Council of the European Union
General Secretariat

Brussels, 25 July 2019

WK 8864/2019 INIT

LIMITE

COMPET
CONSOM
DATAPROTECT
MI
TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	ePrivacy : DE comments (doc. 11001/19)

Delegations will find in annex DE comments on ePrivacy.

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. 11001/19 of 12 July 2019)

Overall comments

I. General remarks:

1. Germany is in favour of continuing to guarantee the confidentiality of communications and protection of privacy and private life via an ePrivacy Regulation as *lex specialis* alongside the General Data Protection Regulation (GDPR). In view of the special protection of privacy afforded by the EU Charter of Fundamental Rights (CFR), communications data must enjoy a higher level of protection and, furthermore, can contain sensitive data within the meaning of Article 9 GDPR. For this reason – as under current legislation in the ePrivacy Directive – a high level of protection going beyond that afforded by the GDPR continues to be required.

2. In the Federal Government's view, the current version of the text does not afford the level of protection for the end-users and the confidentiality of communications which is required by the CFR. The level of protection contained in the GDPR must not be lowered by the ePrivacy Regulation, particularly with regard to communications data as particularly sensitive personal data. Germany is therefore unable to accept the text as it stands at present. Germany rather sees a need for a number of alterations to the text, not least in order to ensure the necessary protection of confidentiality of communications.

II. In detail:

1. General remark:

a) The digital society is reliant on reliable and protected communications. For an effective protection of end-users and confidentiality of communications in compliance with fundamental rights, the prerequisite is, that, in principle, communications data may not be processed without the consent of the affected end-user.

Exceptions from this principle are justified only if the processing is necessary in order to provide the communications service or in exceptional cases if coupled with effective measures to safeguard the rights of the end-user.

Germany believes that the current text from the Presidency fails to meet these standards:

2. The scope

a) Firstly, the ePrivacy Regulation must apply without any restriction to communications data, i.e.: communications data in the hands of the communications service providers should always be covered by the provisions of the ePrivacy Regulation. However, this is not adequately expressed in the scope of the Regulation, which only extends as far as to the receipt of the message. This is insufficient, given that in reality metadata and content are stored in the case of digital communications following the receipt of the message. For Germany, it is crucial that the protection of confidentiality remains comprehensively safeguarded once a communication has been completed but the provider continues to have access to the data, e.g. because metadata or content data remained stored at the provider. The ePrivacy Regulation should also apply to these situations. This is already reflected in Articles 6 and 7 regarding the permissions and obligations following the end of the communication; in the interest of a coherent approach, Articles 3 and 5 should be adapted accordingly (see relevant details there).

Thus, Germany is of the opinion that the approach of restricting the scope until the receipt of the message is insufficient.

Such an approach does not restrict the end-users: communications data in the hands of the end-users are already excluded by Article 5 from the special protection afforded by the ePrivacy Regulation, so that the end-user is not subject to the restrictions of the ePrivacy Regulation.

b) In addition, the protection of confidentiality of communications always covers all communications partners. In the case of the death of one communications partner, therefore, the protection of the communication must in principle continue to be ensured. At the same time, it must be ensured that heirs or other entitled persons are granted access to the content of the communication of the deceased end-user.

c) The Regulation should also not give rise to the impression that activities in the field of national security and defence fall within the scope of European law. Germany supports the Presidency's proposed amendment to Article 2(2)(a) and (aa). Recital 7a still needs to be adapted accordingly.

d) Germany is in favour of refraining from including in the recitals special explanations on machine-to-machine communication relating to the processing of communications data, since this distinction plays no role here and the comments therefore create misunderstandings. In this regard, the comments in Article 2 of Directive (EU) 2018/1972 and Recital 17 of the same Directive are sufficient.

3. Exceptions

Germany believes it should be ensured that existing regulatory objectives relating to the fight against online child pornography and terrorist content online, to the supply of electrical energy and to electronic communications between citizens and the justice system or the administration are not impaired by the ePrivacy Regulation. Exceptions from the scope of application should also apply to the ePrivacy Directive, which remains in force during the transitional period.

In detail:

aa) Fight against child pornography and terrorist content

With regard to the fight against the depiction of sexual exploitation and abuse of children and young people (and especially "child pornography") and with regard to the fight against terrorist and extremist content, Germany advocates a narrow statutory exemption in the ePrivacy Regulation which permits providers of interpersonal communications services to undertake technical measures and process communications data to this extent in order to detect and remove child pornography within the meaning of Directive 2011/92/EU and to report it to the competent authorities. At the same time, in order to provide justification and for reasons of proportionality, the provision should explicitly and in adequate exactness define the statutory requirements and provide for high levels of safeguards, in particular in the case of extremist content it is necessary to ensure that the provision is sufficiently precise. This includes restricting the processing of communications data to what is absolutely necessary for this purpose, corresponding restrictions on use, effective protection against abusive and unjustified use, technical and organisa-

tional safeguards, and prior consultation of the data protection authorities on the methodology.

bb) Supply with electrical energy, gas, water and heat

Germany makes reference to the recast Electricity Market Directive (Directive 2019/944), Directive 2009/73/EC (Gas Market Directive) and the amended Directive 2012/27/EU (Energy Efficiency Directive). In future, common rules for electricity generation, transmission, distribution and supply, energy storage and rules in the field of consumer protection will ensure the establishment of integrated, competition-oriented, consumer-oriented, fair and transparent electricity markets in the Union. This will entail a large number of devices being connected to a public communications network which enables energy suppliers to smartly meter and control the generation, storage and consumption of electrical energy. This activity should not be subjected to any further restrictions via the ePrivacy Regulation with regard to terminal equipment where it is necessary for compliance with a legal obligation deriving from the law of the Union or the Member States, or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in theentitled bodies . This also applies to supply with gas, water and heat.

cc) Electronic communications between citizens, the justice system and the administration

In view of the specificities of special national electronic communications services of public interest, particularly in the field of public authorities, courts and public institutions, Germany deems it necessary to exclude such special communication services from the scope of the ePrivacy Regulation, not least in order to be able to ensure a different, higher level of protection for these services. For this reason, Germany suggests an addition in Art. 2(2)(c) and Recital 13 with a view to a better understanding of the scope of the Regulation.

Proposal:

	Recital (xx) new **The supply with electrical energy, gas, water or heat is subject to spe-**

	cial requirements under the law of the Union and of the Member States which are intended to ensure both security of supply and benefits for the customers. In order to assume these tasks, a large number of devices must be able to communicate via the public communication network. Corresponding provisions are to be found in particular in Directive (EU) 2019/944 of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast), Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC and *[insert the recast of the Energy Efficiency Directive (EU) 2012/27/EU here]*. The activities necessary for this should not be subjected to any restrictions by this Regulation with regard to terminal equipment where it is necessary for compliance with a legal obligation deriving from the law of the Union or the Member States, or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in theentitled bodies .
	Recital (xx) new **In relation to the digitisation of public**

	activities of the state, institutions in the administration of justice, the judiciaryand public administration bodies will in future offer services which, depending on their specific design, may in individual cases be regarded as communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972 and thus be covered by Directive 2002/58/EC as of 21 December 2020. As a rule, such activities are already excluded from the scope of the current Directive and the future Regulation. For reasons of legal certainty, therefore, these state services should remain excluded from this Regulation if they are exceptionally to be regarded as communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972.

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, **regardless if these networks are secured with passwords or not,** the confidentiality of the communications transmitted through such networks should be protected. ~~**Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**~~ The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to ~~**publicly available**~~ electronic communications data using **publicly available** electronic communications services and public **electronic** communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as **home (~~WIFI or~~ fixed or wireless)**	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, **regardless if these networks are secured with passwords or not,** the confidentiality of the communications transmitted through such networks should be protected. ~~**Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**~~ The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to ~~**publicly available**~~ electronic communications data using **publicly available** electronic communications services and public **electronic** communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as **internal** corporate networks **of private busi-**

networks or corporate networks, access to which is limited **pre-defined group of end-users, e.g.** to **family members,** members of **~~the~~ a** corporation**, courts, court administrations, financial, social and employment administrations**. **~~Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation. This Regulation also does not apply to electronic communications data circulating within a home WIFI network. However, a~~As soon as ~~these~~ electronic communications data exit ~~such~~ a closed group network and enter a public~~ly available~~ electronic communications network, this Regulation applies to such data, including when it is M2M/IoT and personal/home assistant data. The provisions of this Regulation regarding the protection of end-users' terminal equipment information also apply in the~~is~~ case ~~to~~ of terminal equipment connected to ~~the~~ a closed group network such as a home (~~WIFI or~~ fixed or wireless) network which in turn is connected to public electronic communications network.	**nesses or administrative networks and services,** access to which is limited to **pre-defined categories ~~group~~** of **end-users, e.g.** to members of the ~~**corporation courts, court administrations, financial, social and employment administrations. Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**~~ company or the authority or groups of authorities such as for the public Safety Digital Radio. Furthermore this regulation should not apply to special electronic communications services and networks and directories that are publicly available and provided by or on behalf of public authorities, courts or public institutions for specific public purposes according to the law of the European Union or its Member States, e. g. to enable communication with courts, court administrations, judicial officers, administrations in general, financial administrations or social and employment administrations or to serve other purposes of administration of justice. These public sectors are immediately bound to the fundamental rights and freedoms such as protection of privacy and data protection. The respect for private life, confidentiality of electronic communications and the pro-

	tection of personal data can be especially regulated for public reasons. Rules for electronic communications as well as for the processing of data are duly determined by particular public or procedural law. The intention of this regulation is not to undermine these legal provisions. Therefore an exception in the scope of application is necessary to avoid any legal conflict.
	Recital (xx) new **Exceptions to the scope of this Regulation regarding** fight against online child pornography and terrorist content online, the supply of electrical energy and to electronic communications between citizens and the justice system or the administration **should, from the time of entry into force of this Regulation, also apply to Directive**

