EDiMA position paper on the draft Regulation on Electronic Privacy (ePR)

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). The ePrivacy Directive (ePD) has been an important instrument to foster national legislation ensuring the privacy, security and confidentiality of communications. We believe that the success of the updated framework on electronic privacy hinges on the following goals:

- To provide predictability for service providers, users, and generally contribute to a more secure communications ecosystem;
- Avoid any unnecessary burdens and strive for practical and meaningful legislation;
- Ensure consistency with other privacy, consumer or security legislation;
- Uphold the principle of technology neutrality.

Timeline

On a procedural note, legislators must take the time to properly consult and evaluate the impact of any new legislation, instead of rushing negotiations to meet an unrealistic timeline. Whilst EDiMA understands the political attraction of aligning the adoption of the ePR with the implementation of the General Data Protection Regulation (GDPR), we worry that a rushed process will not provide sufficient time to thoroughly assess the full implications of the proposal.

Once adopted, companies will also need sufficient time to implement the ePR. Adapting product and service functionality, business models, go-to-market strategy, internal processes and controls, privacy and data protection policies, customer agreements and contracts, and employee, partner and customer education does not happen overnight. The current two year transposition period under the GDPR is in itself proving to be a tough deadline to meet. It involves a determined push from our members and a significant diversion of resources from their core business.

The goal for the ePR to apply (enforced) by May 2018 is extremely worrying and against the principles of legal certainty and rule of law. The CJEU has underlined on several occasions that EU legislation 'must be certain and its application must be foreseeable by those subject to it. That requirement of legal certainty must be observed all the more strictly in the case of rules liable to entail financial consequences, in order that those concerned may know precisely the extent of the obligations which they impose on them[1].' It is hard to argue that a legislation that envisions fines of up to 4% annual worldwide turnover does not meet this threshold.

EDiMA Recommendation: There is no over-riding legal or other need to align the timeline of the implementation of the ePR with that of the GDPR. Instead, the necessary time must be taken to fully assess the impact of the proposals and ensure that the draft Regulation supports rather than hinders the DSM goals.

[1] Kingdom of Denmark v Commission of the European Communities (Case 348/85).

Improved Harmonisation and Enforcement

EDiMA welcomes the choice of a Regulation as an instrument, which will provide greater harmonisation and compatibility with the GDPR. In terms of enforcement, we welcome the proposal that the same supervisory authorities that are responsible for overseeing the GDPR should be responsible for the data protection related provisions in the proposed ePR. We also welcome the intention to follow the same consistency and cooperation procedures for cross-border cooperation.

While the cooperation procedures for the DPAs are well-established, the guidance is unclear as to who the lead authority for entities covered by the ePR will be. Under the GDPR, this is achieved through the determination of a main establishment for data controllers and data processors but no such equivalent provision exists in the context of the ePR. As such, it is not ultimately clear for electronic communication network and service providers, public directory providers, direct marketers or any other covered entities as to which supervisory authority they are responsible.

***EDiMA Recommendation*:** Ensure that the main establishment of the data controllers and processors as defined in the GDPR remains the point of reference to determine the lead-authority under the ePR as well.

Expanded Scope

It is regrettable that the Commission has decided to apply such a broad scope. We see little added value in expanding the scope to cover online communications 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 well regulated by the GDPR and existing EU consumer protection provisions which ensure a high level of protection for consumers and citizens.

The proposal also goes substantially beyond the scope of the European Electronic Communication Code (EECC), as it suggests to cover any service that has even a minor, ancillary communication feature, bringing in scope the vast majority of online activity in both the private and public sectors. This means that the Regulation would apply to a broad range of applications, including chat-enabled games, many babysitter apps, and even websites that allow users to leave comments or have help desks or click-to-call dialling capabilities. Imposing the same requirements on a minor feature as will apply to national telecoms operators and to global communication providers will likely result in many games companies either dropping or choosing not to offer communication functions to EU customers, reducing the attractiveness of their games. Under the proposed EECC, such services with only a minor communications feature will be exempt from telecom regulations. The Regulation should take the same approach.

EDiMA Recommendation: The definition of 'interpersonal communications service' in the Regulation should exclude services that enable communications as a minor ancillary feature. The same definition of ICS should be used as in the EECC.

Confidentiality of Communications (Article 5)

Confidentiality of communications is a fundamental right under Article 7 of the European Charter of Fundamental Rights. Individuals should have access to 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 such as end-to-end encrypted communication services.

The Regulation's scope should be clarified by focusing Article 5 and related provisions on unauthorised access to communications during transmission (allowing an electronic communication service to processes data to provide a requested service) and avoiding terms such as 'processing' or 'scanning'. Unlike telephone services or services used primarily for transmission such as internet access, digital communications applications need to process and store communications data in a variety of ways in order to deliver communications content onwards to its intended recipients and to provide the service and a number of the features people expect from digital communications apps, such as strong spam and malware filtering, automated inbox organisation, and other features such as assistant-type or accessibility features that rely on the processing of both electronic communication content and metadata.

