verbraucherzentrale
Bundesverband

ENSURING PRIVACY AND CONFIDENTIALITY IN ELECTRONIC COMMUNICATIONS

Amendments by the Federation of German Consumer Organisations on the European Commission's proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications

29 June 2017

Editorial information

Federation of German Consumer Organisations

Team Digital and Media

Markgrafenstrasse 66
10969 Berlin

digitales@vzbv.de

Federation of German Consumer Advice Centres and Consumer Associations

Federation of German Consumer Organisations

I. INTRODUCTION

On 21 June 2017 the rapporteur of the European Parliament, Marju Lauristin, presented her draft report[1] on the proposal for a Regulation on Privacy and Electronic Communications[2] (ePrivacy Regulation/ePR). The Federation of German Consumer Organisations (vzbv) broadly welcomes her draft report, as it is a major improvement of the European Commission's proposal.

vzbv strongly welcomes that the rapporteur decided to stick to the European Commission's approach not to introduce a clause allowing processing personal communications data on the legal ground of "legitimate interest" since this would have reduced the rights of individuals in an unacceptable way compared to the current Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector[3] (ePrivacy Directive/ePD). Under no circumstances should the ePR provide a lower standard of protection than that currently enjoyed under the ePD.

Also, vzbv supports the newly introduced provisions that further strengthen users' rights, for example by banning so called "tracking walls" or by introducing stricter requirements for tracking online and offline. Taking into account end-to-end encryption and do-not-track signals are other significant improvements.

But despite these steps in the right direction, some further improvements are still necessary. It is important to clarify the relationship between the ePR and the European General Data Protection Regulation[4] (GDPR) as well as the scope of the ePR. The co-legislators should further strengthen the protection of electronic communication metadata and content, since this data may contain highly sensitive information about the individuals involved. Also, privacy must be the default setting in all software and devices, building on the principles for data protection by design and by default established in the GDPR, to effectively protect the rights of users in a user-friendly way.

vzbv calls upon the co-legislators and the German government to place the rights of individual consumers and citizens firmly at the centre of deliberations concerning the ePR. The starting point for all discussions and for the drafting of the Regulation must be the individual and the individual's right to privacy and confidentiality in the area of electronic communications.

---

[1] Draft report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications); 09.06.2017; http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-606.011&format=PDF&language=EN

[2] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC. All articles and recitals that do not cite specific legislation refer to the ePR.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC dated 25 November 2009.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

II. SUMMARY OF THE KEY DEMANDS

AMENDMENT 30: RELATIONSHIP BETWEEN THE EPR AND THE GDPR

> It has to be clear that, regarding the lawfulness of the processing, the ePrivacy Regulation should prevail over the GDPR. In all other cases, the ePrivacy Regulation should complement the GDPR.

AMENDMENTS 6 & 38: SCOPE OF THE EPR

> To ensure that the confidentiality of communications is comprehensively protected, the Regulation should cover all electronic communications except electronic communication content which was manifestly made public by the user.

AMENDMENT 43: PROCESSING OF ELECTRONIC COMMUNICATIONS METADATA

> A clear-cut separation of communication content and communication metadata as envisaged in the ePR is often impossible in practice. It must therefore be made clear that data must always be treated as content if electronic communication metadata allows conclusions to be drawn as to the content of the communication.

AMENDMENT 54: PROCESSING OF ELECTRONIC COMMUNICATIONS CONTENT

> Electronic communications may contain highly sensitive information about the individuals involved, the disclosure of which may result in serious personal and social harm. Therefore, the processing of electronic communication content should always require explicit consent of the users.
>
> It should not be possible to process electronic communication content for other purposes than the provision of a specific service requested by the user concerned.

AMENDMENTS 21 & 62: PROCESSING OF INFORMATION STORED IN THE USERS' TERMINAL EQUIPMENT OR RELATING TO THIS EQUIPMENT

> "Web audience measurement" is not a purpose by itself for the use of tracking techniques. Therefore, the Regulation should clarify the legitimate purposes allowing to conduct such web audience measurement, like designing an information society service requested by the user in a way to meet users' needs, and introduce appropriate safeguards to ensure that the confidentiality of communications is comprehensively protected.

AMENDMENTS 22 & 66 & 69: COLLECTION OF INFORMATION EMITTED BY TERMINAL EQUIPMENT

> "Statistical counting" is not a purpose by itself for the use of offline tracking techniques. Therefore, the Regulation must clarify the legitimate purposes allowing to conduct such statistical counting, such as counting for public interest or public utility purposes.

Such processing of information emitted by terminal equipment for statistical counting should only be permitted if the purpose could not be fulfilled by other means and provided that necessary privacy safeguards have been put in place.

AMENDMENTS 12 & 73: CONSENT OF USERS

The ePR must clarify the relationship between consent obtained via software settings and consent given independently of those settings. If users are allowed or required to give consent that contradicts their software settings this new (overriding) consent must always have to be given explicitly.

The text must also clearly state that not only consent for processing data from internet or voice communications usage should be invalid if the user has no genuine and free choice or is unable to refuse or withdraw consent without detriment. This should also apply to consent for processing of all electronic communication data in general.

AMENDMENTS 19 & 77: PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

As a general rule, the obligations of “privacy by design” and “privacy by default” should also apply to hardware manufacturers and providers of software permitting electronic communications. That is the only way to effectively and practicably protect the rights of end-users. This would be a streamlined and necessary complement to the GDPR.

AMENDMENTS 5 & 45 & 83: UNSOLICITED E-MAIL COMMUNICATIONS

An extension of the opportunities for direct marketing beyond the situation that exists today is unacceptable. It should not be possible to use end-users’ contact details without their consent for any purpose other than e-mail marketing for similar products and services of the provider concerned.

AMENDMENTS 28 & 93: INTEGRITY OF THE COMMUNICATIONS

As end-users’ daily use of digital technology continues to increase and connected devices are set to become ubiquitous, end-users should have the right to secure communications, private networks and terminal equipment with the best available technologies against unlawful intrusions. It should be prohibited for other parties to circumvent the protective measures taken by users.

AMENDMENTS 97: REPRESENTATION OF DATA SUBJECTS

Article 80 of the GDPR grants data subjects the right to mandate a non-for profit organisation to act on his/her behalf. It also provides the possibility for Member States to allow non-for profit organisations to take action in their own initiative to defend collective interests in the area of data protection. This should also be explicitly allowed under the ePrivacy Regulation to guarantee a comprehensive redress and enforcement framework.

III. AMENDMENTS

Amendment 1: Recital 5

EU-Commission's proposal	vzbv's amendments
(5)The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore *does* not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data ***by providers of electronic communications services should only be permitted in accordance with this Regulation.***	(5)The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore ***should*** not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. ***On the contrary, it aims to provide additional, and complementary, safeguards taking into account the need for additional protection as regards the confidentiality of communications***. Processing of electronic communications data ***should only be permitted in accordance with, and on a legal ground specifically provided under, this Regulation***.

vzbv supports the rapporteur's amendment, but improvements are necessary. Therefore, vzbv supports the EDPS' proposal, that doesn't limit the scope to providers of electronic communications services.

Amendment 2: Recital 7

EU-Commission's proposal	vzbv's amendments
(7) The Member States should be allowed, within the limits of this Regulation, to maintain or introduce national provisions to further specify and clarify the application of the rules of this Regulation in order to ensure an effective application and interpretation of those rules. Therefore, the margin of discretion, which Member States have in this regard, should maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 3: Recital 8

EU-Commission's proposal	vzbv's amendments
(8)This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to software ***providers*** permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing ***commercial*** communications or ***collect*** information related to or stored in end-users' terminal equipment.	(8)This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and ***to providers of*** software ***and hardware*** permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send direct marketing communications or ***process*** information related to, ***processed by*** or stored in end-users' terminal equipment

vzbv supports the rapporteur's amendment, but improvements are necessary.

To archive legal certainty the Regulation should also apply to manufacturers of hardware permitting electronic communications.