	2002/58/EC as long as this Directive remains in force until the end of the transition period following the entry into force of this Regulation.
	Article 2(2)(c): *Regarding Article 2(2)(c): Germany makes reference to the proposal already submitted by it in WK 14646/2017. Germany believes that a clarification is needed regarding the non-public communications services and networks, as is an explicit exemption for the area of special communication services in the field of the administration of justice and the administration.* **c)** electronic communications services **and networks** which are not publicly available; **special electronic communications services and networks and directories that are publicly available and provided by or on behalf of public authorities, courts or public institutions for specific public purposes according to the law of the European Union or its Member States. With regard to such special electronic communications services, networks and directories Member States shall ensure a level of protection that is at least equivalent to the provisions of this regulation.**

	Article 2(2) 2. This Regulation shall not apply to: (...) (da) **activities in the context of the supply of electricity, gas, water or heat with regard to terminal equipment where it is necessary for compliance with a legal obligation deriving from the law of the Union or the Member States, or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in theentitled bodies .**
Presidency's proposal: Article 6(1)(d)(1a): 1. Providers of electronic communications networks and services may shall be permitted to process electronic communications data only if: [(d) it is necessary to enable the detection and deletion of material constituting child pornography, as defined in Article 2(c) of the Directive 2011/93/EU. 1a. Processing for the detection and deletion of material constituting child pornography, in accordance with paragraph 1(d), shall not analyze the actual communications content and shall not store any copies of that content. Processing shall be subject to appropriate safeguards, be limited to the sole purpose of detecting child	**Revision in line with demand in Point II.3.aa**

pornography, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the end user, including carrying out of an impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and a consultation of the supervisory authority.]	
	Article 29(3) new **(…)** **3.Article 2(2) c.) and da.) shall be applied to Directive 2002/58/EC until the end of the transition period.**

III. Further proposals for amendments to the entire text:

Proposed texts according to document 11001/19 of 12 July 2019	**German comments and proposals**
(7a) This Regulation should not apply to the protection of fundamental rights and freedoms regarding activities concerning national security and defence.	**(7a) This Regulation does not apply to issues of protection of fundamental rights and freedoms related to activities which fall outside the scope of Union law, such as activities concerning national security and defence.**
(8) **…Some end-users, for example providers of payment services providers and or payment systems, process as recipi-**	*A reason to specifically cite individual service providers is not apparent, it must therefore be deleted.* *German proposal:* … **Some end-users, ~~for example providers of payment services providers and or payment systems,~~ process as**

ents their electronic communications data for different purposes or permit other request a third parties to process their electronic communications data on their behalf…	**recipients their electronic communications data for ~~different~~ specific purposes or ~~permit other~~ request a third part~~ies~~y to process their electronic communications data on their behalf. …**
(8a) This Regulation does not apply to the electronic communications data of deceased persons. Member States may provide for rules regarding the processing of electronic communications data of deceased persons.	**This Regulation does not apply to the electronic communications data of deceased persons. ~~Member States may provide for rules regarding the processing of electronic communications data of deceased persons.~~ Member States may also provide that in respect of communications of the deceased person with other end-users, the heir of the deceased end-user, or any legitimate person according to member states inheritance laws, may be treated like the deceased end-user for purposes of confidentiality of electronic communications with regard to electronic communications data.**
(12) ~~Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things).~~ **The use of machine-to-machine services, that is to say services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction, is emerging. While the services**	**Recital 12 is to be deleted. Germany refers to Article 2 of Directive (EU) 2018/1972 which defines "services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services" as electronic communication services as well as to Recital 17 of the same Directive**

provided at the application-layer of such services do normally not qualify as an electronic communications service as defined in the [Directive establishing the European Electronic Communications Code], ~~T~~**t**he transmission **services used for the provision** of machine-to-machine ~~communications~~ **services regularly** involves the conveyance of signals ~~over~~ **via** a**n electronic communications** network and, hence, ~~usually~~ ~~**normally**~~ constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation**, in particular the requirements relating to the confidentiality of communications,** should apply to the transmission of machine-to-machine **electronic** communications **where carried out via an electronic communications service**. ~~Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.~~ Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.	**saying "linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines, should not be considered to be (…) communications services." With the reference made in Article 4 1. b) of this Regulation to the definitions of Directive 2018/1972 no further clarification on machine-to-machine-services is needed.**

(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, **regardless if these networks are secured with passwords or not,** the confidentiality of the communications transmitted through such networks should be protected. ~~**Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**~~ The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to ~~**publicly available**~~ electronic communications data using **publicly available** electronic communications services and public **electronic** communications networks. In contrast, this Regulation should not	(13) The development of fast and efficient wireless technologies has fostered the increasing availability for the public of internet access via wireless networks accessible by anyone in public and semi-private spaces such as 'hotspots' situated at different places within a city, department stores, shopping malls and hospitals. To the extent that those communications networks are provided to an undefined group of end-users, **regardless if these networks are secured with passwords or not,** the confidentiality of the communications transmitted through such networks should be protected. ~~**Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**~~ The fact that wireless electronic communications services may be ancillary to other services should not stand in the way of ensuring the protection of confidentiality of communications data and application of this Regulation. Therefore, this Regulation should apply to ~~**publicly available**~~ electronic communications data using **publicly available** electronic communications services and public **electronic** communications networks.

apply to closed groups of end-users such as **home (~~WIFI or~~ fixed or wireless) networks or** corporate networks, access to which is limited **pre-defined group of end-users, e.g.** to **family members,** members of **~~the~~ a** corporation**, courts, court administrations, financial, social and employment administrations**. **~~Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation. This Regulation also does not apply to electronic communications data circulating within a home WIFI network. However, a~~As soon as ~~these~~ electronic communications data exit ~~such~~ a closed group network and enter a public~~ly available~~ electronic communications network, this Regulation applies to such data, including when it is M2M/IoT and personal/home assistant data. The provisions of this Regulation regarding the protection of end-users' terminal equipment information also apply in the~~is~~ case ~~to~~ of terminal equipment connected to ~~the~~ a closed group network such as a home (~~WIFI or~~ fixed or wireless) network which in turn is connected to public electronic communications network.**	In contrast, this Regulation should not apply to closed groups of end-users such as **internal** corporate networks **of private businesses or administrative networks and services,** access to which is limited to **predefined categories ~~group~~** of **end-users, e.g.** to members of the **~~corporation courts, court administrations, financial, social and employment administrations~~**. **Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this ~~Regulation.~~ company or the authority or groups of authorities such as for the public Safety Digital Radio. Furthermore this regulation should not apply to special electronic communications services and networks and directories that are publicly available and provided by or on behalf of public authorities, courts or public institutions for specific public purposes according to the law of the European Union or its Member States, e. g. to enable communication with courts, court administrations, judicial officers, administrations in general, financial administrations or social and employment administrations or to serve other purposes of administra-**

	tion of justice. These public sectors are immediately bound to the fundamental rights and freedoms such as protection of privacy and data protection. The respect for private life, confidentiality of electronic communications and the protection of personal data can be especially regulated for public reasons. Rules for electronic communications as well as for the processing of data are duly determined by particular public or procedural law. The intention of this regulation is not to undermine these legal provisions. Therefore an exception in the scope of application is necessary to avoid any legal conflict.
	The protection of confidentiality of communications must be comprehensively ensured. In view of the existing possibilities to store communications data, the scope of the ePrivacy Regulation should extend to all communications data in the hands of communication service providers at every stage and thus also beyond the process of transmitting the data. Recital

