AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

The Proposal for a Regulation on Privacy and Electronic Communications (E-Privacy Proposal)

Promoting the European data economy: striking the right balance between privacy and innovation

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Contents

Executive summary

The E-Privacy Proposal (EPR) risks to severely limit the potential of a data-driven digital economy, a key objective of the Digital Single Market (DSM) strategy. If the draft proposal is maintained, full alignment with the General Data Protection Regulation (GPDR) and other existing or upcoming legislation, such as the European Electronic Communications Code (Code) should be ensured. With this in mind, AmCham EU issues a number of recommendations:

- On the scope, the EPR should remain as closely aligned with the Code as possible. AmCham EU suggests not to include services based on ancillary features and ensure that machine-to-machine (M2M) services are excluded. Furthermore, in line with the intent of the Code, the EPR should clarify that it applies mainly to consumers and micro and small businesses if they so request. Finally, the EPR should define rules only for devices that were placed on the market in the EU.

- The EPR should clearly identify the minimum principles and safeguards of due process that should be respected by national legislations on law enforcement access to electronic communications data. Furthermore, any law enforcement access requirements cannot undermine the security and resilience of services.

- On confidentiality, there is no clear reason why processing of electronic communications should be prohibited or severely limited under the EPR. The processing of electronic communication data should be allowed under the same condition as personal data under Article 6 of the GDPR. The scope of Articles 5 and 6 should be narrowed to focus on the interception of communications by parties other than the ECS provider and authorised third-party partners.

- On consent for permitted processing, the EPR must refrain from redefining basic concepts of the GDPR. If consent is required, the robust criteria established in the GDPR shall suffice. Additional requirements turning consent into a 'consent +++' as outlined in Article 6 of the proposal should not be introduced.

- Storage and erasure are already adequately addressed by existing GDPR principles of purpose specificity, data minimisation, storage limitation. The GDPR also provides for the right of erasure. Thus, the EPR does not need to introduce additional requirements or restrictions on these specific points. Article 7 unnecessarily increases obstacles to data-centric services and should therefore be deleted.

- The rules on terminal equipment, consent and privacy settings are in direct conflict with the GDPR and need significant revision. By targeting methodologies used in specific products and suggesting reoccurring notifications, the proposed rules are neither truly technology-neutral nor future-proof. What has so far been known as the 'cookie rule' effectively applies to all types of data that relate to end-users' devices – hence covering virtually all types of processing operations in the modern world.

- On security requirements, the EPR now requires ECSs under Art. 17 to inform end-users of security risks that 'may compromise the security of networks and services'. This is very broad and needs to be further clarified to avoid misinterpretations. The approach in the GDPR is more reasonable and therefore the article should be deleted.

Introduction

The trust and confidence of consumers and businesses in digital services is key for the success of the DSM strategy. However, as AmCham EU members have stated previously[1], the proposal for an e-Privacy Regulation does not reach this objective and questions the achievement of a Digital Single Market as a priority for Europe.

European consumers need to be adequately protected in line with new technology developments. However, we are concerned that the proposed approach severely limits the potential of a data-driven digital economy, due to duplication and overlap with existing regulations. The proposal fails to provide a framework that will allow companies to innovate, notably in M2M services, Internet of Things (IoT) and Artificial Intelligence (AI).

The ePrivacy Directive (EPD) and the EPR cover provisions that are either already governed by existing instruments[2], instruments in a draft form[3], that have become irrelevant[4], or would be more adequately addressed through other means.

As a principle, sector-specific regulation should only be introduced or maintained where necessary and proportionate. It should be also given due time to be adequately implemented.

Notwithstanding our firm view that there is limited scope for continued legislation in this area, this paper includes constructive input regarding the substance of the EPR, including general comments (1) and comments on specific articles (2).

[1] See the AmCham EU response to the public consultation on the evaluation and review of the ePrivacy Directive, here.

[2] General Data Protection Regulation (GDPR), the Directive on security of network and information systems (NIS Directive)

[3] The telecoms package, the draft European Electronic Communications Code ('the Code')

[4] Connected Line Identification, directories etc.

General comments

The approach to protect users from communication instead of ensuring the confidentiality of communications poses a major departure from the status quo and is unwarranted.