The Regulation must also provide more guidance on the starting and ending points for the transmission of communications, particularly in the context of common forms of digital communications such as email and messaging. Although first introduced nearly 20 years ago, the Regulation's core rules for communications privacy can still be easily implemented by traditional telephone providers and other service providers that are primarily conduits for message transmission. However, for most online service providers, the boundaries between the sending of a message and its receipt by the intended addressee are different. Therefore, the legislation needs to make it clear that transmission ends with the service provider, not with the "end-user". In particular, restrictions on the processing of communications data should not apply to an intended recipient's service provider once the provider has received communications content – whether text, audio or video – for delivery on to its subscriber. In non-real-time communications applications such as email or messaging, transmission begins when an end-user finishes creating a message and submits the message for delivery and ends when that message is received by the intended recipient's service provider.

EDiMA Recommendation: Article 5 should be amended to make clear that 'interception' refers to unauthorised access *by people* other than the intended recipient. The rules should apply to communications in transit between the communication service providers and not to all forms of 'processing' or 'scanning' of such communications. The Regulation's articles and/or recitals should modify the meaning of 'transmission,' particularly in the context of common forms of digital communications such as email, VoIP and instant messaging.

Permitted Processing of Communications Data (Article 6)

The ePR provides an opportunity to modernise the regulatory approach to the protection of the fundamental right to the confidentiality of communications in light of technological developments. However, any updated confidentiality rule must recognise that communications services now do much more than simply transport messages: the 'Letter Carrier' has become the 'Personal Assistant'. These new communication services that act as a 'personal assistant' *require* access to a message's content (e.g. organise communications (filtering incoming messages into folders, quarantining spam

and malware)). In order to maintain the spirit of the law, while simultaneously acknowledging the changes in technology, the Regulation must clarify that there are legitimate circumstances where service providers might need to access the communications, which are stored on their systems. Below are a few examples of such legitimate circumstances.

- **Information Security:** Service providers should be able to scan, filter and ultimately process both communication content and metadata for malware, phishing and spam detection and to fight other forms of abuse of their networks, services and users, where appropriate. In addition, deployment of scanning to detect known criminal content such as child abuse images should not be precluded. Businesses have a legitimate interest in protecting people who use their services from harm and 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.

***EDiMA Recommendation*:** In order to ensure a sufficient level of legal certainty on the lawfulness of data processing, it is essential that the grounds for processing under the proposed ePR are brought in line with the GDPR. We would therefore recommend that the processing of communication data is permitted on the same basis as the processing of personal data under Article 6 (1) GDPR.

While we agree with the Article 29 working party that a "household exception"[2] could be beneficial, it is important to recognise that Recital 18 of the GDPR suggest that such exception does not apply to service providers. Therefore, it is important to insert an exemption that recognises that processing is necessary for the provision of the service should be allowed in addition to the proposed household exception.

Consent (Article 6, 8 and 9)

Since the adoption and revision of the ePD, 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 ePD 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 personal 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.

For instance, 'legitimate interest' is a ground that justifies data processing as long as those interests are not in conflict with the interests and fundamental rights and freedoms of the user. While under the GDPR 'legitimate interest' is a flexible and non-prescriptive basis for processing, it is currently

[2] http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

absent in the proposed regulation.

By only recognising consent as the way of legitimising processing of personal data, the proposal takes away carefully negotiated and much needed flexibility that ensure that users' consent is only solicited, when it is truly necessary and meaningful. EDiMA fears that an overreliance on consent will have a negative effect on privacy: according to research, when people are repeatedly requested to provide consent, they learn not to pay proper attention to request for consent, clicking them away without reading them, thereby devaluing the use of consent as a mechanism.[3]

EDiMA Recommendation: Consent as the main – almost only - ground to process data should be reconsidered. The grounds for processing should be put in line with Article 6 of the GDPR by allowing, for instance, "legitimate interest", "contractual necessity" as a ground that justifies data processing under article 8 ePR.

Privacy Settings (Article 9 and 10)

Choice, transparency, and control, are crucial elements for user privacy. We welcome the reinforcement of the principle outlined in the GDPR, that relevant settings may be an appropriate way for users to express their choice (Article 9 (2)).

Providers of software placed on the market permitting electronic communications can have the opportunity to build in and present their users with specific privacy settings and provide the individual with choices according to their preferences, including those that are more privacy friendly.

However, we are concerned about the prescriptive nature of Article 10 and the corresponding recitals that were drafted with the current state of the technology of one single software, i.e. browsers, in mind. They also make strong assertions on the best ways and at which time such products should engage with their users, which limits companies' freedom to innovate and develop the most efficient way to interact with people. Both these aspects are in clear contradiction with the currently explicit stated objective of the ePD, i.e. technology neutrality. Codifying in law currently available settings of one single product is also anything but future proof.

