:

The GDPR is expressly limited to the processing of personal data. As a result, the processing of communications data (subject to the protection of the secrecy of telecommunications, but not always personal data) is not considered in the GDPR. Due to a political compromise within the EU, no other regulatory areas which were subject to the ePrivacy Directive (for instance, cookie provisions) were considered. This was explicitly made clear under Art. 95 of the GDPR by including a regulation which provides that the GDPR does not impose any additional obligations in the regulatory areas of the ePrivacy Directive.

According to the wording of Art. 95, precedence of the ePrivacy Directive only applies under the following conditions:

- Precedence of the ePrivacy Directive only for “processing in connection with the provision of publicly accessible electronic communications services in public communications networks“. Thus, no precedence for the processing of simple (non-public) electronic communications services and communications networks.
- Precedence of the ePrivacy Directive only if the obligations laid down under the Directive “pursue the same objective”. When exactly this is the case is not defined in more detail and therefore a matter of interpretation.
- The (limited) precedence of the ePrivacy Directive as defined under Art. 95 of the GDPR is limited to the Directive itself, however, not to the scope for implementation granted under the Directive. In this way, any national (telecommunications) data protection law that goes beyond the mandatory implementation of the Directive is subject to the GDPR – and superseded by it. As a consequence, for instance, German Telecommunications Data Protection Act standards are replaced insofar as they go beyond mandatory Directive Law (for instance, the provisions of §§ 91 et seq. of the German Telecommunications Act also apply to non-public telecommunications services).

As far as we are aware, the EU Commission does not intend to amend Art. 95. The consequence would be that the provision is equally applied to the new ePrivacy Regulation (compare Art. 27 Para. 2 of the ePrivacy Regulation). The wording of Art. 95 of the GDPR would thus imply that the ePrivacy Regulation takes only limited application precedence over the GDPR, that is to say, only to the extent granted under Art. 95 (only in the case of public services, only if the “objectives” of the provisions are identical).

Maintaining Art. 95 of the GDPR would result in obvious problems of delimitation between the two legislative acts because the ePrivacy Regulation is to provide a scope of application (specifically compare Art. 2 Para. 1 in conjunction with the limited reverse exception under Art. 2 Para. 2 Letter d of the ePrivacy Regulation), which the GDPR does not fully granted.

The draft of the ePrivacy Regulation under Sub-Para. 1.2 of the explanations states that the ePrivacy Regulation is intended to be “lex specialis“. Art. 1 Para. 3 of the ePrivacy Regulation stipulates that the ePrivacy Regulation specifies and complements the GDPR by establishing special provisions. However, this objective – precedence as lex

specialis by specifying and complementing – is undoubtedly achieved only if Art. 95 of the GDPR is modified as described above.

A second reference to the current ePrivacy Directive is provided under Art. 21 Para. 5 of the GDPR. This provision is obviously said to mean that browser settings like the “do not track” feature are to be considered as an automatic exercise of the right of objection. Art. 21 Para. 5 of the GDPR falls within the scope of application and is therefore closely related in particular to Art. 9 Para. 2 of the planned ePrivacy Regulation (expressing consent through browser settings). “Tearing apart“ self-determination options for data privacy via the browser on two legislative acts does not make sense. This aspect should be treated consistently and conclusively either as part of the GDPR or the ePrivacy Regulation, but should not be split across two legislative acts. It should also be examined whether the user’s self-determination options must be limited to cookie provisions or whether they can be applied to any kind of data processing provided by information society services comparable to Art. 21 Para. 5 of the GDPR.

Lack of structure for the personal scope of application

Suggestion:

- For clarifying purposes, the regulation should, for all provisions where this has not been the case so far, incorporate the norm addressee to which all provisions apply. This should include consideration of different norm addressees, for instance, providers of electronic communications services, providers of information society services, responsible bodies for the processing of communications data etc.
- Art. 16 of the draft should be separated and incorporated in a regulation which contains content that is appropriate with EU legislation (for instance, Directive 2005/29/EG, so-called UGP Directive).

Reason:

The draft attempts to capture a series of very different facts and norm addressees by applying a “one size fits all“ regulation. According to Art. 2 Para. 1 the draft applies to *“the processing of electronic communications data linked to the provision and use of electronic communications services and for information related to end users’ terminal equipment“.*

This is incorrect from the start because the draft includes regulatory areas beyond the processing of electronic communications data and of end users' terminal equipment. This specifically applies to Art. 16. This article governs the issues of direct marketing under the headline "unsolicited communication" without establishing a relation to communications data or end users' terminal equipment. This standard is simply a provision of advertising and consumer protection law which is systematically improperly included in the ePrivacy Regulation. This provision should be removed from the ePrivacy Regulation for reasons of normative clarity and integrated into one of the EU's provisions relating to marketing. It should also be examined whether such a provision is required at all or if the subject area is already sufficiently regulated.

More severe is the fact that the draft of the ePrivacy Regulation lacks any kind of structure in terms of the personal scope of application. In principle, this applied to the previous ePrivacy Directive as well. However, so far, the member states were free to split provisions into "appropriate" laws and specify the respective addressee of the respective provision due to the nature of the directive. This has been done in Germany by partially incorporating the rules of the previous ePrivacy Directive into the Telecommunications Act, the Telemedia Act and the Federal Data Protection Act. Accordingly, it was comprehensible whether the relevant provisions apply to the operators of telecommunications services (≈electronic communications services, ECS) and to operators of telecommunications networks (≈electronic communications networks, ECN), to providers of telemedia (≈Information Society Services, ICS) or to all parties responsible within the meaning of the Data Protection Law.