Pursuant to the draft Code, the EPR is ambiguous with regards to M2M services (connectivity vs. service). Although it recognises that not all M2M services are electronic communications services (ECS), it still concludes all should be covered without a sufficiently robust basis. The scope must be defined more clearly, or this could be very problematic for the development of newer technologies and the uptake of IoT.

If the draft is maintained, the review of the ePrivacy Directive should be an opportunity to ensure full alignment with the GPDR. We note attempts have been made to ensure consistency (e.g. removing breach notification requirements). However, this attempt is somewhat limited, inconsistent and does not go far enough (consent/legitimate interest, direct marketing provisions, extra security provisions implied with informing on detected security risks etc.).

In terms of the timeframe, a quality output must be ensured, regardless of political considerations. Business needs an adequate timeframe to implement this regulation, as it may require significant changes to business models. It is essential that companies are given at least 18 months to prepare for enforcement of new requirements. Any proposal that suggests immediate enforcement is in breach with the principles of legal certainty, predictability and reasonable time to prepare required by the Court of Justice of the European Union (CJEU). Priority should be given to ensuring the regulation guarantees the necessary privacy protections that are not addressed by the GDPR (if any), whilst providing a framework that enables innovation and investment to make the DSM a success.

We acknowledge some positive elements:

- AmCham EU welcomes the choice of legal instrument - a regulation - which should bring further harmonisation as opposed to the experience so far with the EPD. This is particularly important to companies who operate across multiple EU markets.

- The designation of one competent authority also alleviates some of the complexities around the dual regime. A one-stop-shop/lead competent authority approach will lead to further harmonisation. In this case, reporting lines on GDPR and EPR should be aligned.

- In stating as a key objective the free movement of electronic communications data, the EPR rightly recognises the need for intra-EU data flows. The emergence of data-centric services is essential for both society and the economy.

Comments on articles

Scope

Ancillary & M2M services (Articles 2, 3, 4 and Recitals 11 & 12)

The EPR copies the already broad and ambiguous definition of ECS included in the draft Electronic Communications Code and goes beyond it without valid justification. It fails to adopt the interpretative guidance of the term 'ECS' as understood in the Code with regard to interactive interpersonal communications services (e.g. video on demand, websites, social networks, blogs, or exchange of information between machines) which should not be equated to communications services. Further, the draft includes a 'catch-all' clause (minor ancillary service) that captures any services (even minor) linked to an ECS service and also includes terminal equipment. Existing privacy and security legislation already covers such services. We fail to understand why they need further protection under the EPR.

Similarly to the draft Code, the EPR is ambiguous about M2M services (connectivity/transmission vs. service). Recital 12 suggests that the EPR should apply to M2M communications. The Commission believes the applicability should be limited to 'transmission only'. However, we would like to recall that recital 15 of the proposal suggests that transmission lasts 'until the receipt of the content of the electronic communication by the intended addressee'. This suggests not by the service provider at the end of the network, but the end-user. This broad interpretation of transmission pulls in all services in the scope, including M2M ones. This could mean that various nascent and diverse technologies, essential to the development of a meaningful data-driven economy will be covered by the legislation. An overly prescriptive approach is likely to stifle the development of data technology in a way that will undermine its potential benefits for the economy and society.

Including all M2M communications and applying provisions as currently worded will lead to impractical situations. Given that the EPR would apply (in contrast with Article 3 of the EPD) to non-personal as well as personal data, the new ePrivacy rules could capture data such as soil acidity or air humidity in a farmer's field and subject it to requirements that are obviously irrelevant to such information flows.

An M2M environment does not always have obvious end-users to provide consent. This would make it impossible to process data for analytical purposes and render the connection of devices meaningless. Restricting the data processing in the M2M environment to only one legal basis (i.e. consent) is unworkable, as well as unjustified and unnecessary on privacy grounds. Instead, the GDPR applies to M2M data which is personal data, providing robust privacy protections, flexible rules for the use of data, and a consistent framework.

Therefore, AmCham EU suggests not to include in the scope services based on ancillary features and ensure that M2M services are excluded. The EPR should remain as closely aligned with the Code as possible.

End-user definition (Article 2)

In line with the intent of the Code, the EPR should clarify that it applies mainly to consumers and micro and small businesses if they so request. It should not apply to enterprise services which, due to the nature of their contracts and services, don't require the same protection.

