EPRIVACY REGULATION

Core demands of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) on the pending position by the Council of the European Union (as at: 24 September 2018)

BACKGROUND

With the proposal of the ePrivacy Regulation the European Commission intends to improve data protection and the confidentiality of electronic communications. The European Parliament has already agreed its position on 23 October 2017.

On 8 June 2018, the German government set out its position on the file on the occasion of the discussion of the progress report drafted by the Bulgarian presidency of the Council of the European Union.[1] Austria, which is currently holding the presidency of the Council, published its own text proposals in July 2018[2] and in September 2018[3]. Some approaches discussed in these documents could – in the eyes of vzbv – be a useful basis for the final negotiations with the European Parliament, while others are absolutely unacceptable from a consumer point of view.

PROCESSING OF ELECTRONIC COMMUNICATIONS DATA

Based on the proposal by the European Commission and the European Parliament, electronic communications data – i.e. the content and metadata of electronic communications – could be processed only for purposes permitted by law or if the end-user has consented to the processing. If implemented, these provisions would significantly expand the scope of processing activities that telecommunications companies are currently permitted to perform. At present, the processing of content is not permitted at all and the processing of metadata is subject to much tighter restrictions.

The proposals by the Bulgarian Council presidency and the position stated by the German government would allow pseudonymised metadata – limited to geolocation data only – to be processed by telecommunications providers for the purpose of statistical counting in compliance with some safeguards. But providers would not be permitted to use this data in order to determine the nature or characteristics of an end-user or build a profile of an end-user. Nor could the data reveal special categories of personal data such as personal health details or political views, and it would have to be anonymised or erased as soon as the

[1] See printed paper 19/3384; questions submitted in writing and the corresponding answers provided by the German government during the week beginning on 9 July 2018; as at 13 July 2018; Page 68; http://dipbt.bundestag.de/dip21/btd/19/033/1903384.pdf

[2] ePrivacy Regulation of the Council, working version dated 10 July 2018, for the meeting of WP Tele on 17 July 2018, Council document number 10975/18; https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/00/EU_30006/imfname_10827644.pdf

[3] ePrivacy Regulation of the Council, working version dated 20 September 2018, for the meeting of WP Tele on 27 September 2018, Council document number 12336/18; https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/55/EU_35516/imfname_10840532.pdf

processing purpose was fulfilled. Sharing such data with third parties would not be permitted. In addition, a data protection impact assessment would need to be conducted prior to processing and the competent supervisory authority would need to be consulted. The end-user would also be granted a right to object. In the opinion of vzbv, these proposed compromises would be quite extensive, but would remain within the framework established by the European Charter of Fundamental Rights and be in line with relevant case law from the European Court of Justice.

On the other hand, vzbv is very concerned about the proposals made by the Austrian Council presidency. These proposals would generally permit further processing of electronic communications data for other purposes provided the processing activity is compatible with the purpose for which the data was initially collected. Despite proposed protection measures, this approach would constitute a material change to the status quo and would undermine the confidentiality of communications and the protection of personal data. The European Court of Justice has explicitly established in several judgments that highly sensitive and private information can be disclosed through communications metadata and that this type of data thus requires special protection.[4] The Austrian proposals, however, include neither a purpose limitation nor a limitation to pseudonymised geolocation data or a general exclusion of processing for data that may reveal special categories of personal data. A commercial data retention regime of this kind would also extend to communications metadata of groups of persons such as journalists, lawyers or advice and information centres.

The changes proposed by the Austrian Council presidency also fall short in terms of content. There may be merit in debating the extent to which pseudonymised geolocation data should be made accessible for processing for statistical counting purposes, e.g. to help with the optimisation of traffic flows. Whether and how the Austrian proposals would provide for this type of data usage, however, remains unclear. After all, it is unlikely that this processing purpose would be considered compatible with the original purpose. The Austrian proposals would thus primarily result in years of legal uncertainty for consumers and companies, which would need to be resolved by the courts.