On the effective date of the ePrivacy Regulation, this clarification will no longer be possible. Instead, the rules of the ePrivacy Regulation will apply directly. However, its standards are predominantly explained as if there were no limitations to the personal scope of application. This seems to imply that ultimately everyone must adhere to the provisions of the ePrivacy Regulation. This approach is in principle legally problematic because the ePrivacy Regulation is *not intended to be* an "everyman's right" but part of a special provision for a very specific economic sector and a certain group of norm addressees.

In addition, many of the provisions have obviously been directed at a very specific group of addressees (for instance, operators of websites or providers of electronic communications services), without this being clarified. The effect is that a number of legal provisions are addressed to people who cannot implement them. Some provisions, for instance Art. 3 Para. 1 Letter b) are even totally incomprehensible due to this fact. This problem runs like a red thread through almost the entire draft regulation, which is why the entire draft should be revised and restructured if needed (for instance, by splitting up the regulatory areas, sorted by norm addressees in different sections). Some cases are discussed separately below.

Extension to OTT services

Suggestion:

- Regarding the application on OTT services, the Commission should examine whether all provisions of the ePrivacy Regulation are appropriate for innovative services providers and can be implemented under proportionate conditions.
- It should be examined in particular whether flexible statutory permissions in analogy to Art. 6 Para. 1 Letter b and Letter f of the GDPR can be added for the processing of communications data (processing necessary to perform a contract and based on legitimate interests involving the simultaneous balancing of interests).
- Recital 18 should make clear that the prohibition of coupling of consent solely applies to basic internet access and voice communications services but not to innovative OTT services.

Reason:

The ePrivacy Regulation intends to extend its scope of application according to its recitals to include so-called OTT services. While this has been described in detail in the Commission's explanations with regard to the previous legislative procedure and in the recitals, reference to OTT services in the actual text of the Regulation is limited to the definition part under Art. 4 Para. 1, where reference is made to the European Electronic Communications Code (EECC).

According to the expert committee, the subject of OTT indeed pertains rather to the legislative procedure of the EECC than to the ePrivacy Regulation. The applicability of the special provision to electronic communications services is a basic and general

question in many forms; the regulatory areas of the ePrivacy Regulation are just one form. The expert committee therefore wishes to emphasize that the question of regulating OTT services should not be considered in isolation as a matter of the ePrivacy Regulation but be answered generally as part of the creation of the EECC. Specifically regarding the question of governing OTT services according to the ePrivacy Regulation, it must be stated that under the “Level Playing Field“ aspect there may be convincing evidence for controlling providers with the same business model in equal way, that is to say, technology neutral. But, it should also be considered that OTT services are frequently much more innovative and provide users new functionalities and features. Traditional providers of electronic communications services and communications networks are also becoming increasingly innovative. “Unified communications“, “IoT“ and “M2M“ are the buzzwords to describe the development of new products and business models. They are often based on the innovative combination of different stages of the value chain (for instance, combining the functionality of a telephone system with internet access services) or novel evaluation techniques for personal and non-personal data. The vast majority of these services do not, in itself, represent any increased threat to end users’ privacy; they are simply additional innovative products available on the market.

Innovative products from the OTT segment or the traditional telecommunications sector often require the use of communications data which has not been anticipated by legislators. This fact is an argument against the excessive constriction of statutory permissions as they were not flexible enough to respond to innovative services. The fact that the ePrivacy Regulation does not contain a provision for permission in analogy to Art. 6 Para. 1 Letter b (processing necessary to perform a contract) and Letter f of the GDPR (prevailing interests of the data processor) (statutory permissions see below, Paragraph “Statutory Permissions under Art. 6“) is therefore considered to be critical. As part of the balancing of interests, the increased confidentiality requirement of communications data would have to be taken into account.

Moreover, users do not always have the same confidentiality expectations of OTT services as they have of “classical” electronic communications services. On the contrary, users will frequently expect added value from OTT services, for instance, for

managing or sharing their personal data. The ePrivacy Regulation should consider this structural difference between OTT services and “classical” services as well.

According to the expert committee, this does not imply that the ePrivacy Regulation should give up its technology-neutral approach. However, the provisions of the ePrivacy Regulation should be adapted in such a way that the requirements of OTT providers are taken into account, instead of “killing” them with poorly adapted provisions.

OTT providers must in particular be able to obtain consent from those affected and/or end users to enable them to perform their innovative services. Excessive requirements for effective consent would be incompatible with this. Providers must particularly be able to obtain effective consent at all. This requires providers to provide their services based on the consent for using (personal) communications data (so-called linking) because often, this kind of consent is the prerequisite for the legality of such services.

Whether consent is “voluntary” and therefore valid if linked to performing a service, is often doubted in view of Art. 7 Para. 4 of the GDPR. It must be possible, however if applying the ePrivacy Regulation to OTT services is not meant to result in disproportionate consequences (which would lead to large quantities of users of these services being strongly annoyed). Recital 18 of the ePrivacy Regulation is a step in the right direction. It hints at the fact that – without expressing it clearly – the prohibition of coupling is only effective if the requirement of consent is linked to an “indispensable“ service. According to Recital 18, this refers to “fundamental and broadband internet access and voice communications services” – and therefore, definitely not to OTT services. This approach is to be advocated but should be specified in more detail. So far, the exact wording of Recital 18 does not stipulate that non-fundamental services are not covered by the prohibition of coupling.

Recital 18 should be still be clarified. More details on the permitted combination of services and consent should refer to all providers of electronic communications services and information society services.

