DIGITALEUROPE

DIGITALEUROPE's initial views on the European Commission's proposal for an ePrivacy Regulation

Brussels, 3 April 2017

EXECUTIVE SUMMARY

DIGITALEUROPE, as the voice of the digital technology industry in Europe, welcomes the opportunity to provide its initial views on the recently proposed draft ePrivacy Regulation ("ePR"). We regret that the European Commission has not followed the 'Better Regulation principle', largely ignored the contributions from industry and missed an opportunity to streamline data privacy rules in Europe. We wish to reiterate that the General Data Protection Regulation ("GDPR") already provides for a high level of protection of users' personal data, and addresses the vast majority of the issues that the proposed ePR seeks to cover. Ensuring coherence between these two legal instruments will be essential. The new ePR should not undermine legal certainty by interpreting provisions in the GDPR.

DIGITALEUROPE believes that the prohibitive and unworkable approach put forward in the draft also risks seriously undermining the development of Europe's digital economy and will likely to lead to yet greater confusion, legal fragmentation, and overly-restrictive rules rather than creating a level playing field. As such we would like to bring to the attention of the co-legislators the following issue-specific points:

- Scope – The ePR captures a disproportionately broad range of services. It should avoid to become a 'catch-all' legislation. We encourage exclusion from the scope of those services with only ancillary communications features and of M2M communications to bring the legislation in line with the Electronic Communications Code. We also welcome further clarification around the exclusion of closed user groups.

- Confidentiality – The introduction of extreme limitations on the processing of communications data goes beyond what is necessary to ensure the fundamental right to confidentiality and ignores the technological reality of how communications services work today. The ePR should protect the confidentiality of communication, not protect people against communication.

- Consent - The ePR must provide additional flexibility for the use of communications data through a greater reliance on legal basis' for processing other than end-user consent, such as 'legitimate interest'. It is unclear from whom consent needs to be obtained and who is responsible for obtaining it.

- Terminal Equipment – The ePR places special restrictions on the processing of terminal equipment data and ignores the central role that such data plays in ensuring pertinence, quality of service, and quality of experience for end-users. We encourage aligning the ePR as much as possible with the legal bases and provisions of the GDPR (e.g. legitimate interest)

- Connection Data – Data required to connect devices to a network should be a standalone category and should be subject to the same rules for lawfulness of processing as those outlined in the GDPR.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

- Law Enforcement Access to Data – The ePR provides for significantly more opportunities for law enforcement authorities to request data as it expands on the type of data they can request, the range of providers that have to respond and the list of circumstances where law enforcement can disregard confidentiality requirements. More privacy safeguards must be introduced, based on the recent jurisprudence of the CJEU.

- Timeline – Co-legislators must take the time to properly consult and evaluate the impact of the ePR instead of rushing negotiations to meet an unrealistic timeline. Furthermore, and in line with the established jurisprudence of the CJEU and the principles of legal certainty, the ePR cannot apply the same day as it enters into force. It is impractical to expect that data controllers, who already devote significant time and effort to comply with the new requirements introduced by the GDPR, can somehow also devote resources to complying within the same timeline to requirements that are only in draft form. Especially that this new proposal comes just 14 months before they are expected to comply. This timeline completely ignores the reality of software and hardware development which takes place over a far longer schedule.

OVERALL VIEWS

The ePR will have far reaching effects on how electronic communications and many online services operate in the EU. The Regulation will extend obligations that are significantly more stringent than what currently apply to telecom operators to all over-the-top ("OTT") communications services, machine-to-machine ("M2M") applications, and content services with communications capability such as video games, dating apps and e-commerce sites with built-in chat features. It will also require browsers, mobile apps and many other types of software enabling electronic communications to obtain end-users' opt-in consent upon installation, effectively disregarding other legal bases for data processing. Such a wide extension of both scope and the nature of the obligations will have a significant impact on all industry sectors relying on data driven innovation.

While we recognise the importance of the confidentiality of communications as a component of the right to respect for one's private and family life, it is not clear what is so specific about the sectors covered by this Regulation that requires a standalone instrument independent from the horizontally applicable GDPR. The GDPR includes both an explicit 'integrity and confidentiality' principle and implicit confidentiality protections in the grounds for processing personal data. Moreover, the GDPR is technology and sector neutral, determines safeguards and requirements according to the risk presented and makes a specific distinction for high-risk data. Other sectors are arguably processing more sensitive data – such as healthcare or finance – but are quite rightly determined to be sufficiently covered by the general framework.