Territorial scope (Article 3)

The EPR would apply to any device or terminal equipment located in the EU. This means that anybody who visits Europe and brings a device would expose its manufacturer to sanctions and liability. This cannot be the legislative intention. The EPR should define rules only for devices that were placed on the market in the EU.

It is also unclear what the 'use of a service' entails. Such ambiguous reference points are not satisfactory to define jurisdiction and should be deleted.

Finally, the EPR should also make it clear that (pursuant to Recital 23 of the GDPR) the mere accessibility of a service is insufficient to ascertain jurisdiction.

Law enforcement access requirements (Articles 2.2 & 11.1)

AmCham EU regrets the broad and substantial caveats included in the proposal such as the flexibility granted to Member States to restrict the protections afforded by the EPR. This contradicts the European Commission's objective of harmonisation. The Commission suggests to extend the scope of circumstances under which confidentiality could be disregarded from the traditional law enforcement purposes. It proposes that Member States can disregard this principle in case of monetary, budgetary, taxation and social security matters (Article 23 (e) of the GDPR). Of even more concern is the requirement (article 11.2) for market operators to put in place dedicated policies to serve such restrictions regardless of how fragmented and disharmonious they may be across the Member States.

This is indeed a matter where Member States' national competence cannot be overlooked and must be accommodated. However, in order to provide legal certainty and guarantee privacy as effectively as possible, and in the interest of the DSM, the EPR should clearly identify the minimum principles and safeguards of due process that national legislations on law enforcement access to electronic communications data should respect.

Accordingly, any access request should be:

- based on law;
- limited to what is strictly necessary for the investigation in question;
- focus on data of individuals impacted in the crime;
- be reasoned and subject to review and decision by a court or an independent authorities.

Notifications to users should also be allowed, in line with the Court of Justice of the European Union's (CJEU) jurisprudence.

On top of asserting Europe's values and providing end-users as well as ECS providers with unquestionable legal protections, such a common baseline can help minimise market fragmentation and prevent the kind of legal uncertainty and protracted litigation that have resulted from the former data retention directive and from its annulment in court.

Finally, any law enforcement access requirements cannot undermine the security and resilience of services. Any mandate that requires reverse engineering, back doors and other measures that weaken security/encryption measures should be explicitly prohibited.

Confidentiality of communications (Articles 5 & 6)

Confidentiality is an essential principle for any democratic society. However, the language in the proposal has been broadly extended to any processing of electronic communications data. There is no clear reason why processing of electronic communications should be prohibited or severely limited under the EPR, as it should also be comprehensively covered by the GDPR and in other existing instruments (EU Charter of Fundamental Rights, national constitutions etc.).

Moreover, the concept of confidentiality in the EPR – which presumes that users of online services do not expect processing of their communications beyond mere transmission – is out of step with the reality of ECS nowadays. Many people choose to use email and messaging services because the providers offer smart services (like spam filtering, fraud detection, scheduling, and organisation tools) that rely on the automated processing of

communications while they are occurring. The provision of these services does not constitute a breach of confidentiality, rather users expect these actions and the demand for them is increasing.

The principle of confidentiality should apply to all communication beyond digital services and it should take into consideration and not hamper the stakeholders from collecting and using data where required. Such uses would include for example, fulfilling legal obligations, preventing illegal actions, ensuring security and protecting trade secrets in line with the jurisprudence of the Court of Justice of the European Union.

Therefore, the processing of electronic communication data should be allowed under the same condition as personal data. All the legal basis for processing, as outlined in Article 6 of the GDPR, should also be available to electronic communication data. The scope of Articles 5 and 6 should be narrowed to focus on the interception of communications by parties other than the ECS provider, and authorised third-party partners.

Consent rules for permitted processing (Article 6)

The EPR proposal includes data processing rules that go beyond the already robust GDPR rules which recognises that valuable insights can be gained from data when responsible companies use proper safeguards. While the risk-based approach in the GDPR provides the necessary flexibility to justify data processing in situations where relying on the consent of the user is not appropriate, the EPR requires consent for nearly all processing.

This failure to recognize additional legal bases for processing data, along with the failure to incorporate the GDPR's concept of further processing for compatible data uses, will limit companies' ability to innovate particularly for business models that rely on secondary uses of data that may not be foreseeable when the data are initially processed. Far from advancing the cause of user privacy, this restrictive approach will likely lead to the kind of notice fatigue that characterises the cookie banners that the EPR tries to address. The consent-only model is limited in a small or no-screen environment, where it is not only impractical, but also dangerous to users (e.g. asking consent while driving).