To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing".

Amendment 4: Recital 9

EU-Commission's proposal	vzbv's amendments
(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union.	(9) This Regulation should apply to electronic communications data processed in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union. ***This should be the case irrespective of whether the electronic communications***

are connected to a payment or not.

vzbv fully supports the rapporteur's amendment

Amendment 5: Recital 11

EU-Commission's proposal	**vzbv's amendments**
(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic ***mail*** conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. ***In order to ensure*** an effective and equal protection of end-users when using functionally equivalent services, ***this Regulation uses the definition of electronic communications services set forth in the [Directive*** **of the** ***European Parliament and of the Council establishing the European*** Electronic Communications ***Code]. That definition encompasses*** not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.	(11) The services used for communications purposes, and the technical means of their delivery, have evolved considerably. End-users increasingly replace traditional voice telephony, text messages (SMS) and electronic ***messages*** conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services. ***This Regulation aims at ensuring*** an effective and equal protection of end-users when using functionally equivalent services, ***so as to ensure the protection of confidentiality, irrespective*** of the ***technological medium chosen.*** Electronic communications ***services encompass*** not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.

vzbv supports the rapporteur's amendment, but improvements are necessary. To avoid confusion with e-mail (as defined under RFC 5322), vzbv suggests in line with the EDPS' opinion to replace the term "electronic mail" by the more general term "electronic message".

Amendment 6: Recital 13

EU-Commission's proposal	vzbv's amendments
(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*****,** the confidentiality of the communications transmitted through such networks should be protected. 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 electronic communications data using electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of ***the corporation***.	(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 ***Wi-Fi access points*** situated at different places within a city, ***for example*** department stores, shopping malls and hospitals***, as well as airports, hotels and restaurants. Those Wi-Fi access points might require a login or provide a password and might be provided also by public administrations***. To the extent that those communications networks are provided to ***users***, the confidentiality of the communications transmitted through such networks should be protected. 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 electronic communications data using electronic communications services and public communications networks***, except electronic communication content which was manifestly made public by the user.*** In contrast, this Regulation should not apply to closed groups of end-users such as corporate ***intranet*** networks, access to which is limited to members of ***an organisation***.

vzbv supports the rapporteur's amendment, but improvements are necessary. To ensure that the confidentiality of communications is comprehensively protected, the Regulation should cover all electronic communications except electronic communication content which was manifestly made public by the user.

Amendment 7: Recital 14

EU-Commission's proposal	vzbv's amendments
(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.	(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. ***It should also include specific location data, such as for example, the location of the terminal equipment from or to which a phone call or an internet connection has been made or the Wi-Fi access points that a device is connected to, as well as data necessary to identify users' terminal equipment.*** Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content.

vzbv fully supports the rapporteur's amendment

Amendment 8: Recital 15

EU-Commission's proposal	vzbv's amendments
(15) ***Electronic communications data should be treated as confidential. This means that*** any interference with the transmission 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 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.	(15) ***Any processing of electronic communications data or*** any interference with the transmission of electronic communications, 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. ***When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of that Regulation. This should not prevent requesting additional consent for new processing operations.*** The prohibition of interception of communications should apply ***also*** during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee ***and when stored***. 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 ***other*** parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the ***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 habits for the purpose of creating ***user*** profiles. Other

	examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, ***and analysis of customers' traffic data,*** including browsing habits without the ***users***' consent.

vzbv supports the rapporteur's amendment, but improvements are necessary. As suggested by the opinions of the Article 29 Working Party and the EDPS the Regulation should not only protect the confidentiality and security of electronic communications data when in transit, it should also be protected when stored.

Amendment 9: Recital 16

EU-Commission's proposal	**vzbv's amendments**
(16)The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission ***in the electronic communications network. It should not prohibit either the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc.***	(16)The prohibition of storage of ***electronic*** communications ***data*** is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission.

For clarity and to archive legal certainty, the provisions on the processing of metadata to ensure security and integrity, as well as necessary quality of service requirements should be transferred to Recital 16a and be limited to the requirements and the scope of Regulation 2015/2120. These also include the processing of electronic communication data to ensure the security of the network.

Amendment 10: Recital 16a (new)

EU-Commission's proposal	**vzbv's amendments**
	(16a) It should be possible for providers of electronic communications services to process electronic communications metadata for purposes of traffic

management pursuant to and in the limits and the scope of Regulation 2015/2120. Certain electronic communications metadata are necessary to enable providers to correctly bill end-users for the services used and to allow end-users to verify that the cost incurred corresponds to their actual usage. The processing and storage of such data for these purposes should therefore be permitted without requiring consent by the end-user concerned. This processing includes possible processing for customer service purposes. Metadata may also be processed to detect fraudulent use, or abusive use pursuant to Directive (EU) 2013/0309. Where a type of processing of electronic communications metadata is based on the consent of the user a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679. Moreover, the parties involved in the processing of location data and other metadata should make public their methods of anonymisation and further aggregation, without prejudice to secrecy obligations safeguarded by law. The anonymisation method should, once the defined purposes of the processing have been fulfilled, technically prevent all parties from singling out a user within a set of data or from linking new data collected from the users' device to the existing set of data.

---

vzbv supports the rapporteur's amendment, but improvements are necessary. For clarity and to archive legal certainty, the provisions on the processing of metadata to ensure security and integrity, as well as necessary quality of service requirements should be transferred to Recital 16a and be limited to the requirements and the scope of Regulation 2015/2120. These also include the processing of electronic communication data to ensure the security of the network.

Since metadata derived from electronic communications may reveal very sensitive and personal information, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing,

when of processing of electronic communications metadata is based on the consent of the user.

Amendment 11: Recital 17

EU-Commission's proposal	vzbv's amendments
(17) The processing of electronic communications data can be useful for businesses, consumers and society as a whole. ***Vis-à-vis Directive 2002/58/EC, this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, based on end-users consent. However, end-users attach great importance to the confidentiality of their communications, including their online activities, and that they want to control the use of electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain end-users' consent to process electronic communications metadata, which should include data on the location of the device generated for the purposes of granting and maintaining access and connection to the service. Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata.*** Examples ***commercial*** usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using ***colors*** to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier ***is*** necessary to link the positions of individuals at certain time intervals. ***This identifier would be missing if anonymous data were to be used and such movement could not be dis-***	(17)The processing of electronic communications ***metadata*** can be useful for businesses, consumers and society as a whole. Examples of ***such*** usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using ***colours*** to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier ***might be*** necessary to link the positions of individuals at certain time intervals***, provided that the data are immediately anonymised or anonymisation techniques are used where the user is mixed with others***. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.

played*.** Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure. ***Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679.	

vzbv supports the rapporteur's amendment, but improvements are necessary.

It should be clear, that Recital 17 is about the processing of metadata (as stated in the other parts of this Recital and the corresponding Article 6(2)).

Also, there might be situations when it is not necessary to use an identifier to display the traffic movements in certain directions during a certain period of time.

Amendment 12: Recital 17 a (new)

EU-Commission's proposal	**vzbv's amendments**
	(17a) This Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata based on users' informed consent. However, users attach great importance to the confidentiality of their communications, including their online activities, and they want to control the use of their electronic communications data for purposes other than conveying the communication. Therefore, this Regulation should require providers of electronic communications services to obtain users' consent to process electronic communications metadata, which should include data on the location of

	the device generated for the purposes of granting and maintaining access and connection to the service. For the purposes of this Regulation, the consent of an end-user, regardless of whether the latter is a natural or legal person, should have the same meaning and be subject to the same conditions as the consent of the data subject under Regulation (EU) 2016/679. The end-users should have the right to withdraw their consent from an additional service without breaching the contract for the basic service. Consent for processing electronic communications data should not be valid if the user has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.

vzbv supports the rapporteur's amendment, but improvements are necessary. Not only consent for processing data from internet or voice communications usage should be invalid if the user has no genuine and free choice, or is unable to refuse or withdraw consent without detriment. In line with Article 7(4) GDPR this should also apply to consent for processing of electronic communications data in general.