> A return to the level of protection afforded by the current ePrivacy Directive can only be supported in a very limited number of cases and based on strict conditions. Processing of electronic communications data for ‘compatible purposes’ or even – as occasionally discussed – on the legal basis of legitimate interests, is not acceptable, especially in an area as sensitive as this, and it is also incompatible with relevant case law from the European Court of Justice. vzbv thus strongly rejects any proposals that are based on such premises.

[4] See Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970

PROTECTION OF INFORMATION STORED IN THE END-USERS' TERMINAL EQUIPMENT OR RELATING TO THIS EQUIPMENT ('TRACKING')

With regard to the debate on the protection of information stored in the end-users' terminal equipment or relating to this equipment, vzbv emphasises that the proposals put forward by the European Commission and the European Parliament already fall short of the provisions of the current ePrivacy Directive. vzbv supports exceptions that extend to audience measurement carried out by the provider or on behalf of the provider under the conditions of the GDPR and provided that appropriate safeguards are met. vzbv opposes the inclusion of any further legal bases for processing, including in relation to pseudonymised data.

In the eyes of vzbv, watering down the GDPR requirements for freely given, specific, informed and unambiguous consent – which were also set out by the Article 29 Working Party in its Guidelines on Consent[5] – would violate European law. On this basis, permitting so-called 'tracking walls' – a suggestion put forward by the German government – would also cross a red line. This suggestion would allow online services financed through advertising to make the use of their service dependent on the end-user providing his consent to the use of cookies for advertising purposes. This would undermine the explicit stipulation of the GDPR that consent must be freely given, and it would do so with very wide-ranging effect. For instance, complaints such as those filed by the NGO Noyb with various data protection supervisory authorities against Google, Instagram, WhatsApp and Facebook on grounds of 'forced consent' could be rendered groundless.[6] It would also make it easier for these large corporations to pressure users into consenting because their market power would give them more leverage than smaller providers. The result would be exactly the kind of scenario that critics of the GDPR and the ePrivacy Regulation are concerned about: The new EU data protection regime would play straight into the hands of companies like Google and Facebook and would only serve to strengthen their market dominance.

> Allowing tracking walls in the ePrivacy Regulation would undermine the provisions of the GDPR. This would cross a red line. vzbv strongly rejects all attempts to use the ePrivacy Regulation to lower the level of protection afforded by the GDPR.

DATA PROTECTION BY DEFAULT

The proposal by the Austrian Council presidency to strike out Article 10 of the draft Regulation is also unacceptable. vzbv believes that the GDPR requirements concerning data protection by design and by default should be extended to software providers permitting electronic communications, also including software like web browsers. Any other solution would, first and foremost, fail to take appropriate account of the need for protection of particularly vulnerable groups of

[5] Article 29 Data Protection Working Party; Guidelines on Consent under Regulation 2016/679, WP259 rev.01: last updated on 10 April 2018; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
[6] See "noyb.eu files four complaints over 'forced consent' against Google, Instagram, WhatsApp and Facebook"; 25 May 2018; https://noyb.eu/

consumers such as children, elderly people, and those with a low level of education.

vzbv also believes that software providers should be obliged to implement technological features that ensure compliance with the processing provisions under Article 8 of the ePrivacy Regulation. For example, it must be possible to whitelist websites when consent is given or for the purposes of audience measuring. Appropriate technological solutions already exist and would simply need to be implemented in all browsers.

> Privacy-friendly default settings in communications software and devices could protect the rights of end-users in an effective and practicable way and would constitute an appropriate and necessary addition to the provisions of the GDPR. vzbv therefore rejects the proposal to strike out Article 10 of the draft Regulation.

Contact

Verbraucherzentrale
Bundesverband e.V.

Digital and Media
Policy Team

Markgrafenstrasse 66
10969 Berlin
Germany

digitales@vzbv.de