(15) Electronic communications data should be treated as confidential. This means that any **interference** ~~with the transmission~~ **processing** of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of ~~**all**~~ the communicating parties should be prohibited. ~~**The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee**~~. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing	*15 must therefore be supplemented as follows:* (15) Electronic communications data should be treated as confidential. This means that any **interference** ~~with the transmission~~ **processing** of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of ~~**all**~~ the communicating parties should be prohibited. **The confidentiality of electronic communication and prohibition of interception of communications data should apply during conveyance and after their receipt.** ~~**The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee**~~. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the

habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.	technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.
(15aa) In order to ensure the confidentiality of electronic communications data, providers of electronic communications services should apply security measures in accordance with Article [40] of the [Directive establishing the European Electronic Communications Code] and Article 32 of Regulation (EU) 2016/679. Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.	**(15aa) In order to ensure the confidentiality of electronic communications data, providers of publicly avalable electronic communications services and networks should apply security measures in accordance with Article [40] of the [Directive establishing the European Electronic Communications Code] and Article 32 of Regulation (EU) 2016/679. Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.**
(15a) The prohibition of interception of electronic communications ~~data~~ content under this Regulation should apply until receipt of the content of the electronic	**"(15a) Any provider of publicly available electronic communications networks and services shall be obliged to maintain the confidentiali-ty of electronic communications, as**

communication by the intended addressee, i.e. during the end-to-end exchange of electronic communications content between end-users. Receipt implies that the end-user gains control over, and has the possiblity to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data. The exact moment of the receipt of electronic communications content may depend on the type of electronic communications service that is provided. For instance, depending on the technology used, a voice call may be completed as soon as either of the end-users ends the call. For electronic mail or instant messaging, depending on the technology used, the moment of receipt ~~is~~ may be ~~completed~~ as soon as the addressee has collected the message, typically from the server of the electronic communications service provider. Upon receipt, electronic communications content and related metadata should be erased or made anonymous by the provider of the electronic	**long as the provider is storing, handling or in any other way processing communications data. The obligation to maintain the confidentiality shall apply after the end of the activity of the provider of public electronic communication networks and services. Electronic communications content and related metadata should be erased or made anonymous by the provider of the electronic communications service except when processing is permitted under this Regulation or when the end-users has entrusted the provider of the electronic communications service or another third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.**

communications service except when processing is permitted under this Regulation or when the end-users has entrusted the provider of the electronic communications service or another third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.	
Article 2(2) 2. This Regulation shall not apply to: (...)	Article 2(2) 2. This Regulation shall not apply to: (...) (…) **the processing of electronic communications data by providers of an electronic communications service and electronic communications networks to the extent it is necessary for activities pursuant to point a, b, d.**
(c) electronic communications services which are not publicly available;	(c) electronic communications services **and networks** which are not publicly available; **special electronic communications services and networks and directories that are publicly available and provided by or on behalf of public authorities, courts or public institutions for specific public purposes according to the law of the European Union or its Member States. With regard to such special electronic communications services, networks and directories Member States shall ensure a level of protection that is at least equivalent to the provisions of this regulation.**

(e) electronic communications content processed by the end-users concerned after receipt, or by a third party entrusted by them to record, store or otherwise process ~~such data~~ their electronic communications content;	*The proposed addition to Article 2(2)(e) is unnecessary with regard to the end-users, since Article 5 has already excluded the end-users from the principle of confidentiality. To the extent that third parties store the content of communications (e.g. photos, texts and message content, etc.) on behalf the end-user, the general rules apply in any case and should only apply in this regard.* **(e) electronic communications content processed ~~by the end-users concerned after receipt, or~~ by a third party entrusted by the end-users to record, store or otherwise process such data their electronic communications content;** *Regarding Article 2(2)(f):* *Metadata which in contrast make reference to communications should always remain covered by the scope of the Regulation. The proposed addition to Article 2(2)(f) should therefore be deleted. Consent to storage can be granted by the end-user on the basis of this Regulation. If the provider stores the metadata, or third parties store it for the use of the end-user, there is, pursuant to Article 6(3)(aa), no requirement for the other end-users affected to give their consent.*

(f) electronic communications metadata processed by the end-users concerned or by a third party entrusted by them to record, store or otherwise process their electronic communications metadata ~~on their behalf~~.	**~~(f) electronic communications metadata processed by the end-users concerned or by a third party entrusted by them to record, store or otherwise process their electronic communications metadata on their behalf.~~**
Article 3 (…) **(cb) the offering of publicly available directories of end-users of electronic communications services who are in the Union;**	Article 3: Regarding Article 3(1)(cb): With regard to the exception for certain fields in Article 2(2)(ca) and (cb), it should be clarified here that Article 3(1)(cb) is restricted to the directory services which include electronic communications services in the scope of the Regulation: **(cb) the offering of publicly available directories of end-users of electronic communications services <u>covered by this Regulation</u> who are in the Union**
5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against ~~a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union~~ **the provider or person it represents**.	**5. The representative shall have the power, in addition to or instead of the provider it represents, to answer questions and requests of competent authorities referred to in Article 2 paragraph 2 point d that are authorized by Union or Member state law.**
Article 5 Confidentiality of electronic com-	Article 5 Confidentiality of electronic

munications data Electronic communications data shall be confidential. Any **interference with ~~processing of~~** electronic communications data, ~~such as by~~ **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, **~~or~~** surveillance **~~or~~ and processing** of electronic communications data, by **~~persons~~ anyone**other than the end-users **concerned**, shall be prohibited, except when permitted by this Regulation.	communications data **(1) Electronic communications and e**lectronic communications data shall be confidential. Any interference with **~~processing of~~** electronic **communications or** electronic communications data, ~~such as by~~ **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, **~~or~~** surveillance **~~or~~ or processing** of electronic communications data, by **~~persons~~ anyone**other than the end-users **concerned**, shall be prohibited, except when permitted by this Regulation **or by provisions of Member States permitted by this regulation.** **(2) Without prejudice to paragraph 1, any provider of electronic communications networks and services shall be obliged to maintain the confidentiality of electronic communications. The obligation to maintain the confidentiality shall apply after the end of the activity of the provider of electronic communication networks and services.** **(3) Member States heritage laws remain unaffected. In the case of the decease of the end-user the heir or any legitimate person according to member states heritage laws shall be treated like the deceased end-user for purposes of confidentiality of electronic communications with regard to electronic communications**

	data.
Recital 19 (19) (…)This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. (….)	*Deletion of "in transit", as coherent and technology-neutral protection is necessary for the ePrivacy Regulation (see above and addition to Article 5):* (19) This Regulation provides for the possibility of providers of electronic communications services to process electronic communications **~~data in transit,~~** with the informed consent of all the end-users concerned (…)

2. Article 6 - Permitted processing of communications data

Germany rejects the current version of Article 6 - particularly with regard to the processing of location data and the concept of "compatible further processing". Germany points out that the ePrivacy Regulation is intended to safeguard the confidentiality of communications. Communications data are processed by communication service providers when they deliver communications services. The processing in order to deliver a certain communications service agreed with the user is technically necessary in order to facilitate the right of the end-user to communicate.

Germany believes the processing of communications data for other purposes without the consent of the end-user must only be permissible within narrow limits. This is particularly true of the use of communications data for the provider's own commercial purposes. For the purpose of statistical counting, the processing of metadata should however be permitted under certain preconditions. Germany believes that the approach proposed by the Bulgarian Presidency on 4 May 2018 (Council document No 8537/18) offers a good basis for further negotiations. This proposal, restricted to statistical counting, offers the benefit of clear rules and thus legal certainty for the providers.

Germany can accept the following wording of Article 6 and the Recitals referring to this article:

(16)	*Spam controls are covered by the proposal*

	on Article 6(3)(a); for this reason, the wording is inappropriate at this point; whether spam controls are desired should be decided by the end-user as the recipient; therefore deletion as follows:
(…) **Spam ~~e-mails~~ electronic messages may also affect the availability of ~~email~~ the respective services and could potentially impact the performance of networks and ~~email~~ services, which justifies the processing of electronic communications data to mitigate this risk. Such security measures, including anti-spam measures, should be proportionate and should be performed in the least intrusive manner. Providers of electronic communications services are encouraged to offer end-users the possibility to check ~~e-mails~~ electronic messages deemed as spam in order to ascertain whether they were indeed spam.**	~~**Spam e-mails electronic messages may also affect the availability of email the respective services and could potentially impact the performance of networks and email services, which justifies the processing of electronic communications data to mitigate this risk. Such security measures, including anti-spam measures, should be proportionate and should be performed in the least intrusive manner.**~~ **Providers of electronic communications services are encouraged to offer end-users the possibility to check e-mails electronic messages deemed as spam in order to ascertain whether they were indeed spam.**
(….)The processing of ~~**meta**~~data to make it anonymous ~~**nor the processing of metadata to make it anonymous**~~ **should not be prohibited either**.	*Recital 16 needs to be further clarified regarding the point of anonymisation **("tT**he processing of ~~**meta**~~data to make it anonymous ~~**nor the processing of metadata to make it anonymous**~~ **should not be prohibited either**."):* *There is still considerable lack of clarity about the anonymisation. Problem of coordination with permissions in Articles 6 and 8, since*

