# EDiMA feedback on the REFIT of the ePrivacy Directive

EDiMA, the European association representing online platforms and other innovative tech companies, continues to support the European Commission in its ambition to build an EU Digital Single Market (DSM), and welcomes the Commission's evaluation of the ePrivacy Directive ("ePD"). The ePrivacy Directive has been an important instrument to foster national legislation ensuring the privacy, security and confidentiality of communications. We believe that any future review must be measured, keeping the following goals in mind:

- To provide predictability for service providers, avoid unnecessary burdens, and ensure consistency with other privacy, consumer or security legislation;
- That it does not inadvertently weaken the privacy and security standards it seeks to protect;
- Upholding the principle of technology neutrality as the underlying technology or infrastructure that delivers a service matters and will affect the ability of a service to meet the legal requirements.

**Relationship with GDPR**

Since the adoption and revision of the ePrivacy Directive, a number of new legal instruments have been put in place that both contribute to and achieve the same objectives. This is particularly true of the GDPR, which imposes extensive restrictions on the use of personal data and is applicable to all sectors - thereby extending the obligations originally outlined in the ePrivacy Directive to all sectors. Whilst there may have been a need in the past to further specify the online application of the old data privacy laws, the new GDPR now offers a clearer and higher level of protection regarding the processing of all types of data. Therefore the need for any sector specific rules on privacy must be carefully considered in order to ensure it does not create conflicting requirements. It is important that the review of the ePrivacy Directive the GDPR, rationalising redundant/overlapping provisions, such as security and data breach notification requirements, and ensuring that the remaining provisions are consistent with obligations under the GDPR (i.e. processing of traffic data). Ultimately the review must aim to truly simplify the regulatory environment and focus only on those areas that bring added value that the GDPR and related instruments do not currently cover.

**Scope**

EDIMA questions the added value in expanding the scope to cover online communication services ("interpersonal communication services") and services that merely convey signals (Machine-to-Machine (M2M) or Internet of Things (IoT)), as we have done in the context of the draft EU Communication Code. These services are already sufficiently regulated by existing EU privacy and consumer protection provisions. Extending regulation to OTTs is not required to ensure the appropriate level of protection for consumers, as they are already subject to a variety of EU directives ensuring protection in the digital space, most recently under Article 4 of the GDPR and the NIS Directive. Instead, given appropriate safeguards, regulators should consider removing the telecoms provisions of the ePD, where they are no longer necessary to protect consumers or competition. Furthermore, like the data protection rules, the EU consumer protection rules are also being overhauled in order to ensure that consumer security is sufficiently protected in the digital space.

1. **Confidentiality of Communications**

Confidentiality of communications is a fundamental right under Art.7 of the European Charter of Fundamental Rights. This allows individuals access to and use of the best possible technology to protect the confidentiality of their communications, and no law should restrict that ability. EDIMA members fully support this right and continue to develop and make available many of the tools allowing users to implement it. We don't believe that the ePD is strictly necessary to ensure that communications remain confidential; it is a fundamental right in EU law, which has been enforced and further developed by a wealth of EU national and case law. The GDPR, which covers all entities and services, also provides similar protections to the ePrivacy in securing confidentiality of communications and personal data, such as Articles 32-34 of the GDPR.

That said, the review does provide an opportunity to modernise this right in light of technological developments. It is important the review not only reinforces this right by encouraging communication services to provide users with solutions that allow them to secure their communication, but also clarifies that there are legitimate circumstances where service providers might need to access the communications, which are stored on their systems. Below are a few example of such legitimate circumstances.

- **Information Security:** Service providers should be able to scan and filter communications for malware, phishing and spam detection, where appropriate. Businesses have a legitimate interest in ensuring the security and integrity of their networks/service and the data they are entrusted with.

- **Filtering out illegal or unacceptable content** – Service providers often rely on automated tools to scan communications to identify illegal content, such as child exploitation imagery. Businesses should be allowed to continue such activities.

- **Product features** – Certain product features of service providers provide enhanced capabilities that go far beyond transmitting and routing communications. Product features such as translators, bot functionalities, group video callings, message syncing across devices, or assistive technologies that automatically copy hotel reservations, travel itineraries, etc., in the users' calendar are not possible without access to the communications content itself.

**Access for law enforcement**

Any expansion of the ePrivacy Directive should not have the consequence of undermining the very privacy it seeks to protect. Many of today's communications services, including OTT, employ encryption technology. An expansion of the ePrivacy Directive would mean that these services may no longer be able to guarantee the confidentially of communication through robust encryption (e.g. end-to-end), as Art.15(1) allows Member States to restrict the confidentiality right for data retention, national security, and law enforcement purposes. These services were not designed to comply with many of the data retention and interception obligations that are now being created, but rather were designed to ensure users' the right to privacy of their communications. In fact, an extension of these obligations would fundamentally undermine the security and privacy of these services and user's ability to choose to avail of these services. We would therefore strongly recommend introducing additional safeguards to Article 15 (1) whereby any national measures cannot result in a weakening the security and integrity of the service and an explicit prohibition of any obligation that would require service providers to reverse engineer, provide back doors or implement any other measures to weaken the security/encryption of the service.