We would also like to recall that the Charter of Fundamental right treats the right to privacy and the protection of personal data and the right to the confidentiality of communication as equally important rights. It is thus unclear why the protections afforded by the GDPR are considered insufficient and require a significant rewrite in the ePR proposal.

We believe the proposed ePR should be withdrawn and the current ePrivacy Directive ("ePD") be repealed.

SPECIFIC CONCERNS

1. Scope (Article 2)

DIGITALEUROPE remains concerned that the ePR captures a disproportionately broad range of services. The draft proposal suggests an extension of the rules in existence today, which are applicable mainly to networks that convey communications, to a wide array of services, without consideration as to whether such rules will work in practice.

a) Interpersonal communications services enabling interactive communications as an ancillary feature

DIGITALEUROPE **strongly opposes a broad extension of the scope of 'electronic communication service' that would cover any service that has a minor or ancillary communication feature**. This extension would capture thousands of applications and services that include a communications tool, such as chat-enabled games, babysitter applications and websites with help desk messaging service or 'click-to-call' dialling capabilities. The ePR should seek to align closer to the proposed European Electronic Communications Code ("ECC"), which has excluded such services and instead relies on the already high bar of protections afforded by the GDPR.

b) Closed user groups

We welcome the intention of the European Commission to exclude closed user groups and corporate networks from the scope of the ePR. However, we would like to **see this clarification anchored in the Articles** and expressed in greater detail. For example, it should be made clear whether beta or "taster" services (i.e. services that are ultimately aimed at businesses, but for which a basic version with limited functionality is essentially available for anyone to sign-up to) would fall under the closed network exemption. We also ask for clarification on what amounts to an 'undefined group of users'. Moreover, it is important to clarify that an enterprise itself does not qualify as a provider of electronic communications networks and services when allowing the use of such services (e.g. VoIP) acquired from a third party service provider by its employees (even if permitting the private use of such assets or allowing third parties to dial in). Recital 13 seems to imply this by exempting 'corporate networks'. However, the **extent of the exception remains unclear**. DIGITALEUROPE is concerned that previous interpretations of this term by national regulatory authorities have both included services offered to enterprise as a whole (as opposed to specific sectors) and considered the means of availability (e.g. purchase over the public internet) as significant as opposed to who is being targeted by the service.

Moreover, there needs to be clarity that communications that take place only over Near Field Communication (NFC) networks including Bluetooth and Wi-Fi are not within the scope of the ePR.

c) Machine-to-machine

Recital 12 suggests that the ePR should apply to M2M communications. This could mean that various products and services that contain built-in M2M communication features like automated supply chains, remote control or operation of machines might be covered by the legislation. This does not seem to be consistent with the purpose and objective of the ePR. We see the risk that the inclusion of M2M communications and applying provisions as currently worded would lead to unworkable situations in practice and render standard processes

and developments of Industry 4.0 impossible. We suggest a **clarification that products and services containing an M2M platform do not fall within the scope of the ePR**.

Today, many companies face the challenge that customers do not only request actions from their machines, but also to related platforms that connect their machines with each other ("M2M platform"). Such M2M platforms essentially consist of the following elements: (i) collection of data from the connected machines, (ii) making the data available to the customer via the platform, (iii) offering functions to analyse the data and (iv) transfer signals to operate and control the machines via the platform. The 'conveyance of signals' may partly be the focus of a service provided via the M2M platform while other services may focus on the delivery of (derived) content. **Applying the ePR to M2M platforms would lead to great uncertainty regarding the legal framework**, particularly when the GDPR offers sufficient protection for such types of data processing.

Furthermore, the development and improvement of terminal equipment by Original Equipment Manufacturers ("OEM") and the innovation of new devices, hinges on the ability of collecting information from the users 'terminal equipment'. That information is normally considered telemetry data and is generally not considered Personal Information, but covered by the proposed ePR under Article 8. The transmission of telemetry data is critical to the current deployment and development of new services and business models that have a direct benefit to the user. Moreover, **obtaining user consent via devices with limited user interface that fall under the definition of 'terminal equipment' can present an almost impossible task**. We suggest including an additional exception on paragraph 1 of Article 8 to allow OEM to collect data to ensure proper functionality of equipment, to fulfil services required by costumers (not only information society services) and to conduct research and development of new products and product improvement.