Amendment 13: Recital 18

EU-Commission's proposal	**vzbv's amendments**
(18)End-users may consent to the processing of their metadata to receive specific services such as protection services against fraudulent activities (by analysing usage data, location and customer account in real time). In the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements. For the purposes of this Regulation, consent of an end-user, regardless of whether the latter is a natural or a legal person, should have the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679. Basic broadband internet access and voice communications services are to be consid-	***deleted***

ered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment.	

vzbv fully supports the rapporteur's amendment

Amendment 14: Recital 19

EU-Commission's proposal	**vzbv's amendments**
(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. ***Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse.*** 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. For example, providers may offer services that entail the scanning of ***emails*** to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service re-	(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data ***when stored or*** in transit, with the informed consent of all the ***users*** concerned. For example, providers may offer services that entail the scanning of ***e-mails*** to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the ***user*** where the ***user*** has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After

quested by the ***end-user*** where the ***end-user*** has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the ***end-user*** and received by the intended ***end-user or end-users***, it may be recorded or stored by the ***end-user, end-users*** or by ***a third*** party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.	electronic communications content has been sent by the ***user*** and received by the intended ***user or users***, it may be recorded or stored by the ***user, users*** or by ***another*** party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

vzbv supports the rapporteur's amendment, but improvements are necessary. As suggested by the opinions of the Article 29 Working Party and the EDPS the Regulation should protect the confidentiality and security of electronic communications data, it should also be protected when stored.

Amendment 15: Recital 19a (new)

EU-Commission's proposal	**vzbv's amendments**
	(19a) It should be possible to process electronic communications data for the purposes of providing services explicitly requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users but may only take place with the consent of the user requesting the service. Such specific consent also precludes the provider from processing those data for different purposes.

vzbv fully supports the rapporteur's amendment

Amendment 16: Recital 20

EU-Commission's proposal	vzbv's amendments
(20) Terminal equipment of ***end-users*** of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the ***end-users*** requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes ***information*** that may reveal details of *an* ***individual's*** emotional, political*,* social ***complexities***, including the content of communications, pictures, the location of individuals by accessing the ***device's*** GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. ***Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities.*** Information related to the ***end-user's*** device may also be ***collected*** remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the ***end-user***, and may seriously intrude upon the privacy of these ***end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal***	(20) Terminal equipment of ***users*** of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the ***users*** requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes ***very sensitive data*** that may reveal details of ***the behaviour, psychological features,*** emotional ***condition and*** political ***and*** social ***preferences of an individual***, including the content of communications, pictures, the location of individuals by accessing the GPS capabilities ***of their device***, contact lists, and other information already stored in ***or processed by*** the device, the information related to such equipment requires enhanced privacy protection. Information related to ***or processed by*** the user's device may also be ***processed*** remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the ***user***, and may seriously intrude upon the privacy of these ***users.*** Therefore, any such interference with the ***user's*** terminal equipment should be allowed only with the ***user's*** consent and for specific and transparent purposes. ***Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service. The use of exceptionally privacy invasive technologies and techniques that***

equipment pose a serious threat to the privacy of end-users**.** Therefore, any such interference with the ***end-user's*** terminal equipment should be allowed only with the ***end-user's*** consent and for specific and transparent purposes.	***surreptitiously monitor the actions of users, for example by tracking their activities online or the location of their terminal equipment without the users' knowledge, or subvert the operation of the users' terminal equipment, pose a serious threat to the users' privacy and should be forbidden.***

vzbv supports the rapporteur's amendment, but improvements are necessary.

As suggested by the rapporteur in other Recitals and Articles, the Regulation should include not only information already stored in, but also processed by the device.

To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing".

Exceptionally privacy invasive technology should be forbidden (e.g. so called supercookies and trackers designed to work surreptitiously without the knowledge or consent of the end-users).

Amendment 17: Recital 21

EU-Commission's proposal	**vzbv's amendments**
(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment 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 a specific service explicitly requested by the ***end-user***. This may 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. ***Cookies*** can also be a legitimate and useful tool, for example, in measuring web traffic to a website***.*** 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	(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment 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 a specific service explicitly requested by the ***user***. This may include the storing of ***information (such as*** cookies ***and identifiers)*** for the duration of a single established session on a website to keep track of the user's input when filling in online forms over several pages. ***Tracking techniques, if implemented with appropriate privacy safeguards,*** can also be a legitimate and useful tool, for example, in measuring web traffic to a website ***to design an information society service requested by***

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***.	***the user in a way to meet users' needs***. Information society providers ***could*** engage in configuration checking ***in order*** to provide the service in compliance with the ***user's*** settings and the mere logging ***revealing*** the fact that the user's device is unable to receive content requested by the ***user,*** should not constitute ***illegitimate access***.

vzbv supports the rapporteur's amendment, but improvements are necessary. Web audience measurement is not a purpose by itself for the use of tracking techniques. Therefore, the Regulation should clarify the legitimate purposes allowing to conduct such web audience measurement, like designing an information society service requested by the user in a way to meet users' needs.

Amendment 18: Recital 22

EU-Commission's proposal	**vzbv's amendments**
(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. ***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***	(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, ***users*** are increasingly requested to provide consent to store such ***information*** in their terminal equipment. As a result, ***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 ***prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights. This Regulation should*** provide for the possibility to express consent by ***technical specifications, for instance by*** using the appropriate settings of a browser or other application. ***In this sense, settings must be granular enough to control all data processing that the user consents to and to cover all relevant functionalities (for example, whether websites or apps***

same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged 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.	***can collect location data from the user or can access specific hardware such as a webcam or microphone). Those settings should include a signal which is sent to the other parties to inform them about the user's intentions with regard to consent or objection.*** The ***signals shall*** be binding on, and enforceable against, ***other*** parties.

vzbv supports the rapporteur's amendment, but improvements are necessary.

As a general rule, the obligations of "privacy by design" and "privacy by default" should also apply to hardware manufacturers and providers of software permitting electronic communications. Therefore, these settings shall be binding on, and enforceable against, any other party.

vzbv suggests to use a more technological neutral wording, since cookies are just one tracking technique and web browsers are just one example to control such techniques.

Amendment 19: Recital 23

EU-Commission's proposal	vzbv's amendments
(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 cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only***	(23)The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Therefore, ***hardware manufacturers and*** providers of software ***permitting electronic communications, including*** the retrieval and presentation of information on the internet should have an obligation to configure the ***devices and*** software so that ***their default settings provide the highest level of privacy protection possible, protecting users' against cross-domain tracking and unauthorised interferences with their communications and terminal equipment. If the device or software offers an option to change the default privacy setting, it should offer the user the possibility to express his or her specific consent or his or her objection to the processing***

accept first party cookies'). Such privacy settings should be presented in ***a*** an easily visible and intelligible manner.	***of personal data through technical specifications at any time.*** Such privacy settings should be presented in an easily visible***, objective*** and intelligible manner. ***They should be easily accessible and modifiable during the use of the device or software. Information provided should not incentivise users to select lower privacy settings and should include relevant information about the risks associated with each setting.***

Privacy must be the default setting in all software and devices, building on the principles for data protection by design and by default established in Article 25 of the GDPR, to effectively protect the rights of users in a user-friendly way. Software and hardware permitting electronic communications, should have to be configured so that their default settings provide the highest level of privacy protection possible, protecting users' against cross-domain tracking and unauthorised interferences with their communications and terminal equipment.

If devices or software offer an option to change the default privacy setting, they should offer the user the possibility to express his or her specific consent or his or her objection to the processing of personal data through technical specifications at any time.

vzbv suggests to use a more technological neutral wording, since cookies are just one tracking technique and web browsers are just one example to control such techniques.