We fear that the overly prescriptive nature of Article 9 (3) risks creating "notification fatigue" among users, which paradoxically undermines their ability to make informed choices. Therefore, Article 9 (3) should be deleted.

Article 10 (2) and the corresponding recitals are overly prescriptive in how a vast range of software may engage with their users, which significantly diminishes the Regulation's chances of standing the test of time. Finally, while we share the view that software developers should be encouraged (but not obliged) to provide their users with meaningful privacy settings, Article 10 (1) – as a standalone obligation and not explicitly aligned with Article 8 or 9 – raises a lot of questions as to what this means in practice.

EDiMA Recommendation: We recommend that articles 9 and 10 are modified with the aim of avoiding any "notification fatigue" that could have adverse consequences like deteriorating consumer experience. We would thus recommend removing Article 10 (3) and the corresponding recitals as these are overly prescriptive and fail to be future proof and technology neutral. We furthermore recommend that Article 10 (1) is connected to Articles 8 and 9, as this standalone

[3] See, e.g. Lorrie Faith Cranor et al., "A design space for effective privacy notices," Symposium on Usable Privacy and Security, Ottawa, Canada (July 2015).

obligation creates uncertainty on its practical implications.

Access for Law Enforcement (Article 11)

EDiMA's members provide platforms and services for billions of users across the world. Security and privacy are therefore integral elements in building and maintaining the trust of our users. Article 11 raises significant concerns when applied to cross border communications services in particular, which may paradoxically undermine the very privacy it seeks to protect.

Firstly, the application of Article 11 would allow Member States to restrict the confidentiality right via data retention, national security, and law enforcement purposes and many other circumstances currently not allowed by the ePD. In practice this could mean a potentially broad range of measures which undermine the confidentiality of communications could be introduced at national level, such as restrictions on the ability of services to deliver products and services with robust, end-to-end encryption. These secure services were designed to ensure users the right to privacy of their communications and to meet other EU legal obligations including the security obligations in the GDPR and the Network and Information Security (NIS) Directive. This Article must include safeguards, at a minimum, in line with the recommendations of the Article 29 Working Party, to explicitly prohibit any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures.

Furthermore, we strongly encourage the inclusion of procedural safeguards that would ensure at a minimum that any law enforcement request to access users' data is limited to people implicated in the crime; that the data is proportionate and necessary for the investigation in question; and finally, requests are based on a "reasoned" request backed by a court or independent authority. Authorities should also be obliged to notify users about such requests and companies should be also allowed to do so.

Secondly, as the expanded scope of the Regulation means that online services will be subject to these obligations, there is some uncertainty about how to handle some cross-border law enforcement requests, such as for real-time interception and stored data. Unlike traditional telecom operators, online providers are often established in one market and offer their services cross-border to numerous EU markets. The obligation to disclose data to law enforcement authorities in any member state may conflict with company structures which establish the data controlling entity in a particular member state or trigger conflicts of law that impair criminal investigations and put businesses in difficult situations where they have to comply with incompatible requirements from different jurisdictions. While the Regulation suggests that a communications provider established in only one Member State must respond to data access requests from law enforcements from any other 27 Member States, it should be clarified that requests for lawful interception of communications across national borders remain governed by existing mutual assistance arrangements and the European investigation Order.

EDiMA Recommendation: Cross-border mechanisms such as the European Investigation Order, mutual legal assistance treaties and other diplomatic channels should be respected and further developed to respect providers' controllership and provide mechanisms for agencies in one member state to lawfully request access to user data controlled under the law of another. Further, online communications service providers shall not be required to provide technical assistance for real-time access to communications in conflict with the jurisdiction under which user data is protected and the ePR should make it clear that security measures, such as encryption, shall not be undermined or

conflict with providers' obligations under the GDPR to keep user data secure.

Security Obligations (Article 17)

We welcome the decision to streamline and align the security requirements with those of the GDPR. However, the remaining provisions on providing transparency of risks to end-users sets the threshold for notification extremely and unreasonably low, given network threat monitoring services see billions of security events daily.

Article 17 of the ePR provides for an obligation to inform end-users about 'a particular risk' that 'may' compromise the security of networks and electronic communication services. This requirement is unclear as the nature of the risk to be notified is not adequately defined. There is no significance or seriousness threshold. It is not only duplicative of data breach notification requirements under the GDPR, security incident reporting requirements under the ECC and incident reporting requirements for Digital Service Providers under the NIS Directive, but does not contain the equivalent thresholds and safeguards to ensure only relevant information is provided.

EDiMA Recommendation: The security risk notification requirement in Article 17 should be deleted. If there is any need at all to provide for security obligations in yet another legislative instrument, this should be done by a simple reference to Article 32 of the GDPR.