Extension to communications services provided as an ancillary feature

Suggestion:

Art. 4 Para. 2 of the draft should not be adopted.

Reason:

Beyond the extension to OTT services, Art. 4 Para. 2 of the ePrivacy Regulation states that the term “interpersonal communications service“ (including regulated electronic communications services) shall in the future comprise services *“which enable the interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.“*

This provision would result in the fact that the telecommunications regulation – even beyond the regulation of OTT services – was extended to services with no focus on electronic communications services at all. This is not a question of technology-neutral equality but the attempt to generally extend the scope of application of the telecommunications regulation. Art. 4 Para. 2 of the draft regulation in particular constitutes a breach of the paradigm, stating that those providers of electronic communications services are regulated who provide a service that *fully or predominantly* consists of transmitting signals via electronic communications networks (as stipulated under Art. 2 Letter c of the Framework Directive 2002/21/EG). The applicability of the telecommunications right to service components which can be separated and are considered to be an independent service – based on applicable law – remains unaffected. Thus, the telecommunications regulation can already be applied to these services.

The extension of the ePrivacy Regulation to “ancillary services“ would in contrast comprise, for instance, communications services, which are offered as an add-on for computer games (for instance, chat options or TeamSpeak) or online editing tools for documents (for instance, chat and comments features for Google Docs). The provisions of the telecommunications regulation, however, are designed for professional and specialized providers of electronic communications services and networks. There is no meaningful scope for services with ancillary communication features; moreover, users do not expect confidentiality within the meaning of the secrecy of telecommunications. Moreover, the term “provider” should be defined consistently for reasons of normative

clarity of the EECC. This is another reason why a special provision should not be included in the ePrivacy Regulation.

Clarification of the scope of application: not applied to anonymized metadata

Suggestion:
The following sentence should be added under Art. 4 Para. 3 Letter c: “Data is not deemed to be electronic communications data if not related to natural or legal persons or if data cannot be related to them.”

Reason:
The ePrivacy Regulation draft is unclear with regard to the question whether anonymous and/or anonymized data is protected as communications data.

Art. 7 Para. 1 and Para. 2 seem to assume that the ePrivacy Regulation (like the GDPR) does not apply to fully anonymized data. Recital 17 also seems to assume that non-personal metadata is not subject to the prohibition with the right of permission from the outset. However, there is a lack of any explicit clarification in the draft. The definitions of the terms “electronic communications data” (Art. 4 Para. 3 Letter a); “electronic communication content“ (Art. 4 Para. 3 Letter b), and “electronic communications metadata“ (Art. 4 Para. 3 Letter c) in particular seem to cover data independent of whether they relate to a specific (natural or legal) person and/or are can be related to a specific (natural or legal) person or not.

It seems appropriate to differentiate on this issue.

- The confidentiality of communication content should be protected even if this data is not related to a person. This is because communication content can contain information of high secrecy or privacy interest (for instance, company secrets), independent of its reference to a person.
- In the case of metadata it is not comprehensible why the protection of the ePrivacy Regulation should comprise data even if data has been anonymized. In the event of a lack of personal reference and/or after the anonymization there is no legitimate secrecy or data protection interest anymore.

The usability of non-personal data is essential for the digital economy and in particular for providers of electronic communications services, for instance, for the use of “Internet of Things” services (M2M communications) or for other innovative products (see above, OTT services). No unnecessary obstacles should be put in the way of the digital economy by forcing providers to specifically protect data without any reference to privacy.

Clarification of the scope of application of the secrecy of telecommunications under Art. 5

Suggestion:
Art. 5 should clarify that the group of addressees exclusively consists of providers of electronic communications services, providers of electronic communications networks and persons contributing to performing such services and/or operating such networks who are subject to the obligation of maintaining confidentiality of communication.

Reason:
Art. 5 of the Regulation provides for the secrecy of telecommunications. However, the wording of the provision is contourless so that the traditional secrecy of telecommunications can hardly be recognized.

The secrecy of telecommunications is a fundamental right to preserve confidentiality of communication. Initially, this fundamental right was intended to be a citizen’s right of defense against the state; at the level of EU law it constitutes a form of general protection of remote communication (Art. 7 EU’s Charter of Fundamental Rights and Art. 8 Para. 1 ECHR). In the course of the privatization of the telecommunications sector from about 1995 onwards, the secrecy of telecommunications has been extended to include private companies who replaced state authorities as providers of electronic communications services and/or network operators. To avoid the reduction of the level of protection private providers were required to maintain the confidentiality of communication. The justification for the direct extension of the right to protect a fundamental right to private law (in legal terms a very rare process) is that private companies assume a role and responsibility of guaranteeing the secrecy of telecommunications which is similar to the state’s. The secrecy of telecommunications

is intended to prevent that citizens are deterred from using remote communications means; in the case of remote communications they “lose control” of what they say and inevitably have to provide their communication to unknown entities. To avoid a chilling effect on communication, the structurally higher threat to communication content in transit is compensated by the additional obligation to maintain confidentiality.

For this reason, the secrecy of telecommunications has historically always been limited to a certain group of people and providers, that is to say, to the group of providers who transmit content and get to know such content (for instance, to ensure network security). The secrecy of telecommunications is similar to other secrecy obligations which apply to certain groups of people, for instance, legal or medical professional secrecy. The particular significance of these provisions results from their awareness and validity. Each provider of this group of people and/or group of providers and all parties affected are aware of this kind of secrecy obligations and consider it to be a special obligation.