This approach also makes it difficult to see how third parties would now be able to obtain consent, as opposed to the current Directive, which includes provisions to that effect (EPD 6(5), 9(1) and (3)). We fail to understand why that was removed from the draft EPR. In addition, this omission is also inconsistent with the practical realities of providing communications services using vendors and other third-party contractors to perform essential functions, analytics, and value-added services. It is also inconsistent with the GDPR, which establishes the responsibility of data controllers and processors.

Furthermore, we note that there is a contradiction between 6(1) and 6(3) due to the inclusion of 'only' in 6(3). Therefore, the world 'only' should be deleted. The consent requirement may be problematic in cyber-security investigations. For example, there may be a need to monitor suspicious networks for fraudulent activity. These networks need to be tracked to obtain information on the 'dealer'. Requiring consent, thereby giving the individual(s) in question a warning and a 'veto-right' defeats the purpose of the investigation, unless the 'security' purpose authorising the processing in section 6.1(b) would explicitly broaden the scope of the purpose of the communication services. In this way, it does not just allow the processing for technical reasons if there is a fault, but also for the actual purpose of the service, which could be to provide a secure service to avoid any suspicious cyber activity.

The EPR must refrain from redefining basic concepts of the GDPR. If consent is required, the robust criteria established in the GDPR shall suffice. Additional requirements turning consent into a 'consent +++' as outlined in Article 6 of the proposal should not be introduced. As the European Data Protection Supervisor (EDPS) suggested, 'the strict conditions under which a processing can take place are already set down in the GDPR and do not require amendment or addition'.

We also have serious concerns regarding the concept of 'all party' consent. It is clear that companies can only obtain consent from their own users. Furthermore, many of the communication today is automated (like an automated booking confirmation), which raise important questions on how consent may be obtained. This is why we strongly recommend finding another legal basis for processing communication data fully in line with Article 6 of the GDPR.

Storage and erasure rules (Article 7)

Storage and erasure of data should be context-based to reflect different users' expectations for different types of services (e.g. some users want communication deleted upon receipt by default). The one-size-fits-all approach proposed in the EPR is not in line with market realities and consumer expectations. The GDPR principles on purpose specificity, data minimisation and storage limitation already address this matter adequately. The GDPR also provides for the right of erasure. Thus, the EPR does not need to introduce additional requirements or restrictions on these specific points.

These severe restrictions fail to recognise that many services rely on the need to store data for research and development purposes. The essence of data-driven services is that they use data in order to improve user experience and develop novel, innovative offerings. In today's digital economy, consumers do not sign up for a service and assume it will never change. In fact, people expect that the more they use a service, the better it will respond to their needs. This emerging expectation stems from providers' ability to analyse data generated by users to identify bugs to fix, features to improve, eliminate or develop. This requires the service to store data about how people are using the service. Article 7 will make it significantly more difficult and add to the number of consents that data-driven services will need to seek from users.

Terminal equipment, consent and privacy settings (Articles 8, 9, 10)

These articles do not align with the Commission's objective to improve the rules on cookies where consumers are overburdened by consent requests without being in control. By targeting methodologies used in specific products and suggesting reoccurring notifications, the proposed rules are neither truly technology-neutral nor future-proof. What has so far been known as the 'cookie rule' effectively applies not only to cookies but to all types of data that relate to end-users' devices – hence covering virtually all types of processing operations in the modern world.

Indeed, these rules significantly overlap and directly conflict with GDPR provisions. Without significant revision, we believe they will have negative consequences for third-party services (e.g., ad serving and measurement) that many websites and app developers rely on to monetise their services. This will limit consumers' access to free content and diminish the diversity of voices and perspectives online.

Some opinions on the draft Regulation state that it necessary to prevent so-called tracking walls, which require people to provide consent to third-party data processing and the use of cookies as a condition for using a service. Many online content providers – particularly smaller ones - rely on third parties (and technologies such as cookies used by third parties) to monetise their services through advertising. Indeed advertising still is, next to subscriptions, a key source of revenue for companies. If on-line players cannot make access to their sites subject to users accepting ads and the data processing required to deliver, count and pay for those ads, the proposal would cause unprecedented interference with the Freedom of Expression. Preventing publishers from working with third parties would mean jeopardising certain business models overall and undermining freedom to do business.

