Statement 03/2021 on the ePrivacy Regulation

Adopted on 9 March 2021

The European Data Protection Board has adopted the following statement:

The EDPB welcomes the agreed negotiation mandate adopted by the Council on the protection of privacy and confidentiality in the use of electronic communication services ('the Council's position'), as a positive step towards a new ePrivacy Regulation. It is of utmost importance that the EU general data protection framework is rapidly complemented with harmonised rules for electronic communications.

As already stated on numerous occasions[1], the ePrivacy Regulation must under no circumstances lower the level of protection offered by the current ePrivacy Directive but should complement the GDPR by providing additional strong guarantees for confidentiality and protection of all types of electronic communication. In no way the ePrivacy Regulation can be used to de facto change the GDPR. In this regard, the Council's position is raising a series of concerns and the EDPB wishes to point issues, which should be addressed in the upcoming negotiations.

This statement is without prejudice to a possible future more detailed EDPB statement or opinion on the co-legislators positions.

Concerns regarding processing and retention of electronic communication data for the purposes of law enforcement and safeguarding national security

With respect to Article 6(1)(d) and Article 7(4), the EDPB reiterates that legislative measures requiring providers of electronic communications services to retain electronic communication data have to comply with:

- Articles 7 and 8 of the EU Charter of Fundamental Rights ('Charter'),
- the latest case law of the Court of Justice of the EU ('CJEU')[2] as well as
- Article 8 of the European Convention on Human Rights.

The EDPB considers that the ePrivacy Regulation cannot derogate from the application of the latest CJEU case law, which notably provides that Articles 7, 8, 11 and 52(1) of the Charter must be interpreted as precluding legislative measures, which would provide, as a preventive measure, the

[1] See the complete list of documents on the ePrivacy rules produced by the EDPB and the Article 29 Working Party as annex to this statement.
[2] CJEU joined cases C-511/18, C-512/18 and C-520/18, case C-623/17.

general and indiscriminate retention of traffic and location data. Therefore, providing a legal basis for anything else than targeted retention for the purposes of law enforcement and safeguarding national security is not allowed under the Charter, and would anyhow need to be subject to strict temporal and material limitations as well as review by a Court or by an independent authority.

With regard to the exclusion from the scope of the Regulation of processing activities by providers, the EDPB considers that such exclusion runs against the premise for a consistent EU data protection framework. In the event of an exclusion, the EDPB stresses nevertheless that the GDPR applies.

Confidentiality of electronic communications requires specific protection (Articles 6, 6a, 6b, 6c)

Confidentiality of communications is a fundamental right protected under Article 7 of the Charter already implemented by the ePrivacy Directive. This right to confidentiality must be applied to every electronic communication, regardless of the means by which they are sent, at rest and in transit, from the sender to the receiver, and must also protect the integrity of every user's terminal equipment.

General prohibitions with narrow exceptions for personal data processing

The EDPB fully supports the approach based on general prohibitions and with narrow, specific and clearly defined (purpose oriented) exceptions.

However, the EDPB is concerned that some exceptions (in particular Article 6(1)(c), Article 6b(1)(e), Article 6b(1)(f), Article 6c) introduced by the Council seem to allow for very broad types of processing, and recalls the need to narrow down those exceptions to specific and clearly defined purposes. In any case, those specific purposes should be explicitly listed in order to ensure legal certainty and the highest possible degree of the protection.

Furthermore, the exceptions under Article 6(1)(b), Article 6(1)(c) and Article 6(1)(d), allowing the access of electronic communications data, including content, to ensure network and end user device security could allow full access by the electronic communication service provider or their processors to the contents of all end user communications. Since this could undermine the end user`s right to confidentiality and privacy expectations, it has to be proportionate and should be narrowed down at least to recall that this cannot lead to the systematic monitoring of electronic communication content, nor allow providers or processors to circumvent any encryption.

Lastly, the Regulation should emphasize the role of anonymisation as the core guarantee that should be systematically favoured when it comes to the use of electronic communication data.

The availability of strong and trusted encryption is a necessity in the modern digital world

Strong state-of-the-art encryption should be the general rule to ensure a secure, free and reliable flow of data between citizens, businesses and governments, and is crucial to ensure compliance with the security obligation of the GDPR, for example, for health data, and protection of IT systems in a context of rising threats. End-to-end encryption, from the sender to the recipient, is also the only way to ensure full protection of data in transit. Any possible attempt to weaken encryption, even for purposes such as national security would completely devoid those protection mechanisms due to their possible unlawful use. Encryption must remain standardized, strong and efficient[3].

[3] Statement of the Article 29 Working Party on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, April 11 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

The new Regulation must enforce the consent requirement for cookies and similar technologies, and offer service providers technical tools allowing them to easily obtain such consent (Article 8[4])

The need for a privacy preserving approach regarding "take it or leave it" solutions

It should be recalled that provisions on consent under the GPDR apply in the context of the ePrivacy rules. Therefore, the EDPB considers that the necessity to obtain a genuine freely-given consent should prevent service providers from using unfair practices such as "take it or leave it" solutions, which make access to services and functionalities conditional on the consent of a user to the storing of information, or gaining of access to information already stored in the terminal equipment of a user (the so-called "cookie walls")[5].