	these dispositions in parts also include anonymisation as an additional criterion; the new wording still leaves unclear to what extent the collection of data for subsequent anonymisation is meant to be permissible, or whether this is meant to be admissible as a comprehensive "anonymisation concept.
(17aa) Metadata such as location data can provide valuable information, such as insights in human movement patterns and traffic patterns. Such information may, for example, be used for urban planning purposes. Further ~~P~~processing for such purposes other than for which the metadata where initially collected may take place without the consent of the end-users concerned, provided that such processing is compatible with the	Germany **cannot support this recital**. Germany wishes to underline that the end-user has no alternative to electronic communications metadata processed by electronic communications services and networks. Therefore allowing Service Providers to process without consent communications data for other purposes than those necessary is highly problematic. Germany can – reluctantly - support processing of location data for statistical counting as far enough, as foreseen in the Presidency text from May 4th 2018 (Doc. 8537/18) and on the basis of the respective recital 17aa of Doc. 8537/18 suggests the following text: **"(17aa) Metadata that is location data can <u>constitute sensitive</u> ~~provide valuable~~ information, such as insights in human movement patterns and traffic patterns. ~~Such information may, for example, be used for urban planning purposes.~~ Processing <u>of such location data</u> for purposes of statistical counting may take place without the consent of the end-users concerned, provided that certain conditions are met and safeguards are in place, in-**

purpose for which the metadata are initially collected, certain additional conditions are met and safeguards are in place, including ~~the consultation of the supervisory authority~~ an impact assessment by the provider of electronic communications networks and services and the requirement to anonymise the result before sharing the analysis with third parties. As end-users attach great value to the confidentiality of their communications, including their physical movements, such data cannot be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about these processing activities taking place and given the right to object to such processing.	cluding the consultation of the supervisory authority and the requirement to anonymise the result before sharing the ~~analysis~~ statistical data with third parties. Such statistical data may, for example, be used for urban planning purposes. As end-users attach great value to the confidentiality of their communications, including their physical movements, ~~such~~ the location data ~~cannot~~ must not be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about processing activities taking place for statistical counting and given the right to object to such processing.
(17b) Processing of electronic communication metadata for scientific research or statistical counting purposes should be considered to be permitted processing. This type of processing should be subject to safeguards to ensure privacy of the end-users by employing appropriate security measures such as encryption	(17b) Processing of electronic communication metadata for scientific research based on Union or Member State law or statistical counting purposes should be considered to be permitted processing. This type of processing should be subject to safeguards to ensure privacy of the end-users by employing appropriate security measures such as

and pseudonymisation. In addition, end-users who are natural persons should be given the right to object.	**encryption and pseudonymisation. In addition, end-users who are natural persons should be given the right to object.**

Article 6 *Permitted processing of electronic communications data*	*Article 6* *Permitted processing of electronic communications data*
(…)	(…)
[(d) it is necessary to enable the detection and deletion of material constituting child pornography, as defined in Article 2(c) of the Directive 2011/93/EU.	Revision in line with demand made in point II.3.aa
1a. Processing for the detection and deletion of material constituting child pornography, in accordance with paragraph 1(d), shall not analyze the actual communications content and shall not store any copies of that content. Processing shall be subject to appropriate safeguards, be limited to the sole purpose of detecting child pornography, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the end user, including carrying out of an impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and a consultation of the supervisory authority.]	
(…)	**(…)**
2. **Without prejudice to paragraph 1,** P**p**roviders of electronic communications	2. **Without prejudice to paragraph 1,** P**p**roviders of electronic communications

networks and services ~~may~~ **shall be permitted to** process electronic communications metadata **only** if:	**networks and** services ~~may~~ **shall be permitted to** process electronic communications metadata **only** if:
(a) it is necessary **for the purposes of network management or network optimisation, and for the duration necessary for that purpose, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous ~~and for the duration necessary for that purpose~~,** or to meet ~~**mandatory**~~ **technical** quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120**9** for the duration necessary for that purpose; or	(a) **it is to the extent strictly necessary and proportionate for the purpose of preventing any act against or ensuring the general availability of electronic communications networks and services for the duration neces-sary for that purpose, provided that the purpose could not be fulfilled by processing information that is made anonymous**
	Germany is in favour of re-instating the previous approach to Article 6(2)(e), as this offers the necessary legal certainty to the providers and also offers sufficiently clear preconditions for the restrictions on the fundamental rights of the affected end-users:
~~(e) it is necessary for the purpose of statistical counting, provided that:~~ **~~- the processing is limited to electronic communications meta-data that constitutes geolocation data that is pseudonymised,~~** **~~- the processing could not be carried out by processing information that is~~**	**(e) it is necessary for the purpose of statistical counting, provided that:** **- the processing is limited to electronic communications meta-data that constitutes geolocation data that is pseudonymised,** **- the processing could not be carried out by processing information that is**

~~made anonymous, and the location data is erased or made anonymous when it is no longer needed to fulfil the purpose, and~~ ~~- the location data is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.~~	**made anonymous, and the location data is erased or made anonymous when it is no longer needed to fulfil the purpose, and** **- the location data is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.**
	Regarding Article 6(2)(f): Germany is also in favour of retaining Article 6(2)(f) alongside Article 6 (2)(e) and proposes the following wording (in line with the wording in WK 8537/18):
(f) it is necessary for statistical ~~counting~~purposes, ~~other than based on electronic communications metadata that constitute location data,~~ or for scientific research purposes, provided it is based on Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures, including encryption and pseudonymisation, to safeguard fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.	**(f) it is necessary for scientific research or statistical counting not permitted in accordance with point (e) or for scientific research, provided it is based on Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures, including encryption and pseudonymisation, to safeguard fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.**

	Complete deletion of paragraph 2a:
2a. Where the processing for a purpose other than that for which the electronic communications metadata have been collected under paragraphs 1 and 2 is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 , the provider shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia: **(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;** **(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;** **(c) the nature of the electronic communications metadata, in particular where such data could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;** **(d) the possible consequences of the intended further processing for end-**	~~**2a. Where the processing for a purpose other than that for which the electronic communications metadata have been collected under paragraphs 1 and 2 is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 , the provider shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:**~~ ~~**(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;**~~ ~~**(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;**~~ ~~**(c) the nature of the electronic communications metadata, in particular where such data could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;**~~ ~~**(d) the possible consequences of the intended further processing for end-**~~

users; **(e) the existence of appropriate safe-guards.** **Such processing, if considered compatible, may only take place, provided that:** **- the processing could not be carried out by processing information that is made anonymous, and electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, and** **- the processing is limited to electronic communications metadata that is pseudonymised,** **- the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.**	**~~users;~~** **~~(e) the existence of appropriate safe-guards.~~** **~~Such processing, if considered compatible, may only take place, provided that:~~** **~~- the processing could not be carried out by processing information that is made anonymous, and electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, and~~** **~~- the processing is limited to electronic communications metadata that is pseudonymised,~~** **~~- the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.~~**
	Complete deletion of paragraph 2aa (derives from deletion of paragraph 2a):
~~3a~~2aa. For the purposes of ~~point (e) of~~ paragraph 2a, the providers of electronic communications networks and services shall: **~~(a) exclude electronic communications metadata that constitue location data that reveal special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;~~** **(b) not share such data with third**	**~~3a2aa. For the purposes of point (e) of paragraph 2a, the providers of electronic communications networks and services shall:~~** **~~(a) exclude electronic communications metadata that constitue location data that reveal special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;~~** **~~(b) not share such data with third~~**

parties, unless it is made anonymous; **(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior ~~and~~ consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679. ~~Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority~~; and** **(d) inform the end-user of specific processing on the basis of ~~point (e) of~~ paragraph 2a and ~~give~~ of the right to object to such processing free of charge, at any time, and in an easy and effective manner. If the end-user objects, the electronic communications metadata shall no longer be processed for such purposes.**	~~**parties, unless it is made anonymous;**~~ ~~**(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior and consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority; and**~~ ~~**(d) inform the end-user of specific processing on the basis of point (e) of paragraph 2a and give of the right to object to such processing free of charge, at any time, and in an easy and effective manner. If the end-user objects, the electronic communications metadata shall no longer be processed for such purposes.**~~
(…)	**(… - paragraph 3 shall remain in the text)**
~~**3a. For the purposes of point (e) of paragraph 2, the providers of the electronic communications networks and services shall:**~~ ~~**(a) exclude electronic communications metadata that constitue geolocation data that reveal special categories of**~~	**3a. For the purposes of point (e) of paragraph 2, the provider of the electronic communications service shall:** **(a) exclude electronic communications metadata that constitute geolocation data that reveal special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;**

~~personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;~~ ~~(b) not share such data with third parties, unless it is made anonymous;~~ ~~(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority; and~~ ~~(d) inform the end-user of specific processing on the basis of point (e) of paragraph 2 and give the right to object to such processing.~~ **(…)**	**(b) not share such data with other third parties, unless it is made anonymous;** **(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority; and** **(d) inform the end-user of specific processing on the basis of point (f) of paragraph 2 and give the right to object to such processing.** (…)

3. Retention of data

Germany rejects the proposed additions in Article 11 and Recital 26. Article 11 allows Member States to regulate the retention of data at national level in line with the preconditions set by the ECJ. There is no need for the ePrivacy Regulation to address this issue specifically, since no further provisions are enclosed about this in the Regulation. The requirements set out by the ECJ should not be narrowed further by the ePrivacy Regulation.