Contents of the obligation of secrecy are easily captured and comprehensible and are therefore not only treated as a general compliance issue but as a fundamental issue of professional ethics by obligated parties. Vice versa, personal secrecy obligations like the secrecy of telecommunications experience higher confidence of validity.

However, there seem to be no restrictions to a specific group of people under Art. 5. On the contrary, Art. 5 seems to refer the obligation to maintain confidentiality of communication to “everyman”.

“Messages“ are protected against “eavesdropping“ (“tapping”, “wiretapping”), against “intercepting” and “monitoring” as well as against “storing” pursuant to the previous Art. 5 Para. 1 of the ePrivacy Directive. Art. 5 of the ePrivacy Regulation is intended to extend the scope of the prohibition now: in general, all kinds of “processing“ “communications data“ is to be put under the prohibition with the right of permission. Art. 5 of the ePrivacy Regulation thus seems to put the entire processing of telecommunications data under reservation of permission, *even after the telecommunications process has been concluded*.

On the one hand, this would end the focus of the secrecy of telecommunications on a specific group of people, thereby breaking with the historic tradition of the right of defense against the state and state-like providers.

On the other hand, the extension of the scope of Art. 5 to non-service providers would result in specific practical problems. This is because communications data is not considered to be *communications data at all* by people who are neither providers of electronic communications services nor of electronic communications networks. The previous form of the secrecy of telecommunications no longer protects communications data separately after communication has been received (with the exception of communications metadata which is permanently protected by a protective reflex of the secrecy of telecommunications against data collection by the state).

From the perspective of people who are not providers of communications services or networks, there is no specific reference to the transmission process and consequently no special requirement to protect data that has been received. Nevertheless, Art. 5 would, interpreted in terms of its wording, imply that non-service providers are bound to the secrecy of telecommunications, that is to say, even for data which is not transmitted anymore but has already been received.

Such an extension of the secrecy of telecommunications to “other third parties” is not only incompatible with its specific requirement to protection; it does not make any sense on its merits. Requiring non-service providers to comply with the secrecy of telecommunications would have disproportionate consequences. In this case, access to any kind of telecommunications data would be prohibited to “everyman” and/or would involve extremely tight prerequisites. This would also apply to data that is not being transmitted anymore but has already been received. It would, for instance, be prohibited to store received emails for a third party or read out data about past phone calls from a device memory (for instance, to create a backup of the device).

Permissions under Art. 6

Suggestion:

- The structure of Art. 6 should basically be revised. A new structure of the standard (by splitting several articles if needed) should clarify the relationship between prohibitions and permissions.
- The end user's right to enable the processing of their data by granting consent should not be limited. The right to informational self-determination includes the right to authorize data processing considered to be "unreasonable" from the perspective of restrictive data protection.

Reason:

Art. 6 contains a series of permission provisions addressing providers of electronic communications services and operators of electronic communications networks. Unfortunately, essential aspects of the provision are systematically unclear.

- First of all, the relationships of these permission provisions with the permission provisions of the GDPR are unclear a priori (in particular Art. 6 and Art. 9 of the GDPR). It complies with the traditional understanding of telecommunications data protection if Art. 6 was meant to be final, that is to say, prohibit the processing of electronic communications data, which is not permitted under Art. 6 of the ePrivacy Regulation by the specific group of providers, i.e., providers of electronic communications and operators of electronic communications networks. However, there is no such clarification under Art. 6. The current wording suggests such a prohibition with the right of permission under Para. 3 ("only"), while this addition is not provided under Para. 1 and Para. 2.
- Moreover, the relationship of the permission provision under Para. 1 with the permission provisions under Para. 2 and 3 is unclear. Para. 1 refers to all communications data, while Para. 2 and Para. 3 only capture metadata and/or content data. In addition to providers of electronic communications services Para. 1 includes operators of electronic communications networks, while Para. 2 and Para. 3 only include services providers.
- The entire context of Art. 6 is unclear as to whether these permission provisions are mutually exclusive or whether they are to be applied cumulatively side by side.
- Against this background, the provision should be fundamentally revised. It should be considered that prohibitions ("you are not allowed to") and permissions ("you are allowed to") are systematically separated. The respective scope of application for the prohibition and permission provisions should be undoubtedly clear. Moreover, the relationship of the prohibitions and permissions should be clarified, in particular by stating which prohibition can be overruled by which permission provision, and by which not.

- The respective paragraphs are unclear with regard to the relationship between the statutory permissions stated therein. Art. 6 Para. 3 in particular provides for two different justifications which both require the user's consent. It is not sufficiently clear in which cases the two sub-paragraphs are to be applied.
- The reservation included in many permission provisions under Art. 6 is to be rejected in any case as it stipulates that the user's consent is ineffective in certain cases. The user's consent is to be considered ineffective a priori if "relevant purposes can be achieved through the processing of anonymized information […]" (Art. 6 Para. 2 Letter c); if "the service can be provided without processing the content […]" (Art. 6 Para. 3 Letter a); or if the "purposes […] can be provided through the processing of anonymized information […]" (Art. 6 Para. 3 Letter b). In these cases, the ePrivacy Regulation draft would deprive users of their freedom to dispose of their data: according to the draft, the user's informational self-determination based on their consent will be impossible a priori if data processing – in the view of the legislator – is "unreasonable" because a more data protection-friendly solution would be possible. By applying this regulation, the legislator takes the place of the affected party – and wants to be able to refuse consent in their stead. There is, however, no justification for interfering with the right of self-determination of the parties affected. The exception to the option of consent deprives users of the possibility to weigh the disadvantages of privacy against the advantages in other areas and give their consent based on the overall consideration of advantages and disadvantages. In other words: citizens should not be able to authorize the processing of data even if they consider it advantageous – merely because of a loss of privacy. The restrictions on the user's right to consent should be deleted. The basic obligation for data minimization (Art. 5 Para. 1 Letter c of the GDPR) shall, of course, remain unaffected.