The EDPB stresses the need to include an explicit provision in the ePrivacy Regulation to enshrine this prohibition, in order to enable users to accept or refuse profiling. Users should therefore be proposed with fair alternatives offered by the same service providers. Such principles should apply equally to all service providers, regardless of their sector of activity or of their current financing model (see recital 21aa of the Council's position).

Audience measurement shall be limited to non-intrusive practices that are not likely to create a privacy risk for users

The Council's position creates a new exception for audience measurement as suggested by the Article 29 Working Party[6]. However, the derogation for audience measurement as proposed by the Council is worded too broadly and could lead to an overly broad interpretation of what could fall under the scope of the derogation and consequently lower the level of protection of end users' terminals.

Therefore, the EDPB stresses that the derogation for audience measurement should be limited to low level analytics necessary for the analysis of the performance of the service requested by the user and should be solely limited to providing statistics to the service operator, and must be put in place by the operator or their processors. Therefore, this processing operation cannot give rise, by itself or in combination with other tracking solutions, to any singling-out or any profiling of users by the provider or other data controllers. Moreover, the audience measurement service should not allow to collect navigation information related to users across distinct websites/applications and should include a user-friendly mechanism to opt-out from any data collection.

Effective way to obtain consent for websites and mobile applications (Article 4a)

The EDPB considers that the ePrivacy Regulation should improve the current situation by giving back control to the users and addressing the "consent fatigue". Article 4a should go further and oblige browsers and operating systems to put in place a user friendly and effective mechanism allowing controllers to obtain consent, in order to create a level playing field between all actors. The scope of the Regulation should also explicitly include browser and operating system providers.

---

[4] As well as the associated recitals (20aaaa and 21aa of the Council's position).

[5] As previously stated by the EDPB in Statement on the revision of the ePrivacy Regulation, adopted on 25 May 2018, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf and in the EDPB Guidelines 05/2019 on consent under Regulation 2016/679, para. 39, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[6] See also Opinion 04/2012 on Cookie Consent Exemption (WP 194), p. 10-11. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

Privacy settings should preserve the right to the protection of personal data and the integrity of terminals of users by default and should facilitate expressing and withdrawing consent in an easy, binding and enforceable manner against all parties.

Further processing for compatible purposes (Article 6c and Article 8(1)(g))

In relation to ongoing discussions on the further processing of electronic communications metadata/data collected through cookies and similar technologies, the EDPB reiterates its support to the approach of the ePrivacy Regulation as originally proposed by the European Commission and followed by the European Parliament, based on a general prohibition, followed by narrow exceptions and the use of consent. Further processing for compatible purposes entails the risk of undermining the protection afforded by the ePrivacy regulation, especially for processing electronic communications metadata, by allowing processing for any purpose that is judged by the service provider to meet the 'compatibility' clause while the legislator clearly sought to restrict their use to specific purposes in the absence of consent. The EDPB wishes to emphasise that the aforementioned data can still be further processed without consent and without creating risks for the users after it has been anonymised.

Future role of supervisory authorities, the EDPB and cooperation mechanism (Articles 18 to 20)

The EDPB recalls that, in order to guarantee a level playing field on the Digital Single Market, it is essential to ensure a harmonised interpretation and enforcement of all data processing provisions of the ePrivacy Regulation across the EU.

Oversight of privacy provisions under the ePrivacy Regulation should be entrusted to the competent supervisory authorities under the GDPR to further support consistency

The EDPB would like to recall that there is a clear interconnection of competencies between national authorities competent under the current ePrivacy Directive and data protection authorities. Provisions of the future ePrivacy Regulation related to the protection of privacy should not be applied in isolation, since they are intertwined with personal data processing and the GDPR.

Hence, in order to conciliate a high level of protection of personal data and legal and procedural certainty, national authorities responsible for enforcement of the GDPR should be entrusted with the oversight of the provisions of the future ePrivacy Regulation related to the processing of personal data, as initially proposed by the European Commission[7].

The EDPB notes that, unlike in the initial proposal of the European Commission, all the references to the cooperation and consistency mechanism as provided by Chapter VII of the GDPR have been removed from the Council's position. For the reasons recalled above, the EDPB reiterates that only a perfect alignment with the GDPR cooperation and consistency framework would allow the ePrivacy Regulation to reach its goals, to avoid fragmentation in the enforcement and application of the Regulation, as well as to lessen the burden for the providers that would otherwise have to address possibly over 27 supervisory authorities.

[7] European Commission, 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), 10 January 2017, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010, and the associated opinion of the Article 29 Working Party, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

In case national competent authorities who are not members of the EDPB would have to interact with the EDPB, as currently the Council's position foresees, their ability to contribute timely to the consistent application of the ePrivacy Regulation would diminish to the detriment of both the digital economy and the protection of the fundamental rights.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX: List of previous documents produced by the EDPB and the Article 29 Working Party

- Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf.
- Opinion 04/2012 on Cookie Consent Exemption (WP 194), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.
- Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240), available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
- Opinion of the Article 29 Working Party 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), available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
- Statement of the Article 29 Working Party on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, Brussels, April 11 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
- EDPB Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, adopted on 25 May 2018, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.
- EDPB Statement 3/2019 on an ePrivacy Regulation, adopted on 13 March 2019, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf.
- EDPB Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB, adopted on 19 November 2020, available at: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_en.