(26) When the processing of electronic	(26) When the processing of electronic

communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights**, including by way of derogations,** when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including ~~**national security, defence,**~~ public security and the prevention, investigation, detection or prosecution of criminal offences**, including dissemination of child pornography,** or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic	communications data by providers of electronic communications services falls within its scope, this Regulation should provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights**, including by way of derogations,** when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including ~~**national security, defence,**~~ public security and the prevention, investigation, detection or prosecution of criminal offences**, ~~including dissemination of child pornography,~~** or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. Therefore, this Regulation should not affect the ability of Member States to carry out lawful interception of electronic

communications or take other measures, **such as measures providing for the retention of data for a limited period of time,** if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).	communications or take other measures, ~~**such as measures providing for the retention of data for a limited period of time,**~~ if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights. Providers of electronic communications services should provide for appropriate procedures to facilitate legitimate requests of competent authorities, where relevant also taking into account the role of the representative designated pursuant to Article 3(3).
Article 11 *Restrictions* 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate	*Article 11* *Restrictions* 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate

measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)~~(a)~~ **(c)** to (e)**, (i) and (j)** of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. **To that end and under the same conditions, Union or Member State law may, inter alia, impose an obligation on the providers of electronic communication services to retain electronic communications data to safeguard one or more of the general public interests referred to in this paragraph, for a limited period of time longer than the one provided for in Article 7.**	measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)~~(a)~~ **(c)** to (e)**, (i) and (j)** of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. ~~**To that end and under the same conditions, Union or Member State law may, inter alia, impose an obligation on the providers of electronic communication services to retain electronic communications data to safeguard one or more of the general public interests referred to in this paragraph, for a limited period of time longer than the one provided for in Article 7.**~~

4. Article 8 – Protection of terminal equipment

Germany regards the protection of terminal equipment in Article 8 as essential in order to achieve effective protection of privacy. Protection of privacy and electronic communications precisely does also encompass the protection of terminal equipment. Germany approves of the general direction taken by Article 8. Article 8 uses the existing definition of terminal equipment and end-users, which is far-reaching and adequate.

Germany opposes the substitution of the term "information society service" by "service" in Article 8 and the related recitals. The term "service" is firstly non-specific and non-defined. Secondly, as the European Commission has stated in its comments, this extension of the scope is not necessary in order to include IoT

services, which are as an general rule an "information society service". The information society services can also include software updates, where these are requested by the end-user. There should be no misleading statements in the recitals about this.

Germany proposes the following changes:

(20a) **End-users are ~~increasingly~~ often requested to provide consent to the storage (…)**	**Delete this recital: it leads to unnessary misunderstandings; necessary consent according to Article 8 needs no further explanation. Germany wishes to further discuss white-listing via privacy settings in communication software and refers to the proposal Germany made to Article 10.**
(21) **~~Exceptions to the obligation to obtain consent to make u~~U**se of the processing and storage capabilities of terminal equipment or **to** access **to** information stored in terminal equipment **without the consent of the end-user** should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is ~~strictly~~ necessary and proportionate for the ~~legitimate~~ purpose of ~~enabling the use of~~ **providing** a specific ~~**information society**~~ service**, such as those used by IoT devices (for instance connected devices like connected thermostats),** ~~explicitly~~ requested by the end-user. This may include the storing of cookies for the duration of a single estab-	(21) **~~Exceptions to the obligation to obtain consent to make u~~U**se of the processing and storage capabilities of terminal equipment or **to** access **to** information stored in terminal equipment **without the consent of the end-user** should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is ~~strictly~~ **strictly** necessary and proportionate for the ~~legitimate~~ purpose ~~of enabling the use of~~ **providing** a specific of a specific ~~**information society**~~ **information society** service, **~~such as those used by IoT devices (for instance connected devices like connected thermostats),~~** ~~explicitly~~ requested by the end-user. This may

lished session on a website to keep track of the end-user's input when filling in online forms over several pages**, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket**. ~~**Access to specific website content may still be made conditional on the well-informed acceptance of the storage of a cookie or similar identifier, if it is used for a legitimate purpose. This will for example not be the case of a cookie which is recreated after the deletion by the end-user. Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.**~~ **In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-**	include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages**, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket**. ~~**Access to specific website content may still be made conditional on the well-informed acceptance of the storage of a cookie or similar identifier, if it is used for a legitimate purpose. This will for example not be the case of a cookie which is recreated after the deletion by the end-user. Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.**~~ **In some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed**

user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and [has accepted such use].	**by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use.**
~~Conversely, t~~To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the ~~information society~~ service requested, consent should be required. ~~Where the terminal equipment is provided to the end-user by the provider of the information society service~~, In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service. ~~Where that end-user enables the use of the terminal equipment by other end-users, such as employees, it should respect the rights of those other end-users in accordance with Regulation (EU) 2016/679, employment and other applicable laws.~~	**~~Conversely, t~~To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the ~~information society~~ information society service requested, consent should be required. ~~Where the terminal equipment is provided to the end-user by the provider of the information society service~~, In such a scenario, consent should normally be given by the end-user who requests the information society service from the provider of the service. ~~Where that end-user enables the use of the terminal equipment by other end-users, such as employees, it should respect the rights of those other end-users in accordance with Regulation (EU) 2016/679, employment and other applicable laws.~~**
~~In some cases the use of processing and storage capabilities of terminal~~	**~~In some cases the use of processing and storage capabilities of terminal~~**

~~**equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use.**~~	~~**equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use.**~~
(21a) Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measure**i**ng web traffic to **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site, which always require the consent of the end-user**. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.	**(21a)**Cookies can also be a ~~legitimate and~~ useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measure~~ing web traffic to~~ **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site, which always require the consent of the end-user**. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception. ~~Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.~~	**~~Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception. Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of the information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.~~**
(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be	(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices

identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI**, the WiFi signal** etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer **physical movements'** tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, **such as** providing data on the number of people waiting in line, ascertaining the number of people in a specific area, ~~etc~~ **referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level if security appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is not longer needed for this purpose**. **Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area**	must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI**, the WiFi signal** etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer **physical movements'** tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, **such as** providing data on the number of people waiting in line, ascertaining the number of people in a specific area, ~~etc~~ **referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level if security**

that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.-This information may be used for more intrusive purposes, **which should not be considered statistical counting,** such as to send commercial messages to end-users, for example when they enter stores, with personalized offers locations**, subject to the conditions laid down in this Regulation,** ~~. While some of these functionalities do not entail high privacy risks, others do, for example, those involving~~ **as well as** the tracking of individuals over time, including repeated visits to specified locations. ~~Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to~~	**appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is not longer needed for this purpose**. **Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.**-This information may **only** be used for more intrusive purposes, **which should not be considered statistical counting,** such as to send commercial messages to end-users, for example when they enter stores, with personalized offers locations**, ~~subject to the conditions laid down in this Regulation,~~** ~~. While some of these functionalities do not entail high privacy risks, others do, for~~

~~Article 13 of Regulation (EU) 2016/679.~~	~~example, those involving~~ **as well as** the tracking of individuals over time, including repeated visits to specified locations **if permitted by this Regulation**. ~~Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.~~
Article 8	*Article 8*
Protection of ***end-users' terminal equipment*** *information* ***~~stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment~~***	*Protection of* ***end-users' terminal equipment*** *information* ***~~stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment~~***
1. 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,	1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited,

except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for ~~providing an information society~~ service requested by the end-user; or (…)	except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an **information society** service requested by the end-user or (…) **Germany is in favour of retaining the end of Recital 21 "In some cases…has accepted such use.". If it is deleted, Germany comes back to its demand for Article 8:** **"The provision of information society services, that are wholly or partly financed by advertising, may be made conditional upon the consent to the storage and collection of information for advertising purposes, as far as the end-user is informed accordingly."**

5. Article 10 - Software settings to protect privacy

Germany is in favour of retaining Article 10. We need statutory rules in the EU which ensure that the protection of privacy is not undermined by browser software. For this reason, browsers must include settings to protect privacy, inform the users about this and offer the possibility to select these settings.

At the same time, the requirements must be made user-friendly and pro-competitive. Germany is in favour of standards being established for this.

Germany is sticking to its proposal for Article 10 and also calls for the retention of Recitals 22-24.

~~(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties.~~	**(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible.** ~~Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment.~~ **As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent as defined by Regulation 2016/679/EU by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties.**
~~(22a)Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between~~	**(22a)Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and**

~~the end-user and the website. From this perspective, they are in a privileged the position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored. The responsibility for obtaining consent with the storage of a cookie and for any penalties for breach of duty lies on the information society service provider.~~	**the website. From this perspective, they are in a privileged the position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored. The responsibility for obtaining consent with the storage of a cookie and for any penalties for breach of duty lies on the information society service provider.**
~~(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept~~	**(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. ~~Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'.~~ Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent ~~third parties~~ any other parties than the end-user from storing information on the terminal equipment. ~~; this is often presented as 'reject third party cookies'.~~ Furthermore, ~~E~~end-users should be offered a set of privacy setting op-**

~~allow cookies') to lower (for example, 'always accept allow cookies') and intermediate (for example, 'reject third party cookies' or 'only accept allow first party cookies'). Such privacy settings should be presented offered in a an easily visible and intelligible manner. General privacy settings that do not provide the end-user with information about the purpose for which information can be stored on the terminal equipment, or information already stored on that equipment can be processed, as a consequence of the configured privacy settings, cannot signify the end-user's consent to the storing of information on the terminal equipment or the processing of information already stored on that equipment.~~	tions, ranging from higher ~~(for example, 'never accept allow cookies')~~ to lower ~~(for example, 'always accept allow cookies')~~ and intermediate (for example, 'reject third party cookies' or 'only accept allow first party cookies') allowing for a range of choices to control the flow of information to and from the terminal equipment.. Such privacy settings should be presented offered in a an easily visible and intelligible manner. ~~General privacy settings that do not provide the end-user with information about the purpose for which information can be stored on the terminal equipment, or information already stored on that equipment can be processed, as a consequence of the configured privacy settings, cannot signify the end-user's consent to the storing of information on the terminal equipment or the processing of information already stored on that equipment.~~
~~(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and~~	~~(24) For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to~~

~~from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it It is necessary to require providers of software enabling access to internet that, at the moment of installation or first use and at the moment of every update that change the privacy settings, end-users are informed about the possibility to choose the available privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the default setting and about the risks associated with the different privacy settings, including those related to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Updates of software enabling access to internet should not alter the privacy settings selected by the end-user. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use~~	**~~the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it~~ It is necessary to require providers of software enabling access to internet ~~that,~~ at the moment of installation or first use ~~and at the moment of every update, that change the privacy settings, end-users are informed about the possibility to choose the~~ available privacy settings ~~among the various options and ask them to make a choice~~. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the default setting and about the risks associated with the different privacy settings, including those related to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Updates of software**

~~and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed. This Regulation does should not prevent website providers from requesting the consent of the end-user for the use of cookies irrespective of the privacy setting selected by the end-user.~~	**enabling access to internet should not alter the privacy settings selected by the end-user. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed. This Regulation does should not prevent website providers from requesting the consent of the end-user for the use of cookies irrespective of the privacy setting selected by the end-user.**

~~*Article 10*~~ ~~*Information and options for privacy settings to be provided*~~	**Article 10** **Information and options for privacy settings to be provided**
~~1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.~~	**1. Software permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent any other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.**
~~2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.~~	**2. Once, at the time of first installation or first usage, the software referred to in paragraph 1 shall inform the end-user about the privacy settings options and require the end-user to consent to a setting.**
	2a. The software referred to in paragraph 1 shall provide in a clear manner for easy ways for end-users to change the privacy setting consented to under paragraph 2 at any time during the use.
	2b. In case the software referred to in paragraph 1 prevents any parties other than the end-user from storing information on his terminal equipment or processing information already stored on that equipment, these parties may request the end-user to give the con-

	sent referred to in Article 8 (1) (b), which may change settings accordingly. **3. The Commission shall be empowered to adopt delegated acts after consultation of the European Data Protection Board and in accordance with Article 25 determining standards which permit compliance with the requirements of this Article.**
~~3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.~~	**4. In the case of software which has already been installed on (XX.XX.XXXX) the requirements in this Article shall be complied with at the time of the first update of the software, but no later than (XX.XX.XXXX).**

6. Chapter III:

	As a backbone of democracy political parties should continue to be allowed to directly contact citizens to inform about their positions. Including political parties would furthermore extend the scope of Article 16 which refers to "marketing". "Marketing" means activities to promote own or third parties products and services. This contains the commercial collecting of donations for a party or organization. However, there is no "marketing" by political parties or non-profit organisations when promoting their positions because they act (political) ideally. The changes made by the

	presidencies are going in the right direction, however Germany refers to its previous proposal for further differentiating between fundraising and promoting political positions: *Germany furthermore understands that „direct marketing communications" does not contain making contacts for purposes of scientific research in public interest.* *Recital 32 should therefore read as follows:*
(32) (…) In addition to **direct communications advertising for** the offering of products and services for commercial purposes, **Member States may decide that** ~~this should~~ **direct marketing communications ~~also~~ may** include ~~messages~~ **direct communications** sent by political parties that contact natural persons via **publicly available** electronic communications services in order to promote their parties. The same ~~should~~ apply**ies** to messages sent by other non-profit organisations to support the purposes of the organisation.	(32) (...) In addition to ~~**direct communication advertising for**~~ the offering of products and services for commercial purposes, ~~**Member States may decide that**~~ direct marketing communications **also ~~may~~** include **messages ~~direct communications~~** sent by political parties that contact natural persons via ~~**publicly available**~~ electronic communications services in order to ~~**promote**~~ **collect funds for** their parties. The same applies to messages sent by other non-profit organisations **to that purpose** to support the purposes of the organisation. ~~in order to promote their parties. The same should apply**ies** to messages sent by other non-profit organisations to support the purposes of the organisation.~~
(35) ~~In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address,~~	(35) ~~In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by email should present a link, or a valid electronic mail address,~~

~~which can be easily used by end-users to withdraw their consent.~~ Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should ~~display~~ **present** their identity line on which the company can be called**. Member States are encouraged to introduce by means of national law** ~~or present~~ a specific code **or prefix** identifying the fact that the call is a **direct** marketing call **to improve the tools provided for the end-users in order to protect their privacy in more efficient manner**. **Using a specific code or prefix should not relieve the legal or natural persons sending ~~or presenting~~ direct marketing call from the obligation to present their calling line identification.**	~~which can be easily used by end-users to withdraw their consent.~~ Legal or natural persons conducting direct marketing communications through voice-to-voice calls and through calls by automating calling and communication systems should ~~display~~ **present** their identity line on which the company can be called**. Member States are encouraged to introduce by means of national law <u>the requirement for calls addressing end-users in their territory to present</u>** ~~or present~~ a specific code **or prefix** identifying the fact that the call is a **direct** marketing call **to improve the tools provided for the end-users in order to protect their privacy in more efficient manner**. **Using a specific code or prefix should not relieve the legal or natural persons sending ~~or presenting~~ direct marketing call from the obligation to present their calling line identification**
Article 16 ***Unsolicited and ~~D~~direct marketing*** *communications* 1. Natural or legal persons ~~may~~ **shall be prohibited from** use**ing** electronic communications services for the purposes of sending ~~**or presenting**~~ direct marketing communications to end-users who are natural persons ~~that~~ **unless they** have given their consent.	*Protection from unsolicited communications should be – as far as possible – uniform in the EU. In order to have a high level of privacy protection of consumers in Europe, Germany supports that consumers receive marketing calls only after their prior consent. As far as a uniform level of protection may not be agreed between Member States, Germany supports that as up to now Member States may decide to allow marketing calls on the basis of opt-in or opt-out.*

	Article 16 (2): Germany supports that only E-Mail-marketing in the frame of standing customer relations should be permitted without prior consent of a natural person. Paragraph 2 therefore should read as follows:
2. **Notwithstanding paragraph 1, ~~W~~w**here a natural or legal person obtains ~~electronic~~ contact details for electronic ~~mail~~ **message** from ~~its customer~~ **end-users who are natural persons**, in the context of the **sale purchase** of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these ~~**electronic**~~ contact details for direct marketing of its own similar products or services only if ~~customers~~ **such end-users** are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection **of such end-users' contact details** and**, if that end-user has not initially refused that use,** each time ~~**that**~~ **when a natural or legal person~~s~~ sends a message to that end-user for the purpose of ~~such~~ direct marketing ~~communication is sent or presented~~**.	2. **Notwithstanding paragraph 1, ~~W~~w**here a natural or legal person obtains contact details for electronic **mail ~~message~~** from **its** end-users who are natural persons, in the context of the **sale** of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if such endusers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection **of such end-users' contact details** and **if that end-user has not initially refused that use,** each time ~~**that**~~ **when a natural or legal person~~s~~ sends a message to that end-user for the purpose of ~~such~~ direct marketing ~~communication is sent or presented~~**. .
(…)	(…)
	Article 16 (3) *For the purpose of marketing calls, the as-*

