BEUC The European Consumer Organisation

The Consumer Voice in Europe

Permanent Representation to the EU

BE - Brussels

Ref.: BEUC-X-2018-045/UPA/DMA/cs 04 June 2018

Subject: Telecommunications Council meeting 8th June – proposed e-Privacy Regulation

Dear Deputy Ambassador,

On behalf of the European Consumer Organisation (BEUC), I write to you in relation to the upcoming orientation debate on the proposed **e-Privacy Regulation (ePR).**

The proposed ePR is crucial for the welfare 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 and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services.

We welcome the progress made under the Bulgarian Presidency and urge you to treat this dossier as an absolute priority to ensure the ePR is adopted as soon as possible and before the end of the European Parliament's legislative term.

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

1) <u>Permitted processing of metadata (Article 6): 'Legitimate Interests' must not be introduced as a legal basis for processing</u>

As underlined by the European Data Protection Board[1], **Article 6 should not allow the processing of electronic communications metadata based on 'legitimate interests'**. Introducing such a broad legal basis for processing would create a very dangerous loophole in the protection of the fundamental right to the confidentiality of communications and be contrary to the very objective and purpose of the ePR. Introducing this additional legal ground would significantly decrease the level of protection below the one in place today, which would be unacceptable for consumers. <u>Allowing further processing of metadata for 'compatible purposes' should not be envisaged either</u>, for similar reasons.

We understand that you are discussing several new permissions to process electronic communications metadata, in particular for purposes of network management and optimisation and for purposes of statistical counting. **We consider that the latest publicly available compromise text proposed by the Bulgarian Presidency[2] reaches an acceptable balance on this point and could provide a good basis to move forward.**

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

[2] http://data.consilium.europa.eu/doc/document/ST-8537-2018-INIT/en/pdf

./..

2) Protection of terminal equipment (Article 8): 'Tracking Walls' should be forbidden

Eurobarometer data clearly shows how important it is for consumers that their devices cannot be accessed without their permission and that their online activities cannot be monitored without their consent[3].

Digital tracking and continuous corporate surveillance is one of the main problems that consumers face today. Reliance on tracking and profiling techniques is widespread online, notably for behavioural advertising purposes. These techniques not only have a very negative impact on consumers' privacy, these can also be (ab)used to discriminate consumers and influence their behaviour.

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, as required by the General Data Protection Regulation (GDPR). To achieve this, 'tracking walls' should be forbidden**. This is also the opinion of the European Data Protection Board[4] and the position of the European Parliament[5].

Unfortunately, that is not what the latest publicly available Bulgarian Presidency compromise proposal establishes. Recital 20 of the proposed compromise text from May 4 would specifically authorise 'tracking walls'. The recital states that access to specific website content may still be made conditional on the consent to the storage of a cookie or similar identifier which are used to provide for additional benefits of the website operator. In practice, this means for example that website operators could continue forcing users to consent to being tracked for advertising purposes if they want to access the site. Opening the possibility of forcing users to consent to the processing of data which is not necessary for the provision of a service would run against Article 7.4 of the GDPR.

Putting an end to 'tracking walls' should not lead to an end of services funded through advertising, as 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.

In our view, the choice between "advertising funded model vs. the subscription model" as presented by certain industry stakeholders is a false dichotomy. **There is a choice to be made between different types of advertising**. 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): "Privacy by Default" Should Be Mandatory

Article 10, as proposed in the latest publicly available compromise text by the Bulgarian Presidency, 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.

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

./…

As Eurobarometer[6] data shows, the clear majority of consumers want their devices to be as protected as possible by default. To achieve this, **Article 10 should include an obligation for service providers and hardware manufacturers to provide 'Privacy by default'**. This should mean that the default settings of smart devices and software are configured to guarantee the **highest level of privacy available from the outset**. Choices made by the users in the settings shall be binding and enforceable upon third parties.

We urge you to ensure that the ePR includes these key consumer demands and that it does not decrease the level of protection in the GDPR but reinforce it. This is crucial not only for consumers' privacy but also for the future of the Digital Economy.

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

Yours sincerely,

Ursula Pachl
Deputy Director General
BEUC – The European Consumer Organisation

[6] Eurobarometer on e-Privacy (December 2016)