BEUC The European Consumer Organisation

The Consumer Voice in Europe

Permanent Representation to the EU

BE - Brussels

Ref.: BEUC-X-2018-070

12 July 2018

Subject: e-Privacy Regulation – Austrian Presidency proposed Amendments 10975/18

Dear Attaché,

On behalf of the European Consumer Organisation (BEUC), I write to you to present our views regarding the **proposed amendments to the e-Privacy Regulation (ePR)** by the Austrian Presidency in Council document 10975/18 of 10 July 2018, ahead of the WP TELE of 17 July.

The proposed ePR is crucial for the welfare and trust of European consumers and the success of the Digital Single Market. The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy. A robust legal framework that protects consumers' fundamental rights to privacy, confidentiality of communications and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services.

We strongly urge you to defend the following measures to ensure that the ePR effectively protects and empowers European consumers:

1) Permitted processing of metadata (Article 6): additional grounds for processing are unjustified and problematic for consumers

Introducing "further processing for compatible purposes" as a legal basis for processing of metadata **creates a dangerous loophole** in the protection of the fundamental right to the confidentiality of communications and is contrary to the very objective and purpose of the ePR.

As underlined by the European Data Protection Board[1], **Article 6 shout not contain any further exceptions that would enable the indiscriminate processing of users' metadata.** Introducing this additional legal ground would significantly decrease the level of protection below the one in place today, which would be unacceptable for consumers. We therefore **urge you to reject the proposal to include paragraph 2a** on "further processing for compatible purposes" in Article 6.

Tailored exceptions coupled with the appropriate safeguards can be admissible in certain instances. Such is the case for the purpose of **statistical counting**, as proposed in Article 6.2(f). Processing of metadata when it is necessary to protect the **vital interests** of consumers is also reasonable and can be included as proposed in Article 6.2(c).

2) Protection of terminal equipment (Article 8): the proposed additional text in Recital 20 would allow for unlawful tracking

Consumers must never be tracked without their consent. They must be properly informed and must have a genuine choice when deciding whether to give consent or not to a specific use of

[1] Statement of the European Data Protection Board on the revision of the e-Privacy Regulation

their habits when this practice is allowed in specific and narrow circumstances, as required by the General Data Protection Regulation (GDPR).

Unfortunately, the Austrian Presidency's proposed Recital 20 allows for tracking without consent and should not be supported. Recital 20 of the proposed text explicitly assumes that it would not be disproportionate (and hence permissible) for web providers to store and access cookies without consent to obtain "additional benefits for the website operator". In other words, this means that website operators could continue forcing users to consent to being tracked for advertising purposes if they want to access the site. The intended safeguard of providing users with choice between accessing the website with or without being tracked is only a precision and not an obligation. It is important to remember that forcing users to consent to the processing of data which is not necessary for the provision of a service would be contrary to Article 7.4 of the GDPR. The only way Article 8 and Recital 20 will be compatible with the GDPR is if users are given always and without exceptions the possibility to choose between being tracked – or not.

The end of 'tracking walls' will not mean the end of advertising
It is important to ensure that **'tracking walls' and any other type of bundled consent are forbidden**, as the GDPR mandates. This is also the opinion of the European Data Protection Board[2] and the position of the European Parliament[3].

Yet it is crucial to recognise that **the prohibition of 'tracking walls' will not entail the end of services funded through advertising**. Advertising should not necessarily have to be privacy invasive. For example, there are forms of targeted online advertising, such as contextual advertising, which would not require to track users across the web. Companies that wish to rely on behavioural advertising are free to do so, provided that they obtain valid consent from users.

The choice between **"advertising funded model vs. the subscription model" is a false dichotomy**. There are numerous web advertising technologies available as alternatives for companies to choose from. The Regulation should aim to foster the development of privacy friendly business models and avoid that privacy becomes a luxury only for those who can afford to pay for it.

3) Privacy settings (Article 10): a crucial article to ensure privacy and confidential and secure communications

Article 10 should not be deleted because it provides an essential layer of protective measures for consumers and represents one of the key added values of the e-Privacy Regulation. As Eurobarometer[4] data clearly shows, the vast majority of consumers want their devices to be **as protected as possible by default**. This is important because many consumers do not have the necessary technical skills to understand and configure their devices and apps to protect their privacy.

In addition, **Article 10 should be fully aligned with Article 25 of the GDPR** (principles of "Data Protection by Design and by Default"). To achieve this alignment, **Article 10 should include an obligation for service providers and hardware manufacturers to provide 'Privacy by design and by default'**. This should mean that the default settings of smart devices (hardware and software) are to be configured from the outset at the **highest level of privacy available**. Choices made by the users in the settings shall be binding and enforceable upon third parties.

Article 10, as proposed by the European Commission and in previous Bulgarian Presidency proposals, only requires that users are *informed* of the available privacy settings. This approach is incompatible with Article 25 of the GDPR ("Data Protection by Design and by Default") and is not a sufficient level of protection for consumers.

Concerns regarding so-called 'consent fatigue' are unjustified and misconstrued. If properly regulated and thereafter implemented, the principle of "privacy by default" will ensure consumers have the highest level of privacy protection available within each context. Numerous

[2] Statement of the European Data Protection Board on the revision of the e-Privacy Regulation
[3] European Parliament Position on e-Privacy
[4] Eurobarometer on e-Privacy (December 2016)

technological options are already available – and more will surely be created thanks to the internet's vibrant ecosystem – for users to change the settings of the software they use in a non-invasive manner in case this is needed.

We urge you to ensure that the ePR includes these key consumer demands to respect the level of protection in the GDPR and where possible reinforce it. This is crucial not only for consumers' privacy and trust but also for the future of the entire digital economy in Europe.

We remain at your disposal for any questions you might have.

Yours sincerely,

Guillermo Beltrà
Director Legal and Economic Affairs
BEUC – The European Consumer Organisation