2. Confidentiality of Communications (Articles 5 and 6)

DIGITALEUROPE members fully support the confidentiality of communications as a fundamental right and agree that information exchanged between parties should not be revealed to any person other than to the parties involved in the communication. Our members put in place technical and organisational measures to ensure that this principle is implemented in practice.

a) Prohibition of processing goes beyond what is required for confidentiality

As outlined in the recitals, the essence of confidentiality is and should remain to prevent that a third person acquires knowledge about a communication between parties. We are concerned that despite this stated objective, the **ePR proposal goes beyond protecting the confidentiality of communication and instead applies an approach that de-facto prohibits the processing of data**. This is a radical change that appears to ignore the reality of how the technology actually works.

We regret that contrary to a true 'Better Regulation' approach, the draft ePR has greatly expanded the current framework on confidentiality found in the ePD, introducing a level of complexity and confusion that is unprecedented and unnecessary.

b) Modern communications services are fundamentally different than letter couriers

When considering the ePD, the rules are based on communications services that were designed with message transport services in mind. New confidentiality rules must recognise that communications services now do

much more than simply transport messages as the 'Letter Carrier' has become the 'Personal Assistant.' These services are now expected to:

- Organise communications (filtering incoming messages into folders or group them according to their sender, subject line or other criteria, quarantining spam and malware);
- Automate administrative tasks (automatic calendaring and appointment reminders);
- Integrate enhanced features (voice-to-text accessibility options for disabled users, automatic translation, error correction); and
- Respond to voice commands and new forms of interaction for access to content and control over communications features.

These features sometimes require the processing of content and metadata in transit – to the extent that transit only ends when the message is received by the end-user and not by the service provider, as indicated by the proposal. This type of processing cannot always be performed after a message is delivered to a user's inbox or terminal equipment. Where privacy rules designed for traditional message transport services prevented access by the 'letter carrier' during transmission, new communication services that act as a 'personal assistant' act differently. Some services may require access to a message's content and the corresponding metadata during transmission. **The ePR's confidentiality rules should take into account the different need for access between transport and the applications and services enabled by that transport.**

3. Consent (Articles 6 and 9)

The ePR will require consent for most processing of communications-related data. Article 6 provides only a very narrow set of exceptions for processing related to message transmission or an unclearly defined system security provision. These exceptions do not compensate for the unreasonable prohibitions and proposed consent-only approach.

a) Provisioning of 'low-risk' services

DIGITALEUROPE challenges the assumption that the processing of electronic communication content and metadata always represent a high risk to consumers. Many processing activities such as SPAM detection and displaying or printing an email are executed automatically with no individual(s) gaining knowledge of the content. Such processing activities are necessary to provide services and the features requested and in many instances expected by users. Moreover, there are legal obligations on service providers in many jurisdictions to secure user data which create a requirement to undertake such security measures.

b) From whom to obtain consent

According to the European Commission's proposal, the processing of both electronic communications metadata and electronic communications content by providers of electronic communications services can be done on the basis of consent of the end-users. Unfortunately, **as the concept of end-user includes both natural and legal persons, as well as 'all' the parties, it is not clear who the provider would need to obtain consent from, or who is responsible for obtaining the consent**.

It is not clear if a communication provider with an enterprise customer needs to obtain consent from their customer, or individuals such as the customer's employees and external users of the platform. If it is necessary to obtain the consent of the individuals in question, it is not clear whether that responsibility falls on the

communication provider or the enterprise customer who has a direct relationship with them. Moreover, it is worth noting that the enterprise customer may in any case have to obtain consent from the individuals as well, or use other legal grounds for processing such as legitimate interest or performance of contract, if the data is personal under the GDPR.

c) Limitations of anonymisation

Added confusion stems from the provision that consent can only be used as basis for processing metadata or content under certain circumstances, for example, if anonymised data cannot fulfil the same purpose. While the implication is that anonymising data removes the need to meet additional grounds for processing the data, given that anonymised metadata or content *still qualifies* as metadata or content data under the given definitions, as currently drafted the provider would still need to meet one of the grounds for processing the data in question.