No obligation for service providers acting in the sphere of the recipient to the secrecy of telecommunications

Suggestion:

- The ePrivacy Regulation should clarify that providers of electronic communications services who receive communication content on behalf of a subscriber and process this content after receiving it, are no longer treated as providers of electronic communications services but rather as third parties within the meaning of Art. 7 Para. 1 Sentence 2 of the ePrivacy Regulation.

Reason:

Innovative communications services, in particular (but not limited to) the OTT segment often combine the functionalities of transmitting messages with features that rather belong to the sphere of end user communications. Because these services are from a technical perspective no longer provided where the end user us located but in the cloud, a grey zone has emerged in which these features can be hardly differentiated from electronic communications services.

“Telephone systems in the cloud“, for instance, fall under the abovementioned category. They transfer phone calls to the public switched telephone network (PSTN) and combine them with features of traditional telephone systems (for instance, call forwarding, pickup of calls, storing, processing and transmission of call data and sometimes recording of conversations). These features do not take place locally in the premises of the subscriber (as is the case with a traditional telephone system) but “in the cloud“. Users access these features with the help of connected end devices or via a web portal. The features of a “telephone system in the cloud“ are from a technical perspective and under certain circumstances performed at a time when the communication has not yet reached the end user. This results in difficult delimitations regarding the question whether the provisions for the protection of the secrecy of telecommunications are already being applied (which would legally prohibit essential features of these services).

The same problem occurs with email services (in particular web mail services) offering additional features like the presorting of messages (in particular to fight spam) or the automatic filtering of messages with harmful content (viruses, Trojans).

Some email services are financed through context-based advertising and therefore require the scanning of emails. According to the newly defined wording of Art. 5 of the ePrivacy Regulation, the scanning of communication content is to be considered as an interference in the secrecy of telecommunications – apparently even if it is performed fully automatically and without any human being taking notice. If you think this through to the end, it means that the scanning of emails (for instance, for detecting virus attacks) is not possible, unless consent is available from all affected end users – in

particular the consent of the *sender* of malicious software or spam mail (compare in particular the wording of Art. 6 Para. 3 Letter b of the ePrivacy Regulation and Recital 19 Sentence 4 to 7 of the ePrivacy Regulation). Spam filters are a useful technology which systematically scans emails and searches for typical features of unsolicited messages. Requiring not only the consent of the recipient of the message for such filters but also the consent of the sender (spammer) results in spam mails finding their way to the recipient without being stopped.

The ePrivacy Regulation should not attempt to define spam filtering or cloud telephone systems as an exception to the secrecy of telecommunications but treat them for what they are right from the start: they process communication content that has already reached the sphere of the recipient. Therefore, this data must no longer be subject to special provisions for the protection of communication in transit; regular data protection law is sufficient.

The ePrivacy Directive should provide a structurally clear solution to the problem described by providing clear criteria as to which services fall *into the sphere of the subscriber*, that is to say, are no longer bound to the provisions of communication confidentiality. Once content has reached the sphere of the recipient, it should only be subject to “regular“ data protection law pursuant to the GDPR, according to Recital 19, Sentence 8 and 9 of the ePrivacy Regulation.

In order to prepare this clarification, the elaboration of the current draft may build on Art. 7 Para. 1 Sentence 2. It (obviously declatory) excludes “third parties“ from the scope of confidentiality provisions if they record or store communications data on behalf of the end user. Art. 7 (or the definition part of the ePrivacy Regulation or the EECC) should clarify that providers of electronic communications services are to be treated as third parties within the meaning of Art. 7 Para. 1 Sentence 2 of the ePrivacy Regulation in the case they receive communication content on behalf of a subscriber and process this communication content *after* receiving it.

This solution would ensure that services like the spam filtering of emails or cloud telephone systems remain permissible because they are no longer subject to electronic communications services and thereby not subject to the secrecy of telecommunications.

These services would therefore no longer be subject to the specific provisions of Art. 5 et seq. of the ePrivacy Directive, but (only) be subject to the GDPR. A protection gap is not to be feared because the GDPR will continue to be applicable.

Questionable provision regarding end device information under Art. 8 Para. 2

Suggestion:

- The provision should be deleted. The notion of protection of Art. 8 Para. 2 remains unclear. It is not incomprehensible why end device information require additional protection as opposed to other data. Quite to the contrary, such data has only little privacy reference. But, they are essential for a variety of web applications and for law enforcement on the internet.
- If the standard is sustained, its personal scope should at least be clarified. Applying it to providers of electronic communications services or network operators is not reasonable because this group of providers is already subject to special provisions for communications metadata.

Art. 8 Para. 2 prohibits "*the collection of information sent by terminal equipment in order to connect with other devices or network systems*". As with many other provisions of the ePrivacy Regulation it is not clear who is subject to the personal scope of the standard. The standard seems to address "everyman", even if the EU Commission obviously had specific application scenarios in mind.

At the current stage, the wording of Art. 8 Para. 2 seems to refer to several different application scenarios, for instance, reading out wireless network identifiers by providers of navigation databases, or storing communication-related device data (for instance MAC address, IMSI) by providers of electronic communications services or network operators.

The notion of protection of the standard is not clear.