Additionally, the 'cookie rule' as drafted will also have considerable negative impacts on the evolution of electronic communications as we move towards the IoT and 5G, which will increasingly rely on technical information about the performance of devices to ensure security and quality of service. Requiring consent for such non-invasive types of processing would stand in contradiction with the GDPR, where they would be allowed under other legal bases, without increasing end-user privacy.

Processing of terminal equipment data (Article 8)

To the extent the Commission aims at regulating data produced by and accessing data on the device, the legal bases should be brought fully in line with those of the GDPR. To the extent that terminal equipment data makes it possible to identify end-users (i.e., if it is personal data, which may not always be the case, see our example on M2M above), it is already covered by the GDPR. Furthermore, creating a separate set of more limited legal bases, with the assumption that terminal equipment data is 'sensitive' data and requires heightened protection (whereas it may not even constitute personal data in the first place), directly contradicts the GDPR.

The same degree of flexibility allowed under the GDPR should be allowed under the EPR. This will enable innovating and data-driven business models to emerge while guaranteeing a robust level of protection (e.g. in the IoT space). It also deserves special consideration in light of the ongoing advances in wireless connectivity and location technologies, which will make processing of terminal equipment data more central to electronic communications as a whole.

As with Article 6, we have difficulties understanding if Article 8(1) is an additional layer to GDPR or mandates consent for activities that in certain cases would rely on legitimate interest or other legal bases. There is no hierarchy of legal grounds for processing data. Considering consent as a 'better legal ground' undermines the warning function of a consent provision: ensure that we think twice before consenting.

Online audience measurement is a practice which provides metrics across the industry to shed light into otherwise dark markets. The obligation for online operators to request explicit consent for placing cookies for such activities where they do not conduct this themselves is overly strict, and should be amended to exclude any audience measurement and not only 'web audience measuring' carried out by a website's operator itself (excluding even a processor acting on behalf of that operator).

Consent (Article 9)

The EPR aims at enabling users to express their consent through the appropriate settings of software applications (Article 9(2)). We welcome the intention to make the clarification outlined in Recital 32 of the GDPR clearer and prominent in the EPR. In some circumstances, settings should indeed be an option. Nevertheless, we doubt that Article 9(2) would be able to compensate for the consent-only approach promoted by the Regulation. Contrary to the stated intent, cookie banners will continue to proliferate as the only mechanism capable of meeting the GDPR's detailed notice requirements.

Furthermore, we welcome the recognition that the current approach to cookies 'resulted in an overload of consent requests for internet users', however the new approach is unlikely to deliver a better outcome. Unlike the current regime, the reference to the GDPR will require users to consent to each cookie individually, as it would also make websites (co-)liable for any non-compliance by a third party.

Furthermore, we are extremely concerned about the obligation to remind end-users every 6 months about the possibility to withdraw their consent (9.3). As people start using new services and visit new websites on a daily basis, this suggestion will simply mean that new waves of notification will start every day at 6 month intervals. We believe that offering the possibility to opt out via a link or website would fulfil the purpose of this article. If the current banners are deemed annoying today, let's imagine how such reminders will be received in the future.

Providers should be permitted to make access to their services subject to users consenting to data processing, including for online advertising. Anything else results de facto in an expropriation and unwarranted infringement of the Freedom of Expression and Information and Freedom to Conduct a Business. A more effective manner to protect users and to increase trust would be for the public sector to raise their awareness through education and information campaigns.

Information and options for software privacy settings (Article 10)

This provision could result in a fundamental system architecture change. It requires each and every piece of software on an end-user device to provide options that might block any third party communication.

This is applicable to everything from web browsers to operating systems and any relevant piece of software in any device (terminal equipment) from hardware drivers to mobile applications. Users will be overburdened, conflicts will occur that will confuse them and require the software designers to go for a strict implementation. Given the draconian penalties, they will opt to block any communication in case of conflicts or risks that a request might be a third party communication. The impact goes far beyond cookies. It will affect individual companies' ability to differentiate from competitors by offering a more privacy-friendly relationship – the browser settings will, in all likelihood, treat all sites the same, removing any incentive to offer innovative ways of engaging and communicating with consumers.