d) Relationship with 'all end-users concerned'

Moreover, the processing of content data will be particularly constrained under the ePR. A provider must obtain the consent of 'all end-users concerned' for processing of content for one or more specified purposes. It is clear that **a service provider that does not have a separate relationship with the sender of a communication cannot get that second consent, particularly with email or VoIP-to-PSTN services where users are connecting through different providers.** A suggestion that such consent can be collected in Terms of Service or otherwise appears to block new entrants to the market who would not be able to secure such consent and does not meet the high bar for consent envisaged.

e) DPA consultation

If consent is required for each specific service, consumers will be asked for separate consent for each of the features mentioned above. Article 6(3)(b) also requires the provider to consult a data protection authority ("DPA") before processing, according to a consultation process set out in the GDPR. **We question whether DPAs want to review every new feature that would allow searching through messaging, which by definition requires processing the content of the communication.**

f) Impact on cybersecurity

The consent requirement may also be problematic in cyber-security investigations. For example, there may be a need to monitor suspicious networks for any fraudulent activity. These networks need to be tracked to obtain information on the 'dealer' of these networks. **Requiring consent, thereby giving the individual(s) in question a warning and in essence a 'veto-right' defeats the purpose of any such investigation, unless the 'security' purpose authorising the processing in Article 6(1)(b) would explicitly broaden the scope of the purpose of the communication services**, so 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.

g) GDPR consistency

The definitions and conditions for consent in Article 9 directly reference Articles 4(11) and 7 in the GDPR. While we welcome consistency with GDPR, this is somewhat problematic insofar as there is no equivalent of the roles of data controller, data subject or restriction of scope to personal data in the ePR. All of these concepts are intrinsic to the aforementioned Articles. As a result, it is not clear whether consent is only applicable to personal data in the ePR, who is responsible for obtaining consent or from whom.

h) Impact on technological innovation

Such consent requirements are based on the assumption that communications content processing will only take place in exceptional circumstances. This fits the old paradigm of communications as message transport services, but does not reflect the reality of the latest applications' innovative features. However, we do acknowledge that some use cases may be more sensitive than others. Therefore, **a risk-based approach as defined in the GDPR seems most appropriate.**

i) Need for additional legal bases

The GDPR also allows for the processing of data on the basis of consent but also on other grounds, such as 'legitimate interest', which allows for processing so long as those interests aren't outweighed by the interests and fundamental rights and freedoms of the user. **'Legitimate interest' is a flexible and non-prescriptive basis for processing and can provide a higher standard of protection as entities are obliged to justify to DPAs why they use such as ground.** It is also more likely to be 'future-proof' as it enables use of communications data in new applications that cannot be anticipated today through a more principles-based approach to privacy protection.

j) 'Re-obtaining' consent

The requirement for re-consent at six monthly intervals in Article 9(3) is extremely unclear. At a high level, we agree with the concept that a user should have a means to amend previous choices regarding consent. This can be achieved in a variety of ways through access to easy to use settings for instance or privacy reminders during software updates etc. **It is counter-productive to specify an arbitrary period of six months for re-consent**. This will undermine the intent to ensure that users are not overwhelmed with consent notices. It is also unclear whether the re-consent can be general in nature or whether it is required for each consent previously collected which means that a user may get what amount to daily prompts in relation to their previous choices. This would create a truly awful user experience.

4. Erasure of electronic communications data (Article 7)

The ePR will require communications data to be deleted after transmission. A service provider is permitted to keep content and metadata in only a few limited circumstances. Such a blanket deletion requirement may have been justifiable for a traditional communications transmission service (e.g. copper-wire email service). In such a situation the telephone company simply transferred the data from the sender's service to the server of the recipient and had no reason to make a recording of a telephone call and would never store message content unless ordered by the police.

However, in a cloud context, **the storage of communications content is an essential part of the service provided**. For example, messaging apps usually store the entire thread of messages in the cloud, unless the user decides to delete it, so that a user can go back and look at old messages. Other digital communications using audio, text and video components, are also expected to have features that allow the recording of the communication such as a training done through video conference that individuals can view at a later time.