- The provision cannot be reasonably applied to providers of electronic communications services and operators of electronic communications networks. It is not comprehensible why terminal equipment information for this group of providers require different

protection mechanisms than other communications metadata. Quite on the contrary, there is much to suggest that this information requires exactly the same protection than other communications data.

- For all other potential norm addressees (Art. 8 talks about “everyman’s right“) the notion of protection as defined by Art. 8 Para. 2 seems to be exaggerated. This group of providers do not consider this kind of data as communications data a priori (see above, unclear definition of the term, Paragraphs “Lack of structure for the personal scope of application“ and “Clarification of the scope of application of the secrecy of telecommunications under Art. 5”).
- Furthermore, it is questionable why data sent from end devices are to be specifically protected. Such data are identifiers but they are basically intended for an indefinite public comparable with a phone number. Therefore, they are not at all data which individuals consider to be specifically confidential but – quite on the contrary – data without special privacy reference.
- It may be possible that the Commission used Art. 6 Para. 2 – without making it clear – for a very specific group of providers, that is to say, providers of information society services who as operators of websites or advertising space on such websites use end device data to collect information about their users.

If this presumption is correct, it is still questionable why the ePrivacy Regulation limits the use of transmitted device data. The storing of user-related data in “server logs“ and comparable data has become established practice which serves a number of legitimate purposes; including the defense against hacking and DDoS attacks or the prevention of spam mails (for instance, in commentary columns of web logs). In addition, law enforcement on the internet, for instance, the prosecution of criminally relevant statements in social networks, requires to a certain extent that service providers store user-related data. And, as far as storing user profiles is concerned, profiling is regulated by the GDPR. It is not comprehensible why device-related profiling activities should be treated differently from “normal“ profiling activities.

Clarification of the norm addressee under Art. 9 Para. 3

Suggestion:

Art. 9 Para. 3 should clarify who is obliged to make a reminder and/or guarantee that the reminder is made.

Reason:

Art. 9 Para. 3 uses an unclear passive formulation so that it is not clear who actually is the norm addressee of the provision (see above, Paragraph “Personal Scope“). It should be clarified who exactly must meet this obligation.

Regarding the possible clarification of the prohibition of coupling we refer to Para. “Extension to OTT providers“; regarding the relationship of Art. 9 Para. 2 with Art. 21 Para. 5 of the GDPR we refer to the Para. “Relationship to the GDPR“.

Questionable provision of browser software under Art. 10

Suggestion:

- Art. 10 should use accurate and customary terms. Instead of talking about “software that has been distributed to enable electronic communications, including the retrieving and displaying of information from the internet“, the term “browsers” should be used. Instead of “information in terminal equipment” the term “cookies” should be used.
- Art. 10 Para. 3 should clarify that any obligation to display information exists only to the extent that users download and install a software update.

Reason:

The provision under Art. 10 of the draft refers to product features of software enabling electronic communication. It does not, therefore, refer to any provisions which affect the process of telecommunication itself. In terms of content it provides that such software must be appropriate to prevent that other persons than the user of the software store information on their computer or process information that has already been stored. It is all about providing the user with means to prevent cookies or other tracking methods from tracking their behavior on the internet. The software is also intended to inform the user about data protection settings during installation and request his or her approval of these setting before the installation is completed.

The provision is intended to ensure that the browser and comparable software empower the user to deliberately choose their data protection settings. It does not at all require that the default settings are selected in such a way that the use of common methods is

prevented. The objective of the provision is to be advocated. Moreover, we advocate that it is not compulsory to select special pre-settings that promote data protection. Such a requirement could massively impede the use of the internet because the required pre-settings may hinder the use of many internet websites or even make it impossible to use them.

The wording of the provision also uses the very cumbersome description of *“software enabling electronic communication, including the retrieving and displaying of information from the internet“.* Contrary to what was apparently intended, this very broad definition would not only cover browsers but almost all types of software related to the internet in the broadest sense. Relating the interpretation of the provision solely to its wording includes almost any app on mobile devices and other software on routers, modems and other communications components – all the way through to operating systems of telephone systems and mobile phones.

It is also questionable what is to be understood under the term “information“ which *“third parties […] store in the terminal equipment of an end user“* and/or process in the end device. The expert committee wishes to point out that the supposedly hasty use of websites when “browsing“ always constitutes a download from a technical perspective and that a lot of web content continues to be stored on the user’s device for quite some time (for instance, in the download files or cache memory). The “whether“ of the download and the duration of storage is always at the user’s discretion and can be configured by the user. Even the external access to files and capacities provided in the user’s end device is, from a technical perspective, a standard web content process (for instance, for using JavaScript or apps). However, it is subject to the user’s full control (by means of configuration options).

Whether the inclusion of the provision in a regulation specifically addressing the telecommunications segment is purposeful seems to be doubtful (see above, Para. “Personal Scope“). Art. 10 does not only refer to telecommunications data. It refers to data generated during electronic order processes and even data that has nothing to do at all with telecommunications. In this context, the regulation falls out of the scope of the other provisions contained in the ePrivacy Regulation.

Assuming the approach of regulating the configuration options of browser software sustains, we suggest that software is designed accordingly so that the user can easily change data protection settings. The user must not only be informed, but also be capable of selecting appropriate security settings and of installing and changing them according to their (potentially changing) requirements. Without such a possibility, the provision is incomplete. Software that can only be changed in complicated ways does not make users autonomous.

Lastly, it should be noted that the obligation provided for under Art. 10 Para. 3, i.e., information about the configuration option of the browser by 25 August at the latest can only be fulfilled if the user can download and install a software update. The providers of browser software cannot conclusively influence this. Therefore, it should be specified that the obligation is subject to the condition that users download and install an update that has been made available.