Furthermore, any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures should be explicitly prohibited.

**2. Access to and storage of information**

EDiMA does not see the need to introduce specific measures for user consent Article 5 of the ePD for the access and storage of information on information society services. In the majority of cases this involves the processing of personal data and has therefore been extensively covered by provisions under the GDPR. For cases where personal data is not involved, consumer protection and cybersecurity laws are sufficiently developed to counter any unfair practices.

Specifically, the GDPR has an expansive scope of what is to be considered personal data and related obligations, including requirements of adopting internal policies and implementing measures, which meet the principles of data protection by design and by default. Article 25 underlines that controllers shall implement appropriate technical/organisational measures for ensuring that by default only personal data necessary for each specific purpose of processing are processed. That obligation applies to the amount of personal data collected, extent of processing, period of storage and accessibility. Such measures shall ensure by default that personal data are not made accessible without an individual's intervention to an indefinite number of natural actors. In addition, the GDPR contains detailed provisions on profiling requiring individuals to be informed of the existence and consequences of profiling. It provides a robust right to object in Article 21, specifically highlighting profiling and direct marketing, stating clearly that individuals shall have the right not to be subject to a decision based on automated processing, such as profiling, which produces legal effects or similarly significantly effects the individual. These provisions provide a comprehensive protection for individuals, making any further regulation here redundant.

Finally it must be remembered that many information society services today are based on free-advertising-funded business models that keep the services free of charge for the user by allowing advertisers to show their advertisements to them. Regulation should not unduly interfere with consumers' ability to choose services they wish to use/access and businesses' ability to develop innovative business models where there is clear demand for these models. We therefore strongly caution against any suggestion that would seek to prohibit businesses conditioning access to their services to the acceptance of a cookie.

**3. Improved Harmonisation and enforcement**

EDiMA members have taken note of the lack of harmonisation and interpretation of the obligations under the ePrivacy Directive across the EU. The most obvious examples are the implementation of the breach notification requirements, the cookie rules and the definition of traffic data.

To ensure legal certainty for business and consistency for users, we would welcome a more harmonising instrument for the revised ePrivacy regime in the form of a Regulation.

As for enforcement, ultimately this entity should depend on the nature of the obligation and whether some of these obligations will be transferred to other legislative instruments. As a general point, national data protection authorities should be the sole enforcement body in regards to questions and provisions related to privacy. Anything else leads to confusion and compliance uncertainty. Therefore, EDiMA believes that the GDPR should be the primary legal regime as it provides for a robust

enforcement framework. The future consistency mechanisms created by the GDPR, particularly the One-Stop-Shop mechanism, should be sufficient to apply in a cross-border matter.

**Security obligations**

A number of other legislative instruments contain security and data breach obligations, in addition to the ePrivacy Directive. When the Commission published its proposal on the GDPR, it underlined the need to "introduce a general obligation for data controllers to notify data breaches without undue delay to both data protection authorities and the individuals concerned." The Commission noted that at that time such obligations were only compulsory in the telecommunication sector, "based on the ePrivacy Directive" [1]. It is thus clear that the GDPR obligations are actually based on the obligations of the ePrivacy Directive; as such the data breach notifications of the GDPR should prevail and any further reference to these obligations in the ePD should either be removed or mirror those of the GDPR - in order to avoid overlapping rules

The NIS Directive (A.1 (3)) also clarifies that security and notification requirements provided for in the Directive shall not apply to undertakings, which are subject to the requirements of the Framework Directive (A.13a & 13b). This provision was introduced given the overlap between the two legislative instruments, making it clear that entities falling under the scope of the NIS Directive are subject to the same legislation as those subject to the Framework Directive.

As such, it is clear that the ePrivacy Directive's security provisions are no longer needed and that there is no added value in expanding the scope of the ePrivacy Directive to ensure the security of the services.

**4. Direct Marketing**

When evaluating the provisions relevant to direct marketing, it is important to underline that the GDPR provides specific rules on direct marketing as well – it ensures a higher level of harmonisation than existed in the past. The GDPR thus also regulates any direct communications/messages sent through other means, are covered and therefore there is no regulatory gap that needs to be addressed by maintaining these provisions in the ePD.

[1] See Commission Communication of 25 January 2012, on "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century < http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en>.