A service provider may also store communications data for later analysis in order to protect its network from fraud and security threats, maintain and test the operation of its systems. **Such practices will already be subject to the GDPR's limitations on the storage and later use of personal data.** We believe there is no reason to impose special rules on communications service providers that would only prohibit practices that are otherwise permitted under the GDPR and in most cases expected by the user. **DIGITALEUROPE thus recommends that Article 7 is deleted. The storage and later use of communications data of natural persons will be protected under the GDPR.**

5. Terminal equipment – including cookies (Articles 8)

In its impact assessment, the European Commission noted that the GDPR's new definition of personal data 'clarifies that online identifiers are personal data' and that the GDPR 'further complements the level of information to be provided to the data subjects under Article 12, Article 13 and Article 14. The obligation to inform users about processing of personal data is therefore covered by the GDPR'. Furthermore, the European Commission notes that the 'objective of protection of Article 5.3 of the ePD should be enhanced by the principle of data protection by design and by default under Article 25 of the GDPR.'

Despite all these improvements, which ensure that the objectives of the current rules of more control and transparency to the user have been achieved by the GDPR, the European Commission decided not only to keep the current 'cookie' rules, but also to expand on them and in many ways make them more confusing and contradictory.

A simple solution could have been to state that the above articles of the GDPR are applicable to 'storing of information, or gaining of access to information already stored, in the terminal equipment of an end-user.' This would avoid that manufacturers of hardware and developers of software are faced with obligations that are distinct from those they have where they collect and process personal data.

a) Prohibition of processing

Article 8 seeks to widen the rules to prohibit 'processing' of information, not just access and storage. This could have unforeseen implications. For example, this could subject a device or software developer to strict consent requirements even when it makes use of the terminal equipment's processing capabilities for an offline purpose that is not strictly necessary for an online service and has no privacy impact. Further in the case of some of the devices that would fall under the category of terminal equipment, providing the consent in the way that GDPR requires would be extremely difficult.

b) Exceptions remain narrow

The European Commission only suggests one new exemption, which is extremely narrow, for first party analytics. This exemption for web audience measurement and the associated recitals are very focused on

cookies, while the rules themselves are drafted broadly and apply to all access and storage of data on end-user devices. It is important that exemptions are technology neutral. Without improvements, this addition does little to address the plethora of concerns of this needlessly restrictive provision.

For example, processing capabilities of end-user terminal equipment are used for security and related purposes – such as the disassociation of a 'rogue' device (unmanaged device) from a managed network. The end user in question is connecting an illegitimate device to the network, potentially for malicious purposes such as man-in-the-middle attacks, and is unlikely to be willing to provide their consent. In other cases, the users' device may be hijacked without his or her knowledge – which cannot be dealt with effectively if consent is required.

Network management may also be outsourced to a third party. While it is reasonable to expect the legal entity contracting the third party to have legal arrangements that will allow to such management of devices, but depending on how 'end-user' is construed, the consent may be required from individual users of the network, which is less workable.

c) Strict consent requirements

After the entry into force of the ePD, it became clear how counterproductive an overly strict interpretation of the opt-in requirement is, leading to an overexposure of consent requirements and de-sensitising of users. The draft ePR proposes to keep the consent-only model with an only slightly improved list of exceptions. We do take note of the intention to provide for more user-friendly consent option in Articles 9(2) and 10. However, we are uncertain whether the objective to avoid over-notification would be achieved by the current wording of these articles. Moreover, Article 10 seems to be in direct contradiction with Article 8 to the extent that – contrary to the latter, which allows several legal bases – it only allows processing of terminal equipment data based on users' prior consent.

DIGITALEUROPE believes that allowing the use of all the legal grounds for processing outlined in Article 6 of the GDPR would be appropriate. This article already limits processing of personal data to well defined circumstances and thus provides the necessary protection. However, it also allows the use of cookies and similar technologies based on other appropriate legal basis laid down by law. Allowing the use of all legal basis as defined in Article 6 of the GDPR could avoid continued issues resulting from the existing inflexibility and potential future difficulties highlighted above. Overall, the proposed continuation of specific restrictions on cookies and device data are unnecessary and duplicative.

d) Standardised icons

The ePR proposed the potential development of standardised icons through a delegated act to visibly provide data subjects with an overview of the use of 'cookies'. While we welcome all efforts to make communication of data policies to data subjects clearer and easier to understand, we caution against the adoption of standardised icons aimed at summarising compliance with the ePR. ePR compliance cannot be summarised into 'yes/no' answers. Icons are often difficult to adapt to technological developments and could quickly become outdated or obsolete.

