29 September 2021

Comments by the Centre for Information Policy Leadership on the Draft E-Privacy Regulation for the Purpose of the Trilogue Discussions

Executive Summary

CIPL recommends that, in the context of the trilogue discussions on the e-Privacy Regulation (ePR), the final text provides for the necessary flexibility to enable innovation, while ensuring effective protection of individuals. The ePR must be consistent with the GDPR, rely on an accountability and risk-based model, only fill the gaps of the GDPR in relation to electronic communication data, align with the GDPR's legal bases for processing and enable the development of privacy-enhancing and privacy-preserving technologies that need to leverage on-device data. The ePR should also designate data protection authorities (DPAs) as sole regulators to avoid enforcement overlap and enable harmonisation through the one-stop-