Lack of formulations to protect fundamental rights under Art. 11

Suggestion:

- Art. 11 should use the most recent ECJ rulings for a restrictive clarification of the requirements for intervention, instead of making the fact even more vague. Alternatively, the wording of Art. 15 of the ePrivacy Directive should be maintained.
- The elimination of the data retention provision is not comprehensible. The elimination cannot change the legal situation because the restrictions for the admissibility of data retention directly arise from the EU's Charter of Fundamental Rights. The elimination of the provision, however, affects the transparency and clarity of the standard.
- The wording of Art. 11 Para. 2 is far too imprecise and inappropriate for a "ePrivacy Regulation". The provision should not be adopted, but at most (more precisely) be incorporated into the EECC.

Reason:

Art. 11 of the draft regulation contains provisions allowing individual states to limit the secrecy of telecommunications for certain public interests as stated in Art. 23 (1) (a) to (e) of the GDPR. The addition of the reasons for interventions is explained by the adoption of provisions from the General Data Protection Regulation (VO (EU) 2016/679

dated 27 April 2016). It does not consider the special worthiness of protection of telecommunications data (see above, Paragraph “Introduction“).

Art. 15 Para. 1 of Directive 2002/58/EG (ePrivacy Directive) contained a similar provision. The new provision seems to extend the possibilities of intervention. Public interests that justify interventions now include national security and other important objectives of general public interest within the Union or in its member states in addition to national defense and the prevention, detection and prosecution of criminal offenses. Other important objectives include economic and financial interests of the Union and its member states. Moreover, the provision of the previous Art. 15 Para. 1 Sentence 2 of Directive 2002/58/EG no longer applies, which expressly permitted the retention of data based on tight conditions.

In contrast to Art. 15 Para. 1 of Directive 2002/58/EG the provision does not include any detailed rules which describe the preconditions for interventions. It only requires that interventions maintain the essence of fundamental rights and are necessary, adequate and proportionate. The structure of the provision corresponds with that of Art. 15 Para. 1 of Directive 2002/58/EG. The legislative character corresponds with that of a directive but not that of a regulation.

Moreover, the objective of the proposed regulations remains unclear: while the draft preamble states that it is intended to ensure *“a high level of protection of privacy of users of electronic communications services“*, Recital 42 of the draft reads that the planned regulation aims to *“ensure an equivalent level of data protection”,* which raises the question what level of national data protection is to be used as the point of reference.

The extension of the potential reasons for intervention in the secrecy of telecommunications is dubious in terms of content. It is not perceptible what is considered a threat to national security that is neither related to the defense nor the fight against crime. Therefore, it is totally unclear why this additional justification was incorporated into the legal text. This is even more true of the further justification of the threat to general interests. According to the text of the regulation this includes financial

interests of the government. Altogether, the intervention possibilities have been significantly expanded.

The extension of the possibilities of limiting the principle of confidentiality for the use of electronic communications services is incompatible with EU legislation on the basis of the essential elements of the ruling of the ECJ of 21 December 2016 (C-203/15 and C-698/15). The Luxembourg judges emphasized in their ruling that the narrow interpretation of Art. 15 Para. 1 Sentence 1 of the E-Privacy Directive as an exception in the light of Art. 7, 8, and 11 of the EU's Charter of Fundamental Rights was final and that the retention of data was only permissible for the purpose of crime control. The draft does not consider this limit, which also applies to other interventions in affected fundamental rights.

It is questionable that Art. 15 Para. 1 Sentence 2 of Directive 2002/58/EG is not adopted and not replaced by another regulation. Retention of data is not prohibited thereby; it is just not expressly mentioned anymore. The draft regulation thus avoids a more detailed examination of the ECJ's principles which deals with the regulation in Art. 15 Sentence 2 of the Directive 2002/58/EG in its decision of 21 December 2016 (C-203/15 and C 698/15) and which the ECJ has interpreted very restrictively. The ECJ emphasized in the ruling that no *"general and indiscriminate retention of data traffic and location data"* was permissible even for fighting organized crime and terrorism because the exceptional character of data retention is lost in this case as well. The relevant restriction is not available in the suggestion.

In view of this jurisdiction the extension of intervention possibilities is even more surprising. The ECJ did not for the first time emphasize (compare ruling of 8 April 2014 C-293/12 and C 594-12) the high significance in particular of the protection of the confidentiality of telecommunications and based their ruling on Art. 7, 8, and 11 of the EU's Charter of Fundamental Rights. These fundamental rights are not only to be respected in conjunction with data retention provisions but in conjunction with any other intervention in fundamental rights protected by the ePrivacy Regulation. This particularly applies to "eavesdropping" and "reading" of telecommunications data. This is only permissible if it is imperative to fight the most serious forms of crime. Access to data is possible only in cases where data is stored based on data retention provisions

(according to the ECJ, ruling of 21 December 2016, C-203/15 and C698/15). However, the mere storage and/or knowledge of telecommunications metadata can easily result in extensive personality profiles and therefore in massive interventions in privacy and the freedom of expression. This is the very reason why interventions are only permissible in rare cases (ECJ, ruling of 21 December, 2016, C-203/15 and C698/15).

Art. 11 Para. 1 of the draft does not explicitly address this. Instead, these restrictions result only from the interpretation of the standards provision, which permits interventions only if they are deemed necessary, adequate and proportionate in a democratic society, and if fundamental rights are respected. The states will have to observe all these requirements when devising their provisions (associated limitations arising for the German legislator compare the GBA's opinion 50/16).