The proposal also breaches the technology neutrality principle by privileging business models where the software manufacturer qualifies as a first party and therefore not subject to the restrictions in Art. 10.

The provision makes a differentiation between first and third party on a technical level. It ignores that a technical third party can legally be a data processor as per GDPR and should receive the same treatment as a first party, as it acts on behalf of a data controller who is a first party. The obligation for software manufacturers to inform users about risky processing also shifts an unprecedented level of liability upon them: how shall for instance a browser manufacturer know what risky processing can take place with data collected by another company?

We support meaningful browser settings citizens can understand (and as such the option to provide consent through settings as outlined in the GDPR and Article 9(2) of the proposal). However, browsers, mobile operating systems and apps already provide a number of adequate and user friendly privacy options. The provisions on software settings address the collection and use of data as a result of using the software. The GDPR already contains extensive rules designed to tackle this matter, namely those on lawful processing, privacy by design, privacy by default, and decisions based on automated processing including profiling. In fact the GDPR expressly calls out the use of tracking and monitoring as being part of the specific data processing practices it seeks to regulate.

While we believe Article 10 was well intended, the requirements in EPR would not create a different or even better privacy result for users. In fact they will only burden businesses. The requirements to explain the risks of third-party data collection and to prompt the end-user to choose whether to allow this collection and the use of storage will disrupt the core activities of third-party providers that enable websites and apps to monetise through advertising.

AmCham EU supports meaningful privacy settings, but believes that companies must have the flexibility to design them in a way that makes sense for their users. This is a manner that allows them to create a direct and trusted relationship, and conveys the benefits that third-party data processing provides (e.g., access to free online content). Regulators should define objectives and in this case, make sure that users are in control, but not prescribe the best way to achieve those objectives. For all the reasons above, this article should be deleted.

Connected Line Identification (CLI), Incoming call blocking, Directories (Articles 12, 13, 14, 15)

Considering the evolution of technology and of business models and practices we question whether these provisions are still necessary today. They relate to commercial practices and consumer protection rather than privacy or security. If they remain relevant, they would be better addressed under the telecoms regulatory framework, specifically the Citizens Rights Directive.

Unsolicited communications (Article 16)

We are concerned that the EPR provisions contradict the GDPR. While the Regulation requires consent for direct marketing, the GDPR recognises a number of legal bases for the same activity, including legitimate interests. In fact, the GDPR calls out direct marketing as an example of a practice that should generally be regarded as within a company's legitimate interests.

Security requirements (Article 17)

We welcome the attempt to streamline security requirements and the suggestion to delete the requirements of Article 4 under the current EPD. The current e-Privacy directive contains the same language under Article 4 paragraph 2, however this is now outdated. Most relevant security risks and incidents are now likely to be covered under one of the following legislations: either under the Network and Information Security (NIS) Directive's provisions on incident reporting, the similar requirements of the eIDAS Regulation for certain services, the GDPR's provisions on data breach notification, or the new Electronic Communications Code currently under discussion.

However, the EPR now requires ECSs under Art. 17 to inform end-users of security risks that 'may compromise the security of networks and services'. This is very broad and needs to be further clarified to avoid misinterpretations. If the aim of the article is to raise awareness about possible security risks we believe there are other more effective ways of achieving this. For example, there may be countless cyber-attacks occurring regularly, and many services counter these on a daily (or even hourly) basis. Informing users of each one could lead to a large amount of notifications, and possibly a loss of focus on the issue.

Reporting all risks and incidents can actually lead to an overburdening of scarce resources and is counterproductive. In fact, any number of services are today exposed to cyberattacks. According to the Commission at least 80% of European companies have experienced at least one security incident in 2015. This raises questions on what should the user actually be notified about. The approach taken by the GDPR is much more reasonable and therefore Article 17 in the EPR proposal should be deleted.

Remedies (Article 21) and sanctions (Article 23)

Although we welcome in general alignment with the GDPR, in this case we would question the proportionality of such fines. More importantly it must be ensured that such fines only apply once and are not cumulative under both instruments. We also note that Article 80 of the GDPR already puts forward rules regarding the representation of data subjects in case of infringement of the legislation. It is unclear why the EPR needs to propose a new set of rules in this area.