6. Connection data (Article 8)

Article 8(2) prohibits the collection of information emitted by terminal equipment to enable connection to the network unless it is (i) strictly in order to enable connection or (ii) notice is provided on the processing of the data in line with Article 13 of the GDPR and measures on how to stop or minimise collection are outlined.

While these are understandable conditions on their own, what is less clear is whether they are the only conditions that apply to such information. Considering the definition of metadata as currently framed, it is possible to conclude that such information should also be considered metadata ('data processed in an electronic communications network for the purposes of transmitting […] electronic communications content; including […] data on the location of the device generated in the context of providing electronic communication services […]'). If the information in question is to be considered metadata, it would need to also meet one of the grounds permitting processing of such data - in most cases end user consent. It is unclear whether providing the notice and information on how to stop collection of data would fulfil or replace the condition of consent. **A possible solution would be to clarify that such data is a stand-alone category, rather than a subset of metadata.**

7. Privacy settings (Article 10)

We understand the intent behind Article 10, which seeks to introduce an obligation on browser providers to include privacy sensitive settings to educate users in relation to privacy choices. We consider that placing such obligations on browser providers is not the appropriate means to tackle any perceptions in relation to third party data collection as users browse the internet. Furthermore, the inclusion of 'including the retrieval and presentation of information on the internet' in the definition has broadened the requirement to all software placed on terminal equipment accessing the internet. Such software would include major software releases for phones and computers and applications supplied by developers large and small. We cannot believe that such an extension of regulatory reach to essentially all computer code available on phones and computers was intended. **It imposes an impossible burden on all such developers of code** and will only serve again to confuse users who will now be faced with multiple pop ups just from the use of code.

Moreover, DPAs do not have the experience and expertise to act as a regulator in this space. Their competence relates to the supervision of personal data on relevant filling systems which roughly approximates to personal data processed on servers. This focus stems from the desire to ensure that personal data could not be combined and used across systems to target or profile individuals to their detriment. Software which only processes personal data locally on a device or does not collect personal data itself does not give rise to such privacy concerns and therefore should be outside the scope of Article 10.

8. Law enforcement access to data (Article 11)

DIGITALEUROPE wishes to emphasise that Article 11 **must be read in light of the jurisprudence of the Court of Justice of the EU ("CJEU")**, which notes that the protection of confidentiality 'applies to the measures taken by all persons other than users, whether private persons or bodies or state bodies.'[1] Any exceptions must be interpreted strictly.

[1] Judgment of the Court (Grand Chamber) of December 21, 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970. 77

In light of the above, we are concerned that the ePR proposes an extension of the scope of restrictions which Member States can place on the rights and obligations laid down in Articles 5-8 beyond 'defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system' to include 'economic and financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security'. **DIGITALEUROPE strongly opposes such an expansion of cases when authorities can restrict the scope of this fundamental right. It is unfortunate that a draft Regulation which has the worthy aim of improving user privacy in fact is the vehicle by which Member States can undermine that privacy by means of data retention and interception requirements. This is facilitated by the extension of the definitions of what constitutes a communications service.**

a) Broader range of data that authorities can request

The European Commission proposes to allow national authorities to request access to electronic communication data, which covers both content and metadata. This is in **stark contrast to the views of the Council of Europe**[2], which notes that subscriber information, rather than content data, is the 'most often sought data in criminal investigations'. We strongly suggest not to extend the scope of data beyond what is truly necessary.

b) The ePR should not allow backdoors

In line with the recommendations of the Article 29 Working Party, 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**. Companies should be allowed (even obliged) to put in place security measures to protect their systems from all intrusion, in line with the rules and principles established by Article 32 of the GDPR.

c) Jurisdictional confusion

Unlike traditional telecom operators, online providers offer their services cross-border and in numerous EU markets. As the European Commission itself pointed out in its progress report following the Conclusions of the Council on the European Union on Improving Criminal Justice in Cyberspace (15072/16), the question of jurisdiction in this area is very complex. This is why the European Commission has launched a sophisticated consultation and evaluation process to address this problem.