The regulator should not take the limitations drawn by the ECJ as an opportunity to further weaken imprecise facts but drive the clarification of Art. 11 Para. 1 against Art. 15 Para. 1 Directive 202/58/EG. This would be opportune because of the fact that we are discussing a regulation now, and not only a directive. In this context, the EU legislator should determine the limits of interventions arising from EU primary law and not have national legislators define them. The planned extension of the possibilities for intervention is not compatible with it. Therefore, it should be omitted.

Even more serious concerns arise with regard to Art. 11 Para. 2 of the draft. This standard obliges providers of telecommunications to set up internal procedures to meet the requirements of the authorities for access to telecommunications data. Both the content of telecommunications and metadata generated during the communications process are affected. On request, providers have to inform the regulatory authorities about these procedures as well. Again, the provision does not provide more details, although this standard, unlike Art. 11 Para. 1 of the draft, directly obliges providers and not only empowers the individual states to devise provisions. The obligation relates to the powers of intervention of state authorities, which the draft itself does not regulate. The authors of the draft therefore cannot know the extent of the measures and the costs involved. The provision is therefore disproportionate. It is also extremely uncertain. It does not even to some extent explain the type of measures.

The provision should therefore be restricted to allow states to impose obligations in connection with intervention powers on telecommunications providers which they have mandated based on Art. 11 Para. 1.

The provision is also disproportionate because the obligations are not limited in any way. It is in any way not apparent from the provision that the measures must be taken only if they are appropriate and proportionate. The ECJ emphasized in its ruling of 21 December 2016 that precise provisions regarding “how“ to perform the retention of data and the related retrieval process (“2. stage“ = retrieval of data stored with companies by authorities) are necessary because this is the only way to ensure real control of authorities.

The intended Art. 11 Para. 2 does not even meet this requirement to some extent: the legal text does neither provide information about the previous control of complying with the requirements for retrieval by a court or independent authority as deemed necessary by the EJC, nor that the persons affected by data retrieval need to be informed about the measure regularly afterwards. Finally, there are no provisions about the *“particularly high level of protection and security“* as emphasized by the EJC to ensure the irrevocable deletion of data by operators after expiry of the retention period.

The text of the provision does not provide information about the efforts in connection with the obligations of the service provider. However, the efforts for such measures can make business models unprofitable (especially for smaller providers and providers of OTT services). This must be taken into account by the legislator by applying respective provisions because the entrepreneurial freedom of providers is also protected by Art. 16 of the EU’s Charter of Fundamental Rights. It would be possible that the state which orders the provisions bears the costs for such measures or that the measures are limited to economically acceptable measures in view of the seriousness of the dangers to be fought against. The standard cannot be accepted without these provisions even if it merely contains a regulatory power for the individual states.

Overall, Art. 11 Para. 2 of the draft should only provide for the power for the individual states in the same way as Art. 11 Para. 1 of the draft and oblige the service providers to take appropriate measures for respective occasions, taking into account the interests of

providers which enable authorities to exercise their powers of interventions. Costs would have to be borne by the individual states.

Cooperation between regulatory authorities under Art. 18

Suggestion:

- Art. 18 should clarify that data protection authorities must consider the provisions of the telecommunications law when they exercise their control function pursuant to the ePrivacy Regulation, in particular the regulatory principles (Art. 8 of Framework Directive 2002/21/EG).
- The sentence “The tasks and powers of the regulatory authorities are performed in terms of the end users“ should be deleted. The supervisory authority should not relate to a certain group of people concerned but neutrally refer to the provisions of the ePrivacy Regulation.
- The exception “if it is purposeful“ under Art. 18 Para. 2 should be deleted.

Reason:

It is basically advocated that the ePrivacy Regulation shifts the responsibility for telecommunications data protection away from national sector-specific regulatory authorities to the respective data protection authorities. This complies with the need for protection of this data and the broad overlapping between data protection and the protection of telecommunications data (in the form of the secrecy of telecommunications).

The ePrivacy Regulation should, however, ensure that the competences of the telecommunication-specific regulatory authorities continue to be exploited. On the one hand, these authorities are more familiar with the specifics of telecommunications regulations due to their responsibility for the remaining telecommunications provisions. On the other hand, the ePrivacy Regulation provides for provisions which exclusively relate to telecommunications law and have no reference to personal data whatsoever. Notions of data protection cannot be transferred in such areas (see above, special obligation of providers in the telecommunications sector, Section “Clarification of the scope of application of the secrecy of telecommunications under Art. 5“). Only the mutual obligation to consult each other regarding facts where there are overlaps ensures that data protection authorities keep an eye on the specifics of the

telecommunications data protection law (as an expression of the secrecy of telecommunications).

Against this background, the last sentence of Art. 18 Para. 1 must be rejected and should be removed. If data protection authorities are to become part of the sector-specific regulation of the telecommunications sector, this power must not be limited to “end users“; on the contrary, authorities will have to ensure neutral regulation which is not intended to primarily protect one certain group, but should consider the perspectives of other parties involved and primarily be oriented to the regulation principles of telecommunications law (compare Art. 8 of Framework Directive 2002/21/EG). This should be clarified in the ePrivacy Regulation accordingly.

The restriction of the obligation to consult National Regulatory Authorities under Art. 18 Para. 2 (“if this is appropriate“) is therefore wrong and must be rejected. The obligation to collaborate with the National Regulatory Authorities should be laid down in principle for all provisions of the ePrivacy Regulation without reservation.