Statement of the EDPB 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

The Data Protection Authorities of the European Union, united in the European Data Protection Board, consider that the revision of the current ePrivacy Directive (2002/58/EC, amended by 2009/136/EC) is an important and necessary step that has to be concluded rapidly. The use of IP based communication services has become widespread since 2009, and these 'Over-the-Top' services are currently not covered by the existing Directive; in order to ensure that end-users' confidentiality of communications is protected while using these new services and to create a level playing field for providers of electronic communication and functionally equivalent services, we call on the European Commission, Parliament and Council to work together to ensure a swift adoption of the new ePrivacy Regulation, replacing the current Directive as soon as possible after the coming into effect of the General Data Protection Regulation in May this year.

Given the developments in deliberations on the proposal, and for the benefit of the co-legislators, the EDPB has decided to offer further advice and clarifications on some specific issues raised by the proposed amendments by the co-legislator.

1. Confidentiality of electronic communications requires specific protection beyond the GDPR

Confidentiality of communications (the modern equivalent of the traditional postal secrecy of correspondence) is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union, already implemented by the ePrivacy Directive. This right to confidentiality must be applied to every electronic communications, 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.

Electronic communications are the keystone of many essential activities of our modern societies, since they support the exercise of many fundamental rights such as freedom of thought, conscience, religion, expression, information, assembly, association, etc. Reinforcing the confidentiality and neutrality of the messaging services delivering our communications is therefore a necessity.

Given the importance and the widespread use of electronic communications in our digital lives, they are very likely to contain, or to reveal, special categories of personal data, either explicitly or because of mere accumulation and combination of electronic communications content or metadata, which can allow very precise conclusions concerning the private lives of the people to be drawn, implying high risks for their rights and freedoms, and should therefore be treated accordingly.

Therefore, we fully support the approach of the proposed Regulation, based on broad prohibitions, narrow exceptions, and the use of consent. Accordingly, there should be no possibility under the ePrivacy Regulation to process electronic communications content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service. Furthermore, there should be no possibility under the ePrivacy Regulation to process electronic communications metadata for the performance of a contract, meaning that there should not be an exception based on the

general purpose of the performance of a contract, as the Regulation lays down which exact processing is permitted to this end, such as processing for billing purposes.

The EDPB wishes to emphasise that electronic communications metadata can still be further processed without consent after it has been genuinely anonymised[1]. The EDPB encourages electronic communication service providers to use this possibility, in order to create innovative services while preserving privacy.

2. The ePrivacy Directive is already in force

Protection of confidentiality of communications is a right already existing today. The 2002 ePrivacy Directive, amended in 2009, has already established a general prohibition on the processing of electronic communications content and metadata. Those operations are only possible:

- with the prior consent of the user, or
- if they meet one of the exceptions offered by the ePrivacy Directive (transmission of an electronic communication, billing).

Transmission services used for the provision of machine to machine services are also in the scope of the current Directive. Those provisions are maintained in the proposed Regulation.

Similarly, the protection of terminal equipment is already a right. The use of storage capacities of the user's terminal equipment applies in a technology-neutral manner. Thus, not only cookies, but every tracking technology is already subject to consent of the user or is subject to one of the exceptions specified in the ePrivacy Directive.

Additionally, the proposed Regulation as amended by the co-legislator creates several new exceptions that were proposed by the WP29[2], such as security updates and audience measurement. Those exceptions are related to specific types of processing with very limited privacy risks for the users.

3. The proposed Regulation aims at ensuring its uniform application across every Member State and every type of data controller

The current ePrivacy Directive does not apply to electronic communications services offered by providers that operate over the Internet, despite the fact that they offer a service which is functionally equivalent.

Those providers will however be within the scope of the proposed Regulation. The EDPB emphasises that the extension of the scope of the Regulation to functionally equivalent services, including so called 'Over-the-Top' services is an essential element of the reform. Any proposed changes in the draft Regulation that may undermine this objective (for example, any proposals to limit the scope of protection to communications data 'in transit') should be avoided, to guarantee an equal level playing field for every providers.

The proposed Regulation also applies as soon as data relating to the behaviour of users is collected, whether or not they have created an account for a service. This approach will not only offer the users of those services the protection they deserve, but it will also permit fair competition between data controllers. It should be noted that the consent that must be obtained under the ePrivacy Regulation has the same meaning as in the GDPR. In particular, the necessity to obtain a freely-given consent will prevent service providers from including *cookie walls*[3] for their users, and the obligation for the consent to be specific will create an equal playing field for providers whether or not the user is logged in.

Moreover, the creation of specific sanctions for violating the ePrivacy Regulation combined with an extended territorial scope, both of which mirror the provisions of the GDPR, will give

---

[1] As defined in WP216, whereas pseudonymised data remain personal data.
[2] See WP194 and WP240.
[3] A '*cookie wall*' prevents users who do not consent from accessing a web site or a service.

the effective power to the Data Protection Authorities, which will allow them to enforce the application of the Regulation for all electronic communication tools used by EU-users.

4. The new Regulation must enforce the consent requirement for cookies and similar technologies and offer services providers technical tools allowing them to obtain that consent

As proposed by the European Commission, Article 10 of the proposed Regulation is designed to offer users control over the use of the storage capabilities of their terminal equipment. Article 10 was further developed by the Parliament to require privacy by default in respect of software settings and to provide a technical solution for websites to obtain a valid consent.

The EDPB fully supports strengthening this Article, and considers that it should explicitly apply to operating systems of smartphones, tablets, or any other 'user agent', in order to ensure that communications applications can take into account the choices of their users, no matter what technical means are involved.

Moreover, privacy settings should facilitate expressing and withdrawing consent in an easy, binding and enforceable manner against all parties, and users should be offered a clear choice upon installation, allowing them to give their consent if they wish to do so. Additionally, web site and mobile applications should be able to obtain a GDPR compliant consent through the privacy settings.

5. Conclusions

The EDPB considers that:

- The ePrivacy Regulation should not lower the level of protection offered by the current ePrivacy Directive.
- The ePrivacy Regulation should provide protection for all types of electronic communications, including those carried out by 'Over–the-Top' services, in a technology neutral way.
- User consent should be obtained systematically in a technically viable and enforceable manner before processing electronic communications data or before using the storage or processing capabilities of a user's terminal equipment. There should be no exceptions to process this data based on the 'legitimate interest' of the data controller, or on the general purpose of the performance of a contract.
- Article 10 should provide an effective way to obtain consent for websites and mobile applications. More generally, settings should preserve the privacy of the users by default, and they should be guided to choose a setting, on receipt of relevant and transparent information. In this regard, the Regulation should remain technology neutral to ensure that its application remains consistent whatever the use cases.
- The highest level of scrutiny should be applied for any ad hoc exceptions that the legislators may wish to consider adding to those already included in the Commission and Parliament drafts texts. In particular, any broadly -framed exceptions for cases where 'a public authority' requests processing of data should be carefully scrutinised, and the proposal should not allow the indiscriminate monitoring of user's location or the processing of their metadata.
- In order for consent to be freely given as required by the GDPR, access to services and functionalities must not be made conditional on the consent of a user to the processing of personal data or the processing of information related to or processed by the terminal equipment of end-users, meaning that cookie walls should be explicitly prohibited.
- The use of genuinely anonymised electronic communication data should be encouraged.

- The aforementioned evolutions will protect the privacy of end-users in every relevant context and prevent any distortions of competition.