To the extent that Article 11(2) should be kept and includes online service providers , it is important that the ePR also **provides some clarification regarding jurisdiction**. As both the European Commission and the Council of

[2] Subscriber information is defined by the Council of Europe as:

- Any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
- the type of communication service used, the technical provisions taken thereto and the period of service;
- the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
- any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Europe recognises, the disclosure of data to law enforcement authorities may 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. This will likely be the case for many of the online services now included in the scope of the ePR that by definition operate across borders. **This problem cannot be disregarded**.

It should be made clear that requests for lawful interception of communications across national borders remain governed by existing mutual assistance arrangements and the European Investigation Order.

9. Caller ID and call blocking (Articles 12, 13 and 14)

The provisions relating to caller identification and call blocking apply to providers of publicly available number-based interpersonal communications services. A distinction is made in the draft ECC between number-based and number-independent services. For number-based services, the provider is using a public resource and benefitting from an interoperable system, and therefore warrants a higher degree of regulation. As currently defined, the **definition of number-based services is very broad and undermines the effectiveness of the intended targeted approach** as it captures hybrid services that may enable communication with a number, but often do not have a number allocated to them. Therefore they are not benefiting from the described public resource and interoperable system in the same way.

Some of the specific obligations are **inappropriate for a hybrid service**. The requirement for the called end-user to prevent the presentation of the calling line identification of incoming calls, for example, seems to be predicated on a one-to-one call. In collaboration solutions, however, a common state of affairs involves multiple parties engaging in a joint virtual meeting with voice, video, messaging and document sharing and editing capabilities. Given there are numerous 'called end-users' it is unclear how it would be possible to determine that each has the right to see the caller identification or block it at the same time.

We believe these issues can be resolved if the **definition of number-based services is effectively amended in the ECC**, but policy makers working on the ePR should bear in mind the impact if such changes are not made.

10. Security (Article 17)

DIGITALEUROPE welcomes the European Commission's suggestion to streamline security requirements and align these with the GDPR. However, the remaining provisions on providing transparency of risks to end-users sets the threshold for notification far too 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 Network and Information Security (NIS) Directive, but does not contain the equivalent thresholds and safeguards to ensure only relevant information is provided.**

Furthermore, the article also seems to assume that the natural state of the online environment is zero risk. This is far from being true. As the European Commission itself pointed out, 'according to a recent survey, at least

80% of European companies have experienced at least one cybersecurity incident over the last year and the number of security incidents across all industries worldwide rose by 38% in 2015.' In this context, it is not clear as to what would be the 'particular risk' that 'may compromise' the security of the networks and services that the provider would need to notify. The suggested article also fails to recognise that **notifying the end user is not always good security – such as when the end user is the malicious actor.**

DIGITALEUROPE recommends that 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.

11. Harmonisation and enforcement (Articles 18-20)

DIGITALEUROPE welcomes the choice of a Regulation as an instrument, which brings 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 DPA's 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.

12. Remedies and sanctions (Article 21 and 23)

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, instead of just referencing Article 80 of the GDPR. Furthermore, while we understand the desire to align the ePR sanctions regime with that of the GDPR, the extension of the significant sanctions to breaches for ePR significant provisions, such as Article 16, seems disproportionate.

13. Timeline (Articles 27 and 29)

DIGITALEUROPE strongly urges the co-legislators to take the time to properly consult and evaluate the impact of any new legislation, instead of rushing negotiations to meet an unrealistic timeline. Whilst we understand the merits of aligning the adoption of the ePR with the implementation of the GDPR implementation, we worry that a rushed process will not provide sufficient time to properly assess the full implications of the proposal.

It is not just the policy development process that needs to be given time to mature, but also the time need for companies to implement the ePR once it has finally been adopted. 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 two year deadline under the GDPR is in itself proving to be tough to meet and involves a determined push from our members to achieve. Even if the policy process for the ePR could somehow be fast-

tracked to be finalised within a year, under the current timeline our members would be expected to complete the entire compliance process in only a couple of months.

The proposal to 'apply' (i.e. enforce) the ePR as of May 2018 is therefore 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.**' (Case 348/85) It is hard to argue that a legislation that envisions 4% annual world-wide turnover fine does not meet this thresholds.

Accordingly, companies should have at least the standard **18 months to prepare for this law**.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK