DIGITALEUROPE

DIGITALEUROPE's consolidated position on ePrivacy Regulation

Brussels, 5 February 2018

DIGITALEUROPE is committed to working with the Council and the European Parliament to deliver a new ePrivacy Regulation (ePR) that can truly protect Europeans' right to privacy while not hampering innovation and beneficial data uses. European consumers and companies shouldn't have to choose one or the other, and the right balance can be found if the new law provides for a risk-based approach and ensures full consistency with the letter and the spirit of the General Data Protection Regulation (GDPR) as well as the upcoming European Electronic Communications Code (EECC). In this paper, we provide a detailed overview of the challenges we have identified concerning the ePR proposal and some suggestions as to how to tackle them.

REASONABLE SCOPE THAT COMPLEMENTS EXISTING RULES AND MINIMISES OVERLAPS

Sitting between the EU's data protection and telecoms frameworks, the ePR is meant to build upon and complement both. Making sure the new ePR rules are clear and targeted to **areas where there is a genuine legislative gap** will both better protect Europeans' privacy and help organisations to comply.

The processing of personal data other than by electronic means – including by those that would qualify as 'electronic communications services' and by virtually everybody else given the widespread use of 'processing and storage capabilities of terminal equipment' – is extremely confined in modern times. This means that the ePR will apply to the **vast majority of personal data processing** being carried out and already subject to the GDPR, creating a large grey zone mired in **overlaps and inconsistencies**, solutions to which we detail below.

1. Anonymous data

A basic logical inconsistency stems from the **inclusion in the ePR's scope of data that does not fall under the GDPR's definition of personal data**. Given the ePR's objective to protect, in particular, people's private lives and communications, this inconsistency is remarkable and has deep consequences.

By including non-personal data in its scope, the ePR **effectively removes incentives for responsible companies to develop technologies and build services that are predicated upon anonymity and anonymisation**, for instance through the use of data minimisation techniques.

DIGITALEUROPE therefore urges an alignment of the ePR with the GDPR's Recital 26 and Article 4, which explicitly excludes anonymous data from the scope of the GDPR. This should be reflected in the ePR's Article 2. The exception should not only be applicable to the *process* of anonymisation, but to **anonymous data itself**, i.e. where no further actions are needed to be taken for the data to be considered anonymous. As per our remarks above, this is the case today for the GDPR and strongly incentivises companies to rely on data that is not identifiable. (See Annex for the precise language of 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

2. Ancillary services

The inclusion of minor or ancillary communication features in the ePR's scope would go beyond the original intention to 'protect the confidentiality of functionally equivalent electronic communication services' (WP 240). As a growing number of digital services allow some basic form of communication, including 'ancillary' features would capture thousands of applications and services that would not be considered as 'functionally equivalent' under the upcoming European Electronic Communications Code (EECC). **DIGITALEUROPE urges alignment of the ePR's definitions and scope with the EECC** by excluding ancillary features from the scope of the ePR.

The **scope should also be predictable**. It cannot be that a change in the user setting triggers a completely different set of new rules. This would be the case if we followed Council Doc. 14062/17, which suggest defining the scope based on whether the communication is taking place between a 'finite' or a 'potentially unlimited number of end-users' (See Recital 11a). Such distinction can be a matter of settings. As the rules, including the core legal basis and principles, may be fundamentally different, this extremely nuanced approach could be difficult for organisations to handle. The law should thus be more straightforward in helping organisations understand and plan for their legal obligations.

3. Terminal equipment

The ePR's rules pertaining to terminal equipment are particularly important. In fact, nowadays there are virtually no personal data processing activities that do not use the 'processing and storage capabilities of terminal equipment', thus making it necessary for all controllers and processors (including those that do not qualify as 'electronic communications services') to comply with the ePR's Article 8. And this is despite of the fact that the GDPR would allow their processing operations on different grounds. This casts some fundamental doubts as to whether the ePR really is a targeted and 'sectoral' law, given that it acts as a de facto gatekeeper to processing operations under the GDPR.

While DIGITALEUROPE recognises the sensitivity that some uses of terminal equipment data may have for consumers' private lives, we urge the co-legislators to consider and converge around a **more flexible and granular approach**. This would preserve organisations' ability to use terminal equipment data for **worthy and non-privacy-invasive causes** such as improving security, enabling technical functionalities and developing innovative products and services.

The development and improvement of device functionalities, better connectivity and innovative services hinges on the ability to collect information from users' terminal equipment on the part of a diverse number of parties in the technology value chain, including device makers (OEMs), component manufacturers and more. Data used for these purposes consists mainly of telemetry data, which is purely technical in nature and is generally not considered personal data. Nevertheless, given the inclusion of non-personal data in the ePR proposal, organisations that have to collect such data would have to comply with Article 8. As we have noted in Section 1 above, **excluding non-personal data from the ePR's scope**, bringing it in line with the GDPR, would solve this fundamental inconsistency. Similarly, a proper balance could be struck in the ePR by allowing the collection of **information about technical quality or effectiveness** that is limited by design to have little or no impact on the right to privacy and confidentiality, similar to the current Dutch implementation of the ePrivacy Directive.

Moreover, security plays an integral part in protecting users from malicious activity and generating trust in the reliability of devices and services. The Article 29 Working Party has consistently argued that processing for maintaining and managing technical security should fall under one explicit exception for the processing of

terminal equipment data in the ePR. The European Parliament's report and the Council's Doc. 15333/17 have proposed an exception that only applies for security updates (i.e. *downloads*) to the device, but does not reflect the fact that detecting security vulnerabilities, with a view to creating patches, also requires an *upload* of data from devices. We therefore urge the co-legislators to adopt a **more general security exception that is consistent for all type of data covered by the ePR**.

4. M2M

Similar to terminal equipment more broadly, which includes 'machines', 'M2M' includes a **vast array of disparate devices and services, making inflexible rules under the ePR framework particularly difficult to implement**. Broadening the scope to a broadly defined 'M2M' 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, which focuses on ensuring *people's* privacy, and would unnecessarily lead to unworkable situations in practice, for instance, rendering standard processes and developments of Industry 4.0 laborious or impossible.

Today, many companies face the challenge that customers do not only request actions from their 'connected' machines, but also related services via 'M2M platforms'. 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) transferring 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, to the extent they involve personal data.

DIGITALEUROPE suggests an explicit clarification that **products and services containing an M2M platform do not fall within the scope** of the ePR (for instance by limiting the scope of the ePR in Article 2). We thus welcome the European Parliament's suggestion to delete Recital 12, but regret that the impact of this amendment is then neutralized by suggested amendment 55.

5. Focus on communications and not on software

The ePR should **focus on communications data**. Simply because software allows for access to the internet does not mean that the resulting access to data is communications data. That is too broad a requirement and will impose too high a burden on software developers and create confusion with the GDPR.

By the same token, focusing on **hardware** in and of itself fails to consider the harm that the processed data may or may not have for users' privacy. As we have explained above, hardware data in some instances (e.g. telemetry data) does not even constitute personal data. As such, hardware should not be covered by the scope of the ePR.

6. 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 this exemption to be clarified in an article.

DIGITALEUROPE is concerned that previous interpretations of this term by the National Regulatory Authorities ('NRAs') have both included services offered to enterprises as a whole (as opposed to specific sectors) and

considered the means of availability (e.g. purchase over the public internet) as the determining factor as opposed to who is being targeted by the service.

We would thus like to see some clarification to ensure clarity regarding the scope. We would suggest **making it clear that the following type of communication do not fall within the scope of ePR**:

- Communications that take place only over Near Field Communication (NFC) networks including Bluetooth and Wi-Fi;
- Beta or 'tester' 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);
- 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.
- We also ask for clarification on what amounts to an 'undefined group of users'.

7. End-users / users/ subscribers / consumers vs legal persons

DIGITALEUROPE is concerned about the inclusion of legal persons in the scope of the Regulation. Excluding legal persons would be important to ensure consistency with the GDPR and the focus on protecting personal communications and data. Indeed, the GDPR explicitly excludes legal persons (see Annex), and recalling this is particularly important when evaluating the Estonian Presidency's suggestions to apply the GDPR to legal persons (such as in Recital 2a stating that insofar as end-users who are legal persons are concerned, provisions of Regulation (EU) 2016/679 should apply'). Such contradictions should be avoided and the ePR and the GDPR should be consistent in this regard.

DIGITALEUROPE believes that **the ePR should only apply to consumers, i.e. natural persons who use publicly available electronic communications services outside the context of their profession**. We thus welcome and support replacing references to end-users, which accounts for both natural and legal persons. In our view, **referencing 'consumers' would be the most straightforward solution, but could support references to 'users' as well, to the extent the definition is consistent with that of the Code and covers natural persons only when acting in their personal capacity**. However, reference to 'subscribers' in our view will not substantially improve the current situation, as it equally covers both natural and legal persons.

8. Household exception

DIGITALEUROPE welcomes recognition that providers of electronic communications services need to process electronic communication data for purposes 'such as search or keyword indexing functionality, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities'. However, such permission should not be linked to 'purely individual usage'.

It is important to recall that **the GDPR 'does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity** and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking or online activity undertaken within the context of such activities' (Recital 18 and Article 2). **Such**

processing is thus not subject to consent or any other requirements. The ePR could make similar exception in Article 2.

It is also important to remember that Recital 18 of the GDPR, on the other hand, does apply to 'controllers or processors which provide the means for processing personal data for such personal or household activity'. Thus, while the idea to offer more flexibility for companies to provide the above-mentioned services should clearly be reflected in the law, it should not be linked to these individual or household exceptions.

9. Territorial Scope

DIGITALEUROPE supports clarifications that would ensure that only services intended for the European market are covered by the scope of the legislation. People travel all the time with their devices in a way that is obviously not predictable for the provider.

The European Parliament put forward helpful amendments that would clarify that only services 'offered' (Am 46) to users in the Union are covered. It also deletes reference to an obscure category of 'use of such services' and instead suggests focussing on services that are 'referred to in Article 2' and that 'are provided from the territory of the Union' (Am 47). We would welcome further clarification that for terminal equipment to be covered, it should be 'placed on the market' and not just 'located' in the Union. Furthermore, in line with the GDPR we would also like to see clarification that the mere accessibility of an electronic communication service in the Union is not sufficient to trigger the application of the ePR.

CLEAR RULES THAT ARE FULL CONSISTENT WITH THE GDPR AND THE CODE

1. Consistent use of the definitions – Alignment with the Code

DIGITALEUROPE believes it essential to **avoid parallel and conflicting definitions describing the same phenomena**. Our members strongly oppose the European Parliament's amendments (52-60) that put forward such distinct definitions. Having to deal with two definitions for 'electronic communications network', 'electronic communications services', or 'users' … etc, would lead to insurmountable legal uncertainty. Nevertheless, the scope of the ePR should explicitly exclude M2M communication (see point 4 above).

In addition, the Commission's definition of what consists of 'transmission' also means that the rules applicable within an email service (again based on potentially completely different legal grounds and principles) could depend on whether the user opened an email or not. If the intention is to focus on the transmission, this needs to be clear that such phase ends with the electronic communications service provider of the intended recipient (as suggested by the Parliament in Am 14) and not the user.

2. Consistency with the GDPR

As the main intention behind the revision of the ePrivacy framework is to be adapted to the GDPR, it is essential that it takes full account of rules that already exist under the GDPR and does not contradict established rules and standards. This is particularly important when it comes to ensuring that **consent standards, as well as the relevance of additional legal bases are the same across the two legal instruments (which should be applicable to all processors, for instance to third parties providing cybersecurity or analytics services).** The ePR should also reflect the agreement achieved in the GDPR when it comes to fines, the representative and other areas already covered by the GDPR.

Same consent standard across all legal instruments

The GDPR contains detailed rules on consent, which define when consent is valid, how it should be documented and users' rights regarding withdrawal and other areas. (See Annex for the provisions of the GDPR.) These rules nuance the existing requirements and companies are investing heavily in upgrading their infrastructure to reflect these.

As the current scope of the ePR fails to draw clear lines with the GDPR, many services could be subject simultaneously to both legal regimes. This makes it all the more important for the ePR's consent standards to be fully aligned with the GDPR. This means that **any reference to consent in the ePR should be exclusively limited to it having 'the same meaning and be subject to the same conditions as the data subject's consent under Regulation (EU) 2016/679'**.

Yet, the various Institutions propose over a dozen additional, often conflicting requirements on consent. We urge the co-legislators to delete the following provisions from the text:

- Article 6 suggests that consent should be required 'including for the provision of specific service'. We would like to note that under the GDPR, processing that is necessary for the performance of a contract is subject to a legal basis that is distinct from consent. As such, these requirements are confusing.
- Article 6 also adds an extra condition 'that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous'. We have explained our position on the need to exclude anonymous data from the ePR's scope above, which we believe should be reflected in the body of the law rather than in this specific provision.
- Article 6 also requires 'all end-users' involved in the communication to give consent. This would put an impossible legal requirement in front of any service provider that allows for interoperability with other communication services, where a provider cannot collect valid consent from users it has no interaction with. Adopting these provisions would outlaw an open communication service, such as e-mail.
- Article 9 contains rules on technical settings. While this may be helpful in certain circumstances, such rules are unnecessary as Recital 32 of the GDPR already makes it clear that consent 'could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.'
- Article 9 also suggests regulating the withdrawal of consent. This is entirely redundant as Article 7 of the GDPR and corresponding recitals already make it clear that 'the data subject shall have the right to withdraw his or her consent at any time'. The suggested reminders are also likely to be counterproductive, if the purpose of the rule is to minimise 'consent fatigue'.
- Recital 18 also provides a definition of when consent is valid. This is completely redundant, as we have already noted, as the GDPR already provides detailed rules on the validity of consent (see Article 7 and corresponding recitals 42, 43 and others).

The European Parliament's amendments (103-105 and corresponding recitals) in this area are of particular concern:

- The Parliament proposes to ban 'cookie walls' and suggests that 'no user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on

grounds that he or she has not given his or her consent'. Again, the GDPR provides detailed rules on the validity of consent. Article 7 of the GDPR also state that 'when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'. As DIGITALEUROPE indicated in its response to the Article 29 Working Party consultation on the consent guidelines, companies should retain their freedom to define the services they provide and the conditions (including monetization) under which they make these services available.

- Furthermore, the Parliament suggests adding that 'any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their rights to privacy and protection of personal data'. Again, the validity of consent is regulated in detail in the GDPR. It is unclear what added value this rule would have apart from creating confusion.

The Bulgarian Presidency's Doc. 5165/18 also suggests additional consent standards:

- Possibility for special consent rules for M2M communications or allowing a one-off consent; and
- Possibility for special consent rules for legal persons.

However, in these latter cases, instead of tweaking the consent requirements creating discrepancy and confusion, the choice of another legal basis, like contract, would be more appropriate. This is, of course, without prejudice, to DigitalEurope's position that such services should not be covered.

DIGITALEUROPE believes that **all these additional rules and requirements are redundant and confusing**. We urge the co-legislators to **delete them all** to ensure full alignment with the GDPR, making it clear that the GDPR's 'definition of and conditions for consent' apply.

Storage and 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 and limited circumstances.

Such a blanket deletion requirement may have been justifiable for traditional communications transmission services (e.g. copper-wire e-mail service). In this case, 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 as well as 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.

Article 7 could thus be deleted without any risk to the user. The storage and later use of communications data will be protected under the GDPR.

Security (Article 17)

DIGITALEUROPE welcomes the European Commission's suggestion to streamline security requirements and align these with the GDPR. However, given the detailed rules on security in the GDPR, the Code as well as in the Network and Information Security Directive, the remaining provisions on providing transparency of risks are equally unnecessary. We thus strongly agree with the Estonian Presidency's proposal to delete Article 17 and corresponding Recital 37.

Other redundancies: representative (Article 3), remedies (Article 21), enforcement (Articles 18-20)

DIGITALEUROPE notes that the GDPR already contains rules related to representatives for organisations not established in the Union. There is no need to replicate or rewrite these rules in Article 3(3) of the ePR.

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.

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 communications network and service providers, public directory providers, direct marketers or any other covered entities as to which supervisory authority they are responsible towards.

3. The ePR rules should also be consistent among each other and avoid internal overlaps and duplications – Content, metadata and terminal equipment

As a result of the amendments put forward by the European Parliament, the ePR proposal is not only inconsistent with the rest of the EU acquis, but the various requirements themselves overlap and multiple rules are suggested for the same thing. This overlap is particularly striking between Articles 5, 6 and 8.

Today the ePrivacy Directive contains one article (Article 5) on confidentiality. It states the confidentiality of communications in Article 5(1), provides for exceptions in Article 5(2) and puts forward a rule regarding terminal equipment in Article 5(3). The Commission turns this one article into six distinct articles, each of which has three or more sub-provisions. Moreover, the variance in the provisions relating to electronic communications data, metadata and terminal equipment data – which often overlap – creates incoherent sets of legal bases and requirements.

The Parliament would make this situation even worse, mixing content data, metadata and data related to terminal equipment. In Amendment 61, the Parliament suggests that 'where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the respective service, they shall be considered electronic communications content for the respective service'. Amendment 12 also

suggests that metadata 'should also include data necessary to identify users' terminal equipment and data emitted by terminal equipment when searching for access points or other equipment'.

DIGITALEUROPE suggests **revisiting the structure proposed by the Commission** in order to ensure comprehensibility and thus meaningful compliance. **The ideal solution could consist in merging articles 5-10** thus:

- Article 5(1) **protecting confidentiality as a general rule**; and
- Article 5(2) **consolidating the list of exceptions** outlined in Articles 6, 7 and 8.

MODERN SCOPE, MODERN RULES: RISK-BASED APPROACH, FLEXIBILITY, TECH-NEUTRALITY

Rather than establishing a general prohibition on interception and surveillance as a means to protect confidentiality of communications, the ePR proposal establishes more detailed prohibitions for all processing underpinning a broad range of communications services and terminal equipment. This large net **unjustifiably captures all processing activities with no consideration of their actual or potential harm to privacy**.

DIGITALEUROPE believes it essential for the ePR to follow a risk-based approach, to ensure the necessary legal flexibility, to remain technology neutral and to find a better balance between the fundamentals of confidentiality and law enforcement access.

1. A real risk-based approach and more legal flexibility

The protection afforded to personal data in the GDPR undeniably sets a very high standard. Although many viewpoints have been expressed in the legislative debate so far, we respectfully submit that **no substantive argumentation or evidence has been put forward** to date that justifies why the GDPR's high level of protection does not provide enough safeguards when it comes to processing communications and terminal equipment data.

DIGITALEUROPE challenges the assumption that the processing of electronic communications content and metadata, as well as any use of processing and storage capabilities of terminal equipment, always represents a high risk to consumers.

An overly prohibitive view would impair the performance of communications services and terminal equipment and make many features loved and expected by users more difficult to get to.

Many processing activities, such as spam detection, the display or printing of an e-mail, providing automatic updates and back-ups, ensuring that devices are free from security vulnerabilities and many others happen seamlessly without representing a risk to users' fundamental rights and freedoms.

Terminal equipment receives information that is necessary to enable or considerably improve device functionalities that consumers expect and use for other services, such as the location of satellites to improve a device's ability to determine its location. Information is also automatically emitted by terminal equipment in order to connect to local networks or other devices, such as Wi-Fi networks. This information must be processed by default or individuals would not be able to see or connect to networks in their vicinity.

Assuming that any processing related to communications or terminal equipment represents a high risk is not only a drastic departure from the GDPR's approach, but will also likely to be counterproductive. This is where the risk of consent fatigue becomes clear, with users becoming desensitised to those processing operations that could indeed represent real harm to their privacy.

DIGITALEUROPE agrees that impact assessment and consultation with the Data Protection Authorities may be necessary if the processing represents a high risk to the rights and freedoms of natural persons – **but we urge co-legislators to consider that the notion that processing communications content, metadata and terminal equipment data always represents a high risk is fundamentally flawed**.

The challenge of consent fatigue is widely recognised

The European Commission, the Article 29 Working Party and many others recognise the challenge of consent fatigue. Rather than reinventing the consent standard, contributing to legal uncertainty and confusion, we believe the solution is to **use consent as only one available mechanism among several**.

In some situations, consent simply does not make sense. Asking a fraudster's consent for the purpose of detecting fraudulent activities would hardly be a practical solution. This is why the GDPR makes it clear that processing for the purposes of preventing fraud constitutes a legitimate interest of the data controller (see Recital 47 of the GDPR). Recital 19 of the Commission's text also conditions the 'scanning of e-mails to remove certain predefined material' to consent. This would mean that the removal of child abuse images, for example, would be subject to the abuser's consent.

Hard to come up with a future-proof, fixed set of exceptions

While some exceptions are easy to identify – like the need to protect the security of services, networks, terminal equipment or the user – others are harder. Indeed, during the negotiation process, Members of the European Parliament proposed over a dozen additional exceptions, including, among others: processing based on pseudonymous or anonymous data; processing that is necessary to ensure the security of the networks, the terminal equipment and the users as well as to fight fraud; for compliance with legal obligations; based on legitimate interest or for emergency services; aims to ensure quality of service; or for activities otherwise allowed by Union or Member State law. We regret that these exceptions were not or only partially reflected in the Parliament's final text.

While we appreciate the viability to incorporate a longer list of exceptions to the consent rule, DIGITALEUROPE strongly believes that **following a principle-based approach and introducing all the legal bases of Article 6 of the GDPR** will provide the most straightforward and future-proof solution. As an ever-broader array of services rely on electronic communications and terminal equipment, this principle-based approach is the only way to apply the ePR to not-yet-invented technologies while being subject to the stringent protections enshrined in the GDPR.

Legitimate interest legal basis

DIGITALEUROPE has been particularly supportive of the inclusion of the legitimate interest legal basis for processing electronic communication data as well as for the use of storage and processing capacity of a device, as this would ease the pressure to try to enumerate all the possible exceptions that may be needed today and tomorrow, while ensuring accountability and high-level protection to the user.

Contrary to widespread scepticism about legitimate interest, legitimate interest is not a blank cheque to proceed with any kind of nefarious data processing activities, but it is carefully defined by the GDPR and sets out a **workable**

framework whereby non-invasive processing activities can happen subject to all the obligations and safeguards of EU data protection law.[1]

Necessary for the provision of a service / performance of a contract

There is no doubt that the ePR should allow processing of both communications data and the use of processing and storage capabilities of terminal equipment if this is 'necessary to provide a service to the user' or 'for the performance of a contract to which the user is party or in order to take steps at the request of the user prior to entering into a contract' (language based on GDPR Article 6(1)(b).

However, DIGITALEUROPE is **very concerned about suggestions that these should be limited to what is 'technically' or 'strictly' necessary**. Such terminology could easily exclude processing activities that are needed to make a product or device functionality perform better and/or differentiate the various offerings on the market.

Necessity is in the eye of the beholder. Is a fibre-to-the-home connection 'strictly technically necessary' as opposed to a copper network? Is LTE necessary or can one live with a 3G connection? Providers should be able to provide what they believe to be an optimal user experience and not be limited to archaic technical standards.

Security exceptions

The same way the GDPR explicitly recognises that processing for the purposes of ensuring network and information security constitutes a legitimate interest of the controller; the ePR should also **acknowledge that processing of communications data as well the use of processing and storage capabilities of terminal equipment for security purposes is allowed**.

DIGITALEUROPE welcomed clarifications suggested by the Parliament that **not only service providers, but also 'other parties acting on behalf of the provider or the user'** (Amendment 72) may process information to 'maintain or restore the availability, integrity, confidentiality and security' of the service.

We also welcomed additional flexibility suggested for Article 8 by the Parliament (Amendment 90). We would, nonetheless, ask for the security exemption to go further and **be sufficiently flexible to ensure that users' devices as well as the broader ecosystem can be protected**. For example, an infected device can distribute malicious software across the network and the user of the device may or may not be aware or want to stop this. The software / device provider should still be in the position to address this security threat.

More broadly, as we have argued on page 2, a security exception should recognise that **detecting security threats requires an *upload* of data from devices, not just *downloads* of software updates to the device**.

Last, but not least, the same security exception should apply to all data covered by the ePR.

Compatible use

DIGITALEUROPE supports bringing the ePR legislation in line with the GDPR so as to **allow for further processing of electronic communication data and terminal equipment data for purposes compatible** with those the data was collected for.

1 See Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

2. Maintaining technology neutrality

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. However, 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**.

Furthermore, the inclusion of '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 to confuse users, who will now be faced with multiple pop-ups just from the use of code.

Overall, **DIGITALEUROPE does not believe it appropriate for the ePR to define settings or default settings**, as is suggested by the Commission and Parliament in Article 10 and corresponding Recitals 22-24.

3. Finding a better balance between the fundamentals of confidentiality and law enforcement access

DIGITALEUROPE welcomes the changes made by the Parliament to Article 11. The Parliament has helpfully clarified that any restrictions on the rights of individuals are **only allowed in the areas of national security, defence and the prevention, investigation, detection and prosecution of criminal offences**. We also very much welcome the clarification that the 'Union or Member States shall **not impose any obligation on undertakings that would result in the weakening of the security and encryption of their networks and services**'. We believe this is the right approach as it is not only fundamental for cybersecurity at large but also reaffirms the ePR's ambition to ensure that communications services and devices remain confidential and secure.

Finally, we wish to note that, unlike traditional telecoms operators, online providers offer their services cross-border and in numerous EU markets. This creates a need to address **potential conflict of law issues that many operators face when required to respond to cross-border requests**. Such conflicts should be adequately covered by the Commission's upcoming initiative on improving cross-border access to electronic evidence in criminal matters,[2] which we believe should be referenced in the final ePR proposal.

2 See DIGITALEUROPE's response to the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters, available at this link.

ANNEX – GDPR GLOSSARY

As the ePR should address legislative gaps, regulating what is already covered by the GDPR is not only redundant, but would also create confusion and legal uncertainty. We include below a short glossary of the most relevant provisions of the GDPR.

Scope

Personal data: '*means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.* [Article 4 (1); Recitals 26-31]

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifies such a radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the server, may be used to create profiles of the natural persons and identify them. [Recital 30]

➔ This concept encompasses considerable amounts of information, even where the link between such information and an identifiable individual is tenuous. Any such data is subject to the GDPR. It is hard to envision that data that does not meet this very low threshold could represent any risk to a user's privacy or confidentiality; let alone one that is higher than the processing of personal data.

Anonymous data: *'The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes'.* [Recital 26]

Household exception: *'This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity*' [Article 2(2)(c)]

'This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities'. [Recital 18]

Legal persons: *'This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal persons and the contact details of the legal person'.* [Recital 14]

Principles

'Personal data shall be:

[...] (c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")

(d) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")' [Article 5]

Lawfulness of processing

'In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member States law as referred to in this Regulation' [Recital 40]. Accordingly, the GDPR recognises a number of lawful bases, other than consent, such as fulfilling a contractual obligation, complying with a legal obligation, protecting the data subject's vital interests, performing a task in the public interest and the legitimate interests of the controller or a third party when balanced against the rights and interests of the data subject.

Article 6 states that *'Processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

It is important to note that 'contract' and 'consent' are two distinct legal bases.

Consent: is *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'* [Article 4 (11)]. This is subject to further conditions:

- Where processing is based on consent, *'the controller should be able to demonstrate that the data subject has given consent to the processing operation'.* [Recital 42]

- The request for consent should be also provided in an *'intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.'* [Recital 42]
- Freely given consent means that the data subject must have a genuine choice and must be able to refuse or withdraw consent. [Recital 42]
- Indeed, the data subject *'shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent'.* [Article 7(3)]
- Consent also does not provide a valid legal ground, where there is a 'clear imbalance' between the data subject and the controller, in particular where the controller is a public authority. [Recital 43]
- When assessing whether consent is freely given, *'utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal that that is not necessary for the performance of that contract'* [Article 7(4)]
- Consent *'could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data'* [Recital 32]
- Article 8 provides further requirements where consent is relied upon when offering information society service to a child.

No wonder that the EDPS argued (Opinion 4/2017) that *'the strict conditions under which a processing can take place are already set down in the GDPR and do not require amendment or addition'*. Indeed, the GDPR sets such a high bar that an overly strict interpretation of these rules could easily make this legal basis unavailable for most processing activities. (See DigitalEurope's comment on the Article 29 Guidelines on consent.)

It is hard to envision how adding more requirements on top of this would increase the protection of an individual in any shape or form, yet they could clearly turn consent into an unachievable legal basis.

It is also because of this high bar that the Article 29 Working Party has emphasised that *'a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead'* (WP 259).

Legitimate interest:

'Processing shall be lawful if it 'is necessary for the purpose of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'. [Article 6(1)(f)]

'The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing'. [Recital 47]

'Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller'. [Recital 47]

'The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned'. [Recital 47]

'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'. [Recital 47]

'The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems'. [Recital 49]

Right to object: When processing personal data under this criterion, the data subjects have *'the right to object at any time to processing personal data concerning him or her, including profiling. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims'.* [Article 21(1)]

'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing'. [Article 21(2)]

'Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes'. [Article 21(3)]

'At the latest at the time of the first communication with the data subject, the right shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information'. [Article 21(4)]

'In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications'. [Article 21(5)]

Other relevant provisions

Profiling *'means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences interests, reliability, behaviour, location or movements'.* [Article 4((4)]

'The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes', including 'of the existence of profiling and the consequences of such profiling' [Recital 60]

As per the above, profiling can trigger the right to object. It can also be subject to the provisions on 'automated individual decision-making'.

Automated individual decision-making, including profiling: *'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.* [Article 22(1)] *'This shall not apply if the decision is based on the data subject's explicit consent'.* [Article 22(2)(c)]

The principle of transparency *'requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. [...] This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising'.* [Recital 59]

Third party *'means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and person who, under the direct authority of the controller or processor, are authorised to process personal data'.* [Article 4]

Representative: *'Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor'.* [Recital 81]

--
For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 2 609 53 10 or iva.tasheva@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 in total 25,000 ICT Companies in Europe represented by 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

Adobe, Airbus, Amazon, AMD, Apple, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, 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: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
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