	signed calling line identification should be presented. Under the current draft, the presentation of a calling line on "which they can be contacted" is sufficient. However, a contact could also be established by using a different calling line, e.g. one being provided by a third party. The identification of the calling person would not in any case be possible. Germany therefore suggests the following changes in wording to entail the obligation to present the assigned calling line identification:
3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall~~:~~ ~~(a)~~ present the identity of a **calling** line **identification** on which they can be contacted~~; or~~**.**	3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall~~:~~ present the identity of a calling line **identification <u>assigned to them</u> <u>~~on which they can be contacted.~~</u>**
	Article 16 (3a): *It should be clarified that Member States may demand the use of a prefix from foreign persons or entities as far as these make calls within the member states territory. Paragraph 3a therefore should read as follows:*
~~(b)~~**3a. Member States may require natural or legal person using electronic communications services for the purposes of placing direct marketing calls to** present a specific code/or prefix identifying the fact that the call is a **direct** marketing call **in addition to the obligation**	~~(b)~~**3a. Member States may require natural or legal person using electronic communications services for the purposes of placing direct marketing calls to** present a specific code~~/~~or prefix identifying the fact that the call is a **direct** marketing call **in addition to the obligation set out in**

set out in paragraph 3. Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons who use electronic communications services for the purposes of direct marketing calls. 4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications. (…)	**paragraph 3 <u>when addressing end-users in their territory.</u> Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons who use electronic communications services for the purposes of direct marketing calls** *Article 16 (4):* *It should be taken into account that marketing calls are felt especially disturbing by the addressees. The provisions should therefore be uniform in all Member States. Besides it is unclear, who shall have to bear the burden of proof for the opt-out. It may be considered that the consumer has the burden of proof for the opt-out, as the opt-out is a positive fact for him; in most cases this proof would not be possible to him. Also for reasons of a single protection of personal rights in the EU* ***Germany objects to the provision as proposed in Par. 4.***

7. Chapter IV: Supervision

Germany cannot accept the proposals in the recitals and Article 18. Germany points out that Article 8 of the EU Charter of Fundamental Rights provides for independent data protection supervision only with regard to the processing of personal data. Germany sees no need to impose rules on the Member States regarding the independence of supervision which does not cover the protection of personal data. Germany is in favour of the supervision of protection of personal data in the ePrivacy Regulation being based on the rules of the GDPR.
Germany proposes the following changes to the recitals and Article 18:

(38)~~To ensure full consistency with~~	(38)**To ensure full consistency**

~~Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679.~~ Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. **The designation of supervisory authorities responsible for the monitoring of the application of this Regulation cannot affect the right of natural persons to have compliance with rules regarding the protection of personal data subject to control by an independent authority in accordance with Article 8(3) of the Charter as interpreted by the Court.End-users who are legal persons should have the same rights as end-users who are natural persons regarding any supervisory authority entrusted to monitor any provisions of this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the	**with Regulation (EU) 2016/679, the enforcement of the provisions of this Regulation regarding the processing of personal data should be entrusted to the same independent supervisory authority or authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679. ~~and t~~This Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Regarding this independent supervisory authority Chapter VI and VII of Regulation (EU) 2016/679 should apply.** Member States should be able, **especially with regards to data not constituting personal data,** to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. **~~The designation of supervisory authorities responsible for the monitoring of the application of this Regulation cannot affect the right of natural persons to have compliance with rules regarding the protection of personal data subject to control by an independent authority in accordance with Article 8(3) of the Charter as interpreted by the Court.~~**

effective performance of the additional tasks designated under this Regulation. ~~The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.~~	**End-users who are legal persons should have the same rights as end-users who are natural persons regarding any supervisory authority entrusted to monitor any provisions of this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the additional tasks designated under this Regulation.** ~~The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. Such additional tasks should not jeopardise the ability of the supervisory authority to perform its tasks regarding the protection of personal data under Regulation (EU) 2016/679 and this Regulation. Each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under this Regulation.~~

CHAPTER IV **INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT**	**CHAPTER IV** **SUPERVISORY AUTHORITIES AND ENFORCEMENT**
Article 18 ~~**Independent s**~~**S**upervisory authorities	Article 18 **S**upervisory authorities
0. Each Member State shall provide for one or more independent public authorities meeting the requirements set out in Articles 51 to 54 of Regulation (EU) 2016/679 to be responsible for monitoring the application of this Regulation ('supervisory authorities'), ~~**in accordance with paragraphs 1 and to 1aa of this Article**~~**.**	**0. Each Member State shall provide for one or more** ~~**independent**~~ **public authorities** ~~**meeting the requirements set out in Articles 51 to 54 of Regulation (EU) 2016/679 to be responsible for monitoring the application of this Regulation ('supervisory authorities'),**~~ **in accordance with paragraphs 1 and to 1aa of this Article**~~**.to be responsible for monitoring the application of this Regulation ('supervisory authorities'))**~~**, in accordance with paragraphs 1 and to 1aa of this Article,.**~~
Member States may entrust the monitoring of the application of Articles 12 to ~~**14**~~**16 to the supervisory authority or authorities referred to in the previous subparagraph or to another authority or authorities having the appropriate expertise.**	~~**Member States may entrust the monitoring of the application of Articles 12 to 1416 to the supervisory authority or authorities referred to in the previous subparagraph or to another authority or authorities having the appropriate expertise.**~~
~~**As far as processing of electronic communications data qualifying as personal data is concerned, the supervisory authority referred to in the previous subparagraph shall be responsible for monitoring the application of those articles Regulation (EU) 2016/679**~~	~~**As far as processing of electronic communications data qualifying as personal data is concerned, the supervisory authority referred to in the previous subparagraph shall be responsible for monitoring the application of those articles Regulation (EU) 2016/679**~~

~~shall be responsible for monitoring the application of this Regulation. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.~~	**~~shall be responsible for monitoring the application of this Regulation. Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.~~ <u>As far as a processing of personal data is concerned, the supervisory authority responsible for monitoring the application of regulation (EU) 2016/679 shall be responsible.</u>**
~~1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of~~ **~~Chapter II of~~** ~~this Regulation.~~ **~~Without prejudice to article 19,~~** ~~Chapter~~**~~s~~** ~~VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis*. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.~~	**<u>1.</u>** ~~The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of~~ **~~Chapter II of~~** ~~this Regulation.~~ **Without prejudice to article 19,** with **<u>regard to the processing of personal data Chapters VI and VII of Regulation (EU) 2016/679 shall apply *mutatis mutandis* . The tasks and powers of the supervisory authorities shall be exercised with regard to end-users.</u>**
~~1a. Member Sates shall entrust the monitoring of the application of Chapter III of this Regulation to the supervisory authority or authorities referred to in paragraph 1 of this Article or to another supervisory authority or other supervisory authorities having the appropriate expertise and independence.~~	**~~1a. Member Sates shall entrust the monitoring of the application of Chapter III of this Regulation to the supervisory authority or authorities referred to in paragraph 1 of this Article or to another supervisory authority or other supervisory authorities having the appropriate expertise and independence.~~**
~~1aa. Notwithstanding paragraph 1a, Member States may entrust the moni-~~	**~~1aa. Notwithstanding paragraph 1a, Member States may entrust the moni-~~**

~~toring of the application of Articles 12 to 14 of this Regulation to another supervisory authority or other supervisory authorities having the appropriate expertise.~~	**~~toring of the application of Articles 12 to 14 of this Regulation to another supervisory authority or other supervisory authorities having the appropriate expertise.~~**
1ab. The supervisory authorities referred to in paragraph~~s 1 and to 1aa~~ 0 shall have investigative and corrective powers, including the power ~~to provide remedies pursuant to article 21(1) and~~ to impose administrative fines pursuant to article 23.	**~~1aab.~~ 2. The supervisory authorities referred to in paragraph 1shall have investigative and corrective powers, including the ~~power to provide remedies pursuant to article 21(1) and~~ to impose administrative fines pursuant to article 23.**
1b. Where more than one supervisory authority is responsible for monitoring the application of this Regulation in a Member State, such authorities shall cooperate with each other.	**~~1b.~~3. The supervisory authorities referred to in paragraph 0 shall cooperate with each other.**
2. **Where ~~T~~t**he supervisory ~~authority or~~ authorities referred to in paragraph**~~s~~ 1 ~~and to 1aa~~ 0 ~~shall cooperate with~~ are not the supervisory authority~~ies~~ responsible for monitoring the application of Regulation (EU) 2016/679, they shall cooperate with the latter and,** whenever appropriate**,** with national regulatory authorities established pursuant to the ~~[~~Directive Establishing the European Electronic Communications Code~~]~~ **and other relevant authorities**.	~~2.~~ **~~Where Tt~~**~~he supervisory authority or authorities referred to in paragraph~~**~~s~~** ~~1~~ **~~and to 1aa 0 shall cooperate with are not the supervisory authorityies responsible for monitoring the application of Regulation (EU) 2016/679, they shall cooperate with the latter and,~~** ~~whenever appropriate, with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code]~~ **~~and other relevant authorities~~**~~.~~
Article 19 European Data Protection Board	Article 19 European Data Protection Board

1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have ~~**competence**~~ **the task** to ~~ensure~~ **contribute to** the consistent application of **Chapters ~~I and~~ II and III of** this Regulation~~. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679.~~	1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have **competence ~~the task~~ to ~~ensure~~ contribute to** the consistent application **of Chapters I and II of** this Regulation. ~~To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679~~**.**
2. ~~For the purposes of this Regulation~~To that end, ~~T~~the Board shall also have the following tasks:	**2. ~~For the purposes of this Regulation~~To that end, ~~T~~t**he Board shall also have the following tasks:
~~(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 of Regulation (EU) 2016/679 without prejudice to the tasks of national supervisory authorities;~~	**(aa) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 of Regulation (EU) 2016/679 without prejudice to the tasks of national supervisory authorities;**
(a) advise the Commission on any proposed amendment of this Regulation;	(a) advise the Commission on any proposed amendment of this Regulation;
(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation **in relation to Chapters ~~I, and~~ II and III** and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation**;**	(b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation **in relation to Chapters I and II** and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation**;**
~~(c) draw up guidelines for supervisory~~	**(c) draw up guidelines for supervisory**

~~authorities referred to in paragraph 1 0 of Article 18 in relation to their powers as laid down in Article 58 of Regulation (EU) 2016/679 and setting of administrative fines pursuant to Article 23 of this Regulation~~;	authorities referred to in paragraph ~~1~~ 0 of Article 18 in relation to their powers ~~as laid down in Article 58 of Regulation (EU) 2016/679 and setting of administrative fines pursuant to Article 23 of this Regulation~~;
(d) issue guidelines, recommendations and best practices in order to facilitate cooperation, including exchange of information, between supervisory authorities referred to in paragraph 0 of Article 18 and/or the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 ~~in accordance with point (b) of this paragraph for establishing common procedures for reporting by end-users of infringements of this Regulation regarding rules laid down in paragraph 2 of Article 54 of Regulation (EU) 2016/679~~;	(d) issue guidelines, recommendations and best practices in order to facilitate cooperation, including exchange of information, between supervisory authorities referred to in paragraph 0 of Article 18 and/or the supervisory authority responsible for monitoring the application of Regulation (EU) 2016/679 ~~in accordance with point (b) of this paragraph for establishing common procedures for reporting by end-users of infringements of this Regulation regarding rules laid down in paragraph 2 of Article 54 of Regulation (EU) 2016/679~~;
(da) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph to assess for different types of electronic communications services the moment in time of receipt of electronic communications content;	(da) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph to assess for different types of electronic communications services the moment in time of receipt of electronic communications content;
(db) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph on the provision of consent in the context of	(db) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph on the provision of consent in the context of

Article 6 and 8 of this Regulation by end-users ~~wjp~~ who are legal persons ~~and~~ or in an employment relationship;	**Article 6 and 8 of this Regulation by end-users ~~wjp~~ who are legal persons ~~and~~ or in an employment relationship;**
(e) provide the Commission with an opinion on the icons referred to in paragraph 3 of Article 8;	**(e) provide the Commission with an opinion on the icons referred to in paragraph 3 of Article 8;**
~~(f) promote the cooperation and effective bilateral and multilateral exchange of information and best practices between the supervisory authorities referred to in paragraph 1 0 of Article 18;~~	**~~(f) promote the cooperation and effective bilateral and multilateral exchange of information and best practices between the supervisory authorities referred to in paragraph 1 0 of Article 18;~~**
~~(g) promote common training programmes and facilitate personnel exchanges between the supervisory authorities referred to in paragraph 1 0 of Article 18 and, where appropriate, with the supervisory authorities of third countries or with international organisations;~~	**~~(g) promote common training programmes and facilitate personnel exchanges between the supervisory authorities referred to in paragraph 1 0 of Article 18 and, where appropriate, with the supervisory authorities of third countries or with international organisations;~~**
(h) promote the exchange of knowledge and documentation on legislation on protection of electronic communications of end-users and of the integrity of their terminal equipment as laid down in Chapter II and practice relevant supervisory authorities world wide;	**(h) promote the exchange of knowledge and documentation on legislation on protection of electronic communications of end-users and of the integrity of their terminal equipment as laid down in Chapter II and practice relevant supervisory authorities world wide;**
~~(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities referred to in~~	**<u>(i) maintain a publicly accessible electronic register of decisions taken by supervisory authorities referred to in</u>**

~~**paragraph 0 of Article 18 and courts on issues handled in the consistency mechanism.**~~	**paragraph 0 of Article 18 and courts on issues handled in the consistency mechanism.**
3. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.	**3. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.**
4. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.	**4. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.**
5. The Board shall closely cooperate with the supervisory authorities referred to in Article 18(0) for the purposes of the application of this Regulation. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76 of Regulation (EU) 2016/679, make the result of the consultation procedures publicly available.	**5. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76 of Regulation (EU) 2016/679, make the result of the consultation procedures publicly available.**

CHAPTER V **REMEDIES, LIABILITY AND PENALTIES**		
Article 21 *Remedies*		*Article 21(1):* *The restriction to "every end-user of electronic communications services" is too narrow, since it will not cover violations of Articles 8 and 10. Germany therefore makes the following proposal for a change:* *Germany is also in favour of re-instating the citing of the GDPR provisions:*
1.	1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the ~~same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679~~ **right to an effective judicial remedy in relation to any infringement of his or her rights under this Regulation, the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against any decision of a supervisory authority**.	"1. Without prejudice to any other administrative or judicial remedy, every end-user **covered by this Regulation** of electronic communications services shall have the **same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679**.

~~1a.~~	~~**End-users who are natural persons shall also have the right to representation provided for in** **Articles 77-80 of Regulation (EU) 2016/679 shall apply *mutatis mutandis*.**~~	
		Article 21(2): *Germany is opposed to the proposed deletion and instead proposes the following additions and deletions:*
2.	Any natural or legal person other than end-users adversely affected by infringements of this Regulation ~~and having a legitimate interest in the cessation or prohibition of alleged infringements~~, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.	2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation **and having a legitimate interest in the cessation or prohibition of alleged infringements,** ~~including~~ **such as** provider**s** of electronic communication services ~~protecting its legitimate business interests~~ shall have a right to bring legal proceedings in respect of such infringements.
		Article 21(3) - new *In the proposed version of the ePrivacy Regulation, there is no right, e.g. for associations representing competitors, to sue within the scope of the ePrivacy Regulation; a corresponding addition is required here.*
		3. In respect of persons or organisations which are not adversely affected in own rights by infringements of this

	Regulation but which have the right to sue under national law Article 11 of Directive 2005/29/EC shall apply.
Article 22 *Right to compensation and liability* Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered~~, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage~~ in accordance with Article 82 of Regulation (EU) 2016/679.	*Germany welcomes the deletion of the half-sentence ("unless…") and the related clarification that Article 82 GDPR fully applies.* *However, it is unclear who is the liable infringer.* *Germany therefore sees the need for the following clarification: "infringers" covers not only operators of an electronic communications service, but – as in the GDPR – also third parties (subcontractors, hackers, etc.).*
Article 23 *General conditions for imposing administrative fines* 1. ~~**For the purpose of this Article, Chapter VIII**~~ Article 83 of Regulation (EU) 2016/679 shall apply ***mutatis mutandis*** to infringements of this Regulation. 2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of any legal or	*Articles 23, 24 use the regulatory approach taken by the GDPR. This is logical and consistent, since the ePrivacy Regulation is meant to apply as a complementary and specifying act in relation to the GDPR.*

	natural person who process electronic communications data pursuant to Article 8;	
~~**(b)**~~	~~**the obligations of the provider of software enabling electronic communications, pursuant to Article 10;**~~	(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;
(c)	the obligations of the providers of publicly available directories pursuant to Article 15;	
(d)	the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.	*Regarding Article 23(2)(d):* *- A general point is made about the differing degree of nuisance caused by advertising phone calls and other undesired advertising.* *- A scrutiny reservation is made regarding the level of the proposed fines for undesired communications.*
3.	Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	
4.	Member States shall lay down the rules on penalties for infringements	*Article 23(4):* *Germany wonders why Article 23(4) is*

	of Articles 12, 13, **and** 14~~, and 17~~.	*needed in addition to Art. 24(1). Both provisions regulate the same matter for Articles 12, 13 and 14. Article 24(1) states that the Member States shall stipulate provisions on sanctions for the violations of the Regulation which are not subject to Article 23. This means that violations of Articles 12, 13 and 14 cited in Article 23(4) are already covered by Article 24. This is also systematically correct. In this way, Article 23 could focus on specific, cited violations and sanctions, whilst Article 24 regulates the general sanctions rule to be implemented by the Member States.*
5.	Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	
6.	Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.	*Article 23(6):* *Germany is firmly opposed to the imposition of fines on state agencies, since public persons and bodies can primarily be addressed by supervisory measures or punishments under civil service law in order to oblige them to comply with current legislation. For this reason - in view of the proportionality principle - there is generally no need to impose a fine. If the clause should be neces-*

	sary for other MS, it can only be accepted with the wording provided in the draft: "Member States may lay down rules".
7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process. 8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.	

Article 24 *Penalties* 1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. 2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.	