Amendment 20: Recital 23a (new)

EU-Commission's proposal	**vzbv's amendments**
	(23a)Children merit specific protection with regard to their online privacy. They usually start using the internet at an early age and become very active users. Yet, they may be less aware of the risks and consequences associated to their online activities, as well as less aware of their rights. Specific safeguards are necessary in relation to the use of children's data, notably for the purposes of marketing and the creation of personality or user profiles.

Children deserve special protection against tracking and against the use of their communications data for advertising purposes.

Amendment 21: Recital 24

EU-Commission's proposal	vzbv's amendments
(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 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 is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the 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 risks associated 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. 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.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 22: Recital 25

EU-Commission's proposal	vzbv's amendments
(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 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 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 tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to ***end-users***, for example when they enter stores, with ***personalized*** offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving 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	(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 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 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 tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for more intrusive purposes, such as to send commercial messages to ***users***, for example when they enter stores, with ***personalised*** offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. ***Users' privacy should be adequately protected in these situations. Information emitted by terminal equipment of users when connecting to a network or other device should only be processed for specific and transparent purposes if the users have consented or if the processing is necessary for statistical counting, as long as such counting is carried out for public interest or public utility purposes, and if there are no other means to achieve the envisaged purpose, including processing of anonymised data, and***

provided where personal data are ***collected*** pursuant to Article 13 of Regulation (EU) 2016/679.	***that the measures established in Article 35 and Article 36 of Regulation (EU) 2016/679 have been fulfilled.*** Providers engaged in such practices ***shall ensure the principle of data minimisation by appropriate technical and organisational measures such as pseudonymisation of the information, restriction of the processing in terms of time and space to the extent strictly necessary for this purpose and anonymisation or erasure as soon as it is no longer needed for this purpose.*** ***They shall also*** display prominent notices located on the edge of the area of coverage informing ***users*** prior to entering the defined area that the ***processing for statistical counting*** is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the ***users' right to object the processing***. Additional information should be provided where personal data are ***processed*** pursuant to Article 13 of Regulation (EU) 2016/679.

vzbv supports the rapporteur's amendment, but improvements are needed.

To prevent high privacy risks for the users, the Regulation should make clear, that it is only legitimate to process information emitted by terminal equipment of users on the basis of their consent or for statistical counting for public interest or public utility purposes, provided that there are no other means to archive the envisaged purpose and provided that necessary privacy safeguards have been put in place.

To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing".

Amendment 23: Recital 32

EU-Commission's proposal	**vzbv's amendments**
(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services. In addition to the offering of products and	(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services***, regardless of the form it takes***. In addi-

services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.	tion to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

vzbv fully supports the rapporteur's amendment

Amendment 24: Recital 33

EU-Commission's proposal	**vzbv's amendments**
(33) Safeguards should be provided to protect end-users against unsolicited communications ***for*** direct marketing ***purposes***, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, ***emails***, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an ***equivalent*** level of protection for all ***citizens*** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer	(33) Safeguards should be provided to protect end-users against unsolicited communications ***or*** direct marketing, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication systems, instant messaging applications, ***e-mails***, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof ***and*** justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an ***equivalently high*** level of protection for all ***individuals*** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer

relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.	relationship for the offering of similar products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.

vzbv fully supports the rapporteur's amendment

Amendment 25: Recital 35

EU-Commission's proposal	vzbv's amendments
(35)In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by ***e-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 their identity line on which the company can be called ***or*** present a specific code identifying the fact that the call is a marketing call.	(35)In order to allow easy withdrawal of consent, legal or natural persons conducting direct marketing communications by ***e-mail*** should present a link, or a valid electronic ***e-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 their identity line on which the company can be called ***and may*** present a specific code identifying the fact that the call is a marketing call.

The German Telecommunications Act stipulates that natural or legal persons using electronic communications services for the purposes of placing direct marketing calls have to present the identity of a line on which they can be contacted. It would be unacceptable if the Regulation falls back behind existing national law by the possibility to choose between the contact line identification or the presentation of a specific code/or prefix.

Amendment 26: Recital 36

EU-Commission's proposal	vzbv's amendments
(36) Voice-to-voice direct marketing calls that do not involve the use of automated calling and communication systems, given that they are more costly for the sender and impose no financial costs on end-users. Member States should therefore be able to establish	***deleted***

and or maintain national systems only allowing such calls to end-users who have not objected.	

vzbv fully supports the rapporteur's amendment

Amendment 27: Recital 37

EU-Commission's proposal	vzbv's amendments
(37) Service providers who offer electronic communications services should ***inform end- users of measures they can take to protect the security of their*** communications ***for instance*** by using specific types of software ***or*** encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679.	(37) Service providers who offer electronic communications services should ***process electronic communications data in such a way as to prevent unauthorised access, disclosure or alteration, ensure that such unauthorised access, disclosure or alteration is capable of being ascertained, and also ensure that such electronic*** communications ***data are protected*** by using specific types of software ***and*** encryption technologies. The requirement to inform end-users of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge. Security is appraised in the light of Article 32 of Regulation (EU) 2016/679. ***The obligations of Article 40 of the [European Electronic Communications Code] should apply to all services within the scope of this Regulation as regards the security of networks and services and related security obligations thereto.***

vzbv fully supports the rapporteur's amendment

Amendment 28: Recital 37a (new)

EU-Commission's proposal	vzbv's amendments
	(37a) As end-users' daily use of digital technology continues to increase and

	connected devices are set to become ubiquitous, end-users should have the right to secure communications, private networks and terminal equipment with the best available technologies against unlawful intrusions. It should be prohibited for other parties to circumvent the protective measures taken by users.

This amendment is necessary to ensure that the confidentiality of communications is comprehensively protected and to prevent privacy risks for the users.

Amendment 29: Recital 41

EU-Commission's proposal	**vzbv's amendments**
(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the ***collection*** of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the ***collection***. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Par-	(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the ***processing*** of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the end-user of the terminal equipment can take to minimise the ***processing***. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the Euro-

liament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.	pean Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. Furthermore, in order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term “collection” should be replaced by the term “processing”.

Amendment 30: Article 1 – paragraph 3

EU-Commission’s proposal	**vzbv’s amendments**
3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.	3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2. ***Therefore,*** ***(a)processing of electronic communications data shall only be permitted on a legal ground specifically provided under this Regulation,*** ***(b)processing of electronic communications data for other purposes shall only be permitted on a legal ground specifically provided under this Regulation,*** ***(c)except as otherwise provided, the provisions of the Regulation (EU) 2016/679 shall apply when personal data is processed.***

This amendment is necessary to clarify the relationship between this Regulation and the GDPR. It has to be clear, that regarding the substantive law (lawfulness of processing) the ePrivacy Regulation prevails over the GDPR. In all other cases (e.g. regarding principles relating to processing of personal data, conditions for consent, conditions to child's consent, rights of the data subject, obligations of the controller and processor, …) the ePrivacy Regulation should complement the GDPR. This approach

is inspired by paragraph 12 of the German Telemedia Act.

Amendment 31: Article 2 – paragraph 1

EU-Commission's proposal	vzbv's amendments
1.This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services ***and*** to information related to the terminal equipment of ***end-users***.	1.This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, ***irrespective of whether a payment is required;*** to ***the protection of*** information related to ***or processed by*** the terminal equipment of***; to the placing on the market of software and hardware enabling electronic communications; to the provision of publicly available directories of users and to the sending direct marketing to users via electronic communications.***.

This amendment seeks to bring clarity to the scope of application of the legislation. To archive legal certainty the Regulation should also clearly apply to providers of hardware and software permitting electronic communications, to providers of publicly available directories and to the use of electronic communications to send direct marketing.

Amendment 32: Article 3 – paragraph 1 – point a

EU-Commission's proposal	vzbv's amendments
(a)the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;	(a)the provision of electronic communications services ***or of software and hardware enabling electronic communications*** to end-users in the Union, irrespective of whether a payment of the end-user is required;

This amendment seeks to bring clarity to the scope of application of the legislation. To archive legal certainty the Regulation should also apply to manufacturers of hardware permitting electronic communications.

Amendment 33: Article 3 – paragraph 1 – point c

EU-Commission's proposal	vzbv's amendments
(c) the protection of information related to	(c) the protection of information related to

the terminal equipment of end-users ***located*** in the Union.	***or processed by*** the terminal equipment of end-users in the Union.

vzbv fully supports the rapporteur's amendment

Amendment 34: Article 3 – paragraph 2

EU-Commission's proposal	vzbv's amendments
2. Where the provider of an electronic communications service is not established in the Union it shall designate in writing a representative in the Union.	2. Where the provider of an electronic communications service***, provider of a publicly available directory, software provider enabling electronic communications or person sending direct marketing commercial communications or processing (other) information related to or stored in the end-users terminal equipment*** is not established in the Union it shall designate in writing a representative in the Union.

vzbv supports the rapporteur's amendment, but improvements are necessary. To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing"

Amendment 35: Article 4 – paragraph 2

EU-Commission's proposal	vzbv's amendments
2. For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 36: Article 4 – paragraph 3 – point -a (new)

EU-Commission's proposal	vzbv's amendments
	(-a) 'electronic communications network' means a transmission system,

	whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

vzbv fully supports the rapporteur's amendment

Amendment 37: Article 4 – paragraph 3 – point -a a (new)

EU-Commission's proposal	**vzbv's amendments**
	(-aa) 'electronic communications service' means a service provided via electronic communications networks, whether for remuneration or not, which encompasses one or more of the following: an 'internet access service' as defined in Article 2(2) or Regulation (EU) 2015/2120; an interpersonal communications service; a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

vzbv fully supports the rapporteur's amendment

Amendment 38: Article 4 – paragraph 3 – point -a b (new)

EU-Commission's proposal	vzbv's amendments
	(-ab) 'interpersonal communications service' means a service, provided for remuneration or not, that enables direct interpersonal and interactive exchange of information via all electronic communications networks; it includes services enabling interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service; it excludes electronic communication content, which was demonstrably made public by the user.

To ensure that the confidentiality of communications is comprehensively protected, the Regulation should cover all electronic communications except electronic communication content which was demonstrably made public by the user.

Amendment 39: Article 4 – paragraph 3 – point -a c (new)

EU-Commission's proposal	vzbv's amendments
	(-ac) 'number-based interpersonal communications service' means an interpersonal communications service which connects to the public switched telephone network, either by means of assigned numbering resources, i.e. number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

vzbv fully supports the rapporteur's amendment

Amendment 40: Article 4 – paragraph 3 – point -a d (new)

EU-Commission's proposal	vzbv's amendments
	(-ad) 'number-independent interpersonal communications service' means an interpersonal communications service

	which does not connect with the public switched telephone network, either by means of assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

vzbv fully supports the rapporteur's amendment

Amendment 41: Article 4 – paragraph 3 – point -a e (new)

EU-Commission's proposal	**vzbv's amendments**
	(-ae) 'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service;

vzbv fully supports the rapporteur's amendment

Amendment 42: Article 4 – paragraph 3 – point -a f (new)

EU-Commission's proposal	**vzbv's amendments**
	(-af) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

vzbv fully supports the rapporteur's amendment

Amendment 43: Article 4 – paragraph 3 – point b

EU-Commission's proposal	**vzbv's amendments**
(b)'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;	(b)'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound***; including electronic communications metadata that enables conclusions to be drawn as to the content of***

	the communication;

It should be clear, that the definition of electronic communications content includes metadata that allows conclusions to be drawn as to the content of the communication. The header of an e-mail for example might be seen as electronic communications metadata, but since it includes the e-mail's subject, it often qualifies as electronic communications content at the same time.

Amendment 44: Article 4 – paragraph 3 – point c

EU-Commission's proposal	vzbv's amendments
(c)'electronic communications metadata' means data ***processed in an*** electronic communications ***network*** for the purposes of transmitting, distributing or exchanging electronic communications content; including ***data used*** to trace and identify the source and destination of a communication, ***data on the location of the device generated in the context of providing electronic*** communications ***services, and the date, time, duration and the type of communication*;**	(c)'electronic communications metadata' means data ***related to a user or*** electronic communications ***service, processed*** for the purposes of transmitting, distributing or exchanging electronic communications content ***and any other communications related data processed for the provision of the service, which is not considered content***; including ***data*** to trace and identify the source and destination of a communication, ***and the date, time, duration and the type of communication; it includes data broadcasted or emitted by the terminal equipment to identify users'*** communications ***and/or the terminal equipment or its location and enable it to connect to a network or to another device***;

vzbv fully supports the rapporteur's amendment.

Amendment 45: Article 4 – paragraph 3 – point e

EU-Commission's proposal	vzbv's amendments
(e)'electronic ***mail'*** means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;	(e)'electronic ***message***' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;

To avoid confusion with e-mail (as defined under RFC 5322), vzbv suggests in line with the EDPS' opinion to replace the term "electronic mail" by the more general term

"electronic message". See also Amendment 83.

Amendment 46: Article 4 – paragraph 3 – point f

EU-Commission's proposal	vzbv's amendments
(f) 'direct marketing communications' means any form of advertising, whether written ***or oral, sent*** to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic ***mail***, SMS, etc.;	(f) 'direct marketing communications' means any form of advertising, whether ***in*** written***, oral or video format, sent, served or presented*** to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic ***message***, SMS, etc.;

vzbv supports the rapporteur's amendment, but improvements are necessary. To avoid confusion with e-mail (as defined under RFC 5322), vzbv suggests replace the term "electronic mail" by the more general term "electronic message".

Amendment 47: Article 5

EU-Commission's proposal	vzbv's amendments
Electronic communications data shall be confidential. Any *interference* with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Electronic communications data shall be confidential. Any ***processing of*** electronic communications data, ***including any interference with electronic communications data*** such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data ***in transit or stored,*** by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

As suggested by the opinions of the Article 29 Working Party and the EDPS the Regulation should not only protect the confidentiality and security of electronic communications data when in transit, it should also be protected when stored.

Amendment 48: Article 5 – paragraph 1 a (new)

EU-Commission's proposal	vzbv's amendments
	(a)Confidentiality of electronic communications shall also include terminal equipment and machine-to-machine communications.

vzbv supports the rapporteur's amendment, but improvements are necessary. All machine-to-machine communications should be included, when they meet the conditions of Article 2 respectively if they don't meet the conditions of Article 2(2).

Amendment 49: Article 6 – title

EU-Commission's proposal	vzbv's amendments
Permitted processing of electronic communications data	***Lawful*** processing of electronic communications data

vzbv fully supports the rapporteur's amendment

Amendment 50: Article 6 – paragraph 1 – introductory part

EU-Commission's proposal	vzbv's amendments
1. Providers of electronic communications networks and services may process electronic communications data if:	1. Providers of electronic communications networks and services may process electronic communications data ***only*** if:

vzbv fully supports the rapporteur's amendment

Amendment 51: Article 6 – paragraph 1 – point b

EU-Commission's proposal	vzbv's amendments
(b)it is necessary to maintain or restore the ***security*** of electronic communications networks ***and*** services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.	(b)it is necessary to maintain or restore the ***availability, integrity and confidentiality*** of ***the respective*** electronic communications networks ***or*** services, or ***to*** detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

This amendment seeks to bring legal certainty. Therefore, the security objectives

should be named in the Regulation instead the vague term “security”.

Amendment 52: Article 6 – paragraph 2 – introductory part

EU-Commission’s proposal	vzbv’s amendments
2. Providers of electronic communications services may process electronic communications metadata if:	2. Providers of electronic communications services may process electronic communications metadata ***only*** if:

vzbv fully supports the rapporteur’s amendment

Amendment 53: Article 6 – paragraph 2 – point c

EU-Commission’s proposal	vzbv’s amendments
(c) ***the*** *end-user* concerned ***has*** given ***his or her*** consent to the processing of ***his or her*** communications metadata for one or more specified purposes, including for the provision of specific services to such *end-users*, provided that the purpose or purposes concerned could not be fulfilled ***by processing information that is made anonymous*.**	(c) ***the user or users*** concerned ***have*** given ***their specific*** consent to the processing of ***their*** communications metadata for one or more specified purposes, including for the provision of specific services to such ***users***, provided that the purpose or purposes concerned could not be fulfilled ***without the processing of such metadata***. ***A data protection impact assessment and a consultation of the supervisory authority should always take place prior to the processing of communications metadata of the basis of the users’ consent. Articles 35 and 36 of Regulation (EU) 2016/679 shall apply with regard to the impact assessment and the consultation to the supervisory authority.***

vzbv supports the rapporteur’s amendment, but improvements are necessary. Consent has always to be informed. Therefore, it would lead to confusion, if this requirement would (only) be mentioned here, as suggested by the rapporteur.

Since metadata derived from electronic communications may reveal sensitive and personal information, a data protection impact assessment and, as the case may be, a consultation of the supervisory authority should always take place prior to the processing, when of processing of electronic communications metadata is based on the consent of the user.

Amendment 54: Article 6 – paragraph 3

EU-Commission's proposal	vzbv's amendments
Providers of the electronic communications services may process electronic communications content only***:***	Providers of the electronic communications services may process electronic communications content only for the sole purpose of the provision of a specific service to a ***user,*** if the ***user has explicitly requested such service and*** the ***users*** concerned have given their ***explicit*** consent to the processing of ***their*** electronic communications content***, provided that*** the provision of that ***specific*** service cannot be fulfilled without the processing of such content ***by the provider*** and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.
(a)for the sole purpose of the provision of a specific service ***to an end-user, if*** the ***end-user*** or ***end-users*** concerned have given their consent to the processing of ***his or her*** electronic communications content *and* the provision of that service cannot be fulfilled without the processing of such content*; or*	
*(****b)if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous****,* and the provider has consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.	

Electronic communications may contain highly sensitive information about the individuals involved, the disclosure of which may result in serious personal and social harm. Therefore, the processing of electronic communication content should always require explicit consent of the users.

To strengthen the rights to privacy and confidentiality of the users, the processing of electronic communication content should be limited the necessary minimum. It should not be possible to process electronic communication content for other purposes than the provision of a specific service requested by the user concerned.

Amendment 55: Article 6 – paragraph 3 a (new)

EU-Commission's proposal	vzbv's amendments
	3a. For the provision of a service explicitly requested by a user of an electronic communications service for their purely individual or individual work-related usage, the provider of the electronic communications service may process electronic communications

	data solely for the provision of the explicitly requested service and without the consent of all users only where such requested processing produces effects solely in relation to the user who requested the service and does not adversely affect the fundamental rights of another user or users. Such a specific consent by the user shall preclude the provider from processing these data for any other purpose.

Children deserve special protection against tracking and against the use of their communications data for advertising purposes.

Amendment 56: Article 6 – paragraph 4 a (new)

EU-Commission's proposal	vzbv's amendments
	4a. Communications data generated in the provision of an electronic communications service specifically intended for children's use or targeted at them shall not be processed for any profiling, marketing or advertising purposes.

Children deserve special protection against tracking and against the use of their communications data for advertising purposes.

Amendment 57: Article 7 – paragraph 2

EU-Commission's proposal	vzbv's amendments
2.Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.	2.Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications ***network or*** service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

Since electronic communications networks are allowed to process electronic communications metadata, they should also be obliged to erase this data or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

Amendment 58: Article 8 – title

EU-Commission's proposal	vzbv's amendments
Protection of information stored in and related to ***end-users'*** terminal equipment	Protection of information stored in, ***processed by*** and related to ***users***' terminal equipment

As suggested by the rapporteur in other Recitals and Articles, the Regulation should include not only information already stored in, but also processed by the device.

Amendment 59: Article 8 – paragraph 1 – introductory part

EU-Commission's proposal	vzbv's amendments
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:	1. The use of processing and storage capabilities of terminal equipment and the ***processing*** of information from ***users***' terminal equipment, ***or making information available through the terminal equipment,*** including ***information*** about ***or generated by*** its software and hardware, other than by the ***user*** concerned shall be prohibited, except on the following grounds:

vzbv supports the rapporteur's amendment, but improvements are necessary. To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing".

Amendment 60: Article 8 – paragraph 1 – point b

EU-Commission's proposal	vzbv's amendments
(b) the ***end-user*** *has* given ***his or her*** consent; or	(b) ***all users concerned have*** given ***their specific*** consent; or

vzbv supports the rapporteur's amendment, but improvements are necessary. Consent needs to be given by all users concerned. Some is terminal equipment, like routers or tablets, is often used by several users.

Amendment 61: Article 8 – paragraph 1 – point d

EU-Commission's proposal	vzbv's amendments
(d)if it is necessary for web audience measuring***, provided that such measurement is carried out by the provider of the information society service requested by the end-user.***	(d)if it is necessary for web audience measuring ***to design an information society service requested by the end-user in a way to meet users' needs. In these cases the provider of this service may produce profiles of usage based on pseudonyms to the extent that the end-user does not object to this. The information society provider shall inform the end-user about his right to object. These profiles of usage must not be combined with data on the bearer of the pseudonym.***

vzbv supports the rapporteur's amendment, but improvements are necessary. Web audience measurement is not a purpose by itself for the use of tracking techniques. Therefore, the Regulation should clarify the legitimate purposes allowing to conduct such web audience measurement, like designing an information society service requested by the user in a way to meet users' needs and introduce appropriate safeguards to ensure that the confidentiality of communications is comprehensively protected. This approach is inspired by Paragraph 15(3) of the German Telemedia Act.

Amendment 62: Article 8 – paragraph 1 – point d a (new)

EU-Commission's proposal	vzbv's amendments
	(da) if it is necessary for a security update, provided that: ***(i) security updates are discreetly packaged and do not in any way change the privacy settings chosen by the user;*** ***(ii) the user is informed in advance each time an update is being installed; and*** ***(iii) the user has the possibility to turn off the automatic installation of these updates;***

vzbv fully supports the rapporteur's amendment

Amendment 63: Article 8 – paragraph 2 – introductory part

EU-Commission's proposal	vzbv's amendments
2.The ***collection*** of information emitted by terminal equipment ***to enable it to connect to another device and, or to network equipment*** shall be prohibited, except if:	2.The ***processing*** of information emitted by terminal equipment shall be prohibited, except if:

All information emitted by terminal equipment should be covered by the Regulation.

Amendment 64: Article 8 – paragraph 2 – subparagraph 1 – point a

EU-Commission's proposal	vzbv's amendments
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or	(a) it is done exclusively in order to, for the time necessary for, and for the ***sole*** purpose of establishing a connection ***requested by the user***; or

vzbv fully supports the rapporteur's amendment

Amendment 65: Article 8 – paragraph 2 – subparagraph 1 – point a a (new)

EU-Commission's proposal	vzbv's amendments
	(aa) the users concerned have given their consent; or

vzbv supports the rapporteur's amendment, but improvements are necessary. There is terminal equipment, like routers or tablets, which is often used by multiple users.

Amendment 66: Article 8 – paragraph 2 – subparagraph 1 – point a b (new)

EU-Commission's proposal	vzbv's amendments
	(ab) it is necessary for the purpose carrying out statistical counting for public interest or public utility purposes and this purpose cannot not be fulfilled by other means.

Statistical counting is not a purpose by itself for the use of tracking techniques. Therefore, the Regulation must clarify the legitimate purposes allowing to conduct such statistical counting, such as counting for public interest or public utility purposes, and in-

troduce appropriate safeguards to ensure that the confidentiality of communications is comprehensively protected. Such processing of information emitted by terminal equipment for statistical counting should only be permitted, if the purpose could not be fulfilled by other means, including processing anonymised data.

Amendment 67: Article 8 – paragraph 2 – subparagraph 1 – point b

EU-Commission's proposal	vzbv's amendments
(b)a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 68: Article 8 – paragraph 2 – subparagraph 2

EU-Commission's proposal	vzbv's amendments
The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 69: Article 8 – paragraph 2 a (new)

EU-Commission's proposal	vzbv's amendments
	2a. For the purpose of point (ab) of paragraph 2, the following safeguards shall be implemented to mitigate the risks: ***(a) the tracking shall be limited to pseudonymised data; and***

	(b) the tracking shall be limited in time and space to the strict minimum necessary to fulfil the established purpose; and ***(c) the data processed shall be deleted or anonymised immediately after the established purpose is fulfilled; and*** ***(d) the users shall have the possibility to easily opt-out, and*** ***(e) technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied .***

vzbv supports the rapporteur's amendment, but improvements are necessary to introduce appropriate safeguards that ensure that the confidentiality of communications is comprehensively protected.

Amendment 70: Article 8 – paragraph 2 b (new)

EU-Commission's proposal	vzbv's amendments
	2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be processed, the purpose of processing, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679, where personal data are collected as well as the users' right to object the processing.

vzbv supports the rapporteur's amendment, but improvements are necessary.

To align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing"

Users should also be informed about their right to object.

Amendment 71: Article 8 – paragraph 2 c (new)

EU-Commission's proposal	vzbv's amendments
	2c. A data protection impact assessment and a consultation of the supervisory authority should always take place prior to the processing of communications data under points (aa) and (ab) of paragraph 2. Articles 35 and 36 of Regulation (EU) 2016/679 shall apply with regard to the impact assessment and the consultation to the supervisory authority.

Since the processing of information emitted by terminal equipment could be used for very intrusive purposes, a data protection impact assessment and a consultation of the supervisory authority should always take place prior to the processing, when the processing is based on the consent of the user or when it is necessary for statistical counting for public interest or public utility purposes.

Amendment 72: Article 8 – paragraph 3

EU-Commission's proposal	vzbv's amendments
3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.	***deleted***

This is already possible pursuant to the GDPR

Amendment 73: Article 9 – paragraph 2

EU-Commission's proposal	vzbv's amendments
2.Without prejudice to paragraph 1, where technically ***possible and*** feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the ***appropriate*** technical ***settings*** of a software application ***enabling access to the internet*.**	2.Without prejudice to paragraph 1, where technically feasible, for the purposes of point (b) of Article 8(1) ***and of point (aa) of Article 8(2)***, consent may be expressed by using the technical ***specifications*** of a software application, ***terminal equipment or information society services. These specifications shall be***

	binding on, and enforceable against, any other party**. **If users are required to give consent that contradicts the settings of their software, this consent shall always have to be given explicitly.

It should be possible to express specific consent also by using the technical specifications of an information society service.

As a general rule, the obligations of "privacy by design" and "privacy by default" should also apply to hardware manufacturers and providers of software permitting electronic communications. Therefore, these settings shall be binding on, and enforceable against, any other party.

Also, the relationship between the privacy settings and consent given by other means should be clarified. A problem might arise for example, when a user objects browser fingerprinting by using a general do-not-track-setting, but is asked by a specific website for his or her consent to such tracking. Therefore, if users are allowed or required to give consent that contradicts the settings of their software, this new (overriding) consent should always have to be given explicitly to avoid confusion.

Amendment 74: Article 9 – paragraph 3

EU-Commission's proposal	vzbv's amendments
3. ***End-users*** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	3. ***Users*** who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3)***, point (b) of Article 8(1) and point (aa) of Article 8(2)*** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.

vzbv fully supports the rapporteur's amendment

Amendment 75: Article 9 – paragraph 4 (new)

EU-Commission's proposal	vzbv's amendments
	4. A user shall not be denied access to any electronic communications service, information society service or func-

	tionality of a terminal equipment, regardless of whether this is remunerated or not, on the mere grounds that he or she has not given his or her consent to
	(a)the processing of electronic communications data, metadata or content pursuant to Article 6; or
	(b)the use of sensing, processing and storage capabilities of terminal equipment and the processing of information from the users' terminal equipment, or making information available through the terminal equipment, including information about and processed by its software and hardware, pursuant to Article 8(1); or
	(c)the processing of information emitted by terminal equipment pursuant to Article 8(2)
	that is not necessary for the provision of that service or functionality.

vzbv supports the rapporteur's amendment, but improvements are necessary. For clarity the amendments on the requirements, when consent can be considered freely given, should be summarised in Article 9.

Amendment 76: Article 10 – title

EU-Commission's proposal	**vzbv's amendments**
Information and options for privacy settings to be provided	***Privacy by design and by default***

Privacy must be the default setting in all software and devices, building on the principles for data protection by design and by default established in Article 25 of the GDPR. That is the only way to effectively protect the rights of users in a user-friendly way. As a general rule, the obligations of "privacy by design" and "privacy by default" should also apply to hardware manufacturers and providers of software permitting electronic communications.

Amendment 77: Article 10 – paragraph -1a (new)

EU-Commission's proposal	**vzbv's amendments**
	(-1a) The default settings of devices and

	software permitting electronic communications, including the retrieval and presentation of information on the internet, shall be configured to provide the highest level of privacy protection possible and protect users' against unauthorised interferences. In particular, default settings shall prevent the tracking of users' online behaviour by other parties.

Privacy must be the default setting in all software and devices, building on the principles for data protection by design and by default established in Article 25 of the GDPR, to effectively protect the rights of users in a user-friendly way. As a general rule, the obligations of "privacy by design" and "privacy by default" should also apply to hardware manufacturers and providers of software permitting electronic communications.

Amendment 78: Article 10 – paragraph 1

EU-Commission's proposal	**vzbv's amendments**
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. ***If devices or*** software permitting electronic communications, including the retrieval and presentation of information on the internet, ***offers the user to change the default privacy settings, it*** shall offer the ***user the possibility to express his or her specific consent for the purposes of point (b) of Article 8(1) and of point (aa) of Article 8(2) or his or her objection to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679 through technical specifications.*** ***These Settings must be easily accessible and modifiable during the use of the device or software.***

If devices or software offer an option to change the default privacy setting, they should offer the user the possibility to express his or her specific consent for the purposes of point (b) of Article 8(1) and of point (aa) of Article 8(2) or his or her objection to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679 through technical specifications at any time.

Amendment 79: Article 10 – paragraph 1 a (new)

EU-Commission's proposal	vzbv's amendments
	1a. For the purpose of paragraph (-1a) and paragraph (1), the settings shall include a signal which is sent to the other parties to inform them about the user's intentions with regard to consent or objection. These signals shall be binding on, and enforceable against, any other party.

vzbv supports the rapporteur's amendment, but improvements are necessary to ensure clarity and to protect the users' rights. Therefore, these settings shall be binding on, and enforceable against, any other party.

Amendment 80: Article 10 – paragraph 2

EU-Commission's proposal	vzbv's amendments
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.In the case of paragraph 1,*** the ***device or*** software shall inform the end-user about the privacy settings options. ***These information shall be presented in an easily visible and intelligible manner. It shall not incentivise end-users to select lower privacy settings and shall include relevant information about the risks associated with each setting.***

If a device or software offers an option to change the default privacy settings, such privacy settings should be presented in an easily visible, objective and intelligible manner. They must be easily accessible and modifiable during the use of the device or software. Information provided should not incentivise end-users to select lower privacy settings and should include relevant information about the risks associated with each setting.

Amendment 81: Article 10 – paragraph 2 a (new)

EU-Commission's proposal	vzbv's amendments
	2a. Hardware and software which enables electronic communications and is specifically intended for children's use or targeted at children shall not allow tracking of its user's behaviour and

	activities for profiling, marketing or advertising purposes.

Children deserve special protection against tracking and against the use of their communications data for advertising purposes.

Amendment 82: Article 16 – paragraph 1

EU-Commission's proposal	**vzbv's amendments**
1. Natural or legal persons ***may use*** electronic communications services for the purposes of ***sending*** direct marketing communications to end-users ***who are natural persons that*** have given their consent.	1. ***The use by*** natural or legal persons ***of electronic communications services, including voice-to-voice calls, automated calling and communications systems, including semi-automated systems that connect the call person to an individual, faxes, e-mail or other use of*** electronic communications services for the purposes of ***presenting unsolicited or*** direct marketing communications to end-users***, shall be allowed only in respect of end-users who*** have given their ***prior explicit*** consent.

vzbv supports the rapporteur's amendment, but improvements are necessary. The German Act Against Unfair Competition stipulates prior explicit consent for advertising by means of a voice-to-voice call or advertising using automated calling machines, faxes or e-mails. It would be unacceptable if the Regulation falls back behind existing national law by reducing the consent requirements.

Amendment 83: Article 16 – paragraph 2

EU-Commission's proposal	**vzbv's amendments**
2.Where a natural or legal person obtains electronic contact details for ***electronic mail*** from its customer, 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 customers 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 and each time a	2.Where a natural or legal person obtains electronic contact details for ***e-mail*** from its customer, 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 customers 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 and each time a message is

message is sent.	sent.

An extension of the opportunities for direct marketing beyond the situation that exists today is unacceptable. To avoid confusion it should be clear that only electronic contact details for e-mail (as defined under RFC 5322) falls under this provision. See also Amendment 45.

Amendment 84: Article 16 – paragraph 3

EU-Commission's proposal	vzbv's amendments
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 line on which they can be contacted; ***or*** (b)present a specific code/or prefix identifying the fact that the call is a marketing call.	3.Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls (a)***shall*** present the identity of a line on which they can be contacted; ***and*** (b)***may*** present a specific code/or prefix identifying the fact that the call is a marketing call.

The German Telecommunications Act stipulates that natural or legal persons using electronic communications services for the purposes of placing direct marketing calls have to present the identity of a line on which they can be contacted. It would be unacceptable if the Regulation falls back behind existing national law by the possibility to choose between the contact line identification or the presentation of a specific code/or prefix.

Amendment 85: Article 16 – paragraph 3 a (new)

EU-Commission's proposal	vzbv's amendments
	3a. Unsolicited marketing communications shall be clearly recognisable as such and shall indicate the identity of the legal or natural person transmitting the communication or on behalf of whom the communication is transmitted. Such communications shall provide the necessary information for recipients to exercise their right to refuse further written or oral marketing messages.

vzbv fully supports the rapporteur's amendment

Amendment 86: Article 16 – paragraph 4

EU-Commission's proposal	vzbv's amendments
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.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 87: Article 16 – paragraph 6

EU-Commission's proposal	vzbv's amendments
6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in ***an easy*** manner, to receiving further marketing communications.	6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in ***a*** manner ***that is as easy as giving the consent and free of charge***, to receiving further marketing communications.

vzbv fully supports the rapporteur's amendment

Amendment 88: Article 17 – title

EU-Commission's proposal	vzbv's amendments
Information about ***detected*** security risks	***Integrity of the communications and*** information about security risks

vzbv fully supports the rapporteur's amendment

Amendment 89: Article 17 – paragraph 1

EU-Commission's proposal	vzbv's amendments
In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 90: Article 17 – paragraph 1 a (new)

EU-Commission's proposal	vzbv's amendments
	(1a)The providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and safety of the transmission are also guaranteed by the nature of the means of transmission used or by state-of-the-art end-to-end encryption of the electronic communications data. Furthermore, when encryption of electronic communications data is used, decryption, reverse engineering or monitoring of such communications shall be prohibited. Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services.

vzbv fully supports the rapporteur's amendment

Amendment 91: Article 17 – paragraph 1 b (new)

EU-Commission's proposal	vzbv's amendments
	(1b)In the case of a particular risk that may compromise the security of networks and electronic communications services, the relevant provider of an electronic communications service shall inform end- users of such a risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies.

vzbv fully supports the rapporteur's amendment

Amendment 92: Article 17 – paragraph 1 c (new)

EU-Commission's proposal	vzbv's amendments
	(1c)As regards the security of networks and services and related security obligations, the obligations of Article 40 of the [European Electronic Communications Code] shall apply mutatis mutandis to all services in the scope of this Regulation.

vzbv fully supports the rapporteur's amendment

Amendment 93: Article 17 – paragraph 1 d (new)

EU-Commission's proposal	vzbv's amendments
	(1d)End-users shall have the right to secure their networks, terminal equipment and electronic communications with the best available technologies against unlawful intrusions. It shall be prohibited to break, decrypt, restrict or circumvent the measure taken by the end-users in this regard.

This amendment is necessary to ensure that the confidentiality of communications is comprehensively protected and to prevent privacy risks for the users.

Amendment 94: Article 19 – paragraph 1 – point b a (new)

EU-Commission's proposal	vzbv's amendments
	(ba) draw up guidelines for supervisory authorities concerning the application of Article 9(1) and the particularities of expression of consent by legal entities;

vzbv fully supports the rapporteur's amendment

Amendment 95: Article 19 – paragraph 1 – point b b (new)

EU-Commission's proposal	vzbv's amendments
	(bb) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for types of services that may be requested for purely individual or work-related usage as referred to in Article 6(3a);

vzbv fully supports the rapporteur's amendment

Amendment 96: Article 19 – paragraph 1 – point b c (new)

EU-Commission's proposal	vzbv's amendments
	(bc) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for: ***(i) web audience measuring to design an information society service requested by the user in a way to meet users' needs referred to in Article 8(1)(d);*** ***(ii) security updates referred to in Article 8(1)(da);*** ***(iii) the processing of information emitted by the terminal equipment referred to in Article 8(2a) and (2b); and***

	(iv) software settings referred to in Article 10;

vzbv supports the rapporteur's amendment, but improvements are necessary due some of vzbv's amendment 61.

Also, to align the Regulation to the GDPR, to archive legal certainty and to protect the confidentiality of electronic communications, the term "collection" should be replaced by the term "processing".

Amendment 97: Article 21 – paragraph 1

EU-Commission's proposal	**vzbv's amendments**
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.	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, 79 ***and 80*** of Regulation (EU) 2016/679.

Article 80 of the GDPR grants data subjects the right to mandate a non-for profit organisation to act on his/her behalf. It also provides the possibility for Member States to allow non-for profit organisations to take action in their own initiative to defend collective interests in the area of data protection. This should also be explicitly allowed under the ePrivacy Regulation to guarantee a comprehensive redress and enforcement framework.

Amendment 98: Article 23 – paragraph 2 – point a

EU-Commission's proposal	**vzbv's amendments**
(a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;	***deleted***

vzbv fully supports the rapporteur's amendment

Amendment 99: Article 23 – paragraph 2 – point b a (new)

EU-Commission's proposal	**vzbv's amendments**
	(ba) the obligations of the providers of publicly available number-based interpersonal communication services pur-

	suant to Article 12, 13 and 14;

vzbv fully supports the rapporteur's amendment

Amendment 100: Article 23 – paragraph 2 – point d a (new)

EU-Commission's proposal	vzbv's amendments
	(da) the obligations of the provider of an electronic communications service and infringements of the right of the end-users pursuant to Article 17.

vzbv supports the rapporteur's amendment, but improvements are necessary. See also amendment 93.

Amendment 101: Article 23 – paragraph 2 – point b

EU-Commission's proposal	vzbv's amendments
(b)the obligations of the provider of software enabling electronic communications, pursuant to Article 10;	(b)the obligations of the provider of software ***and hardware*** enabling electronic communications, pursuant to Article 10;

To archive legal certainty the Regulation should also apply to manufacturers of hardware enabling electronic communications.

Amendment 102: Article 23 – paragraph 3

EU-Commission's proposal	vzbv's amendments
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.	3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure ***and the protection of information stored in, related to or processed by users' terminal equipment*** pursuant to Articles 5 ***to 8*** 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.

vzbv supports the rapporteur's amendment, but improvements are necessary to include infringements of the protection of information stored in, related to or processed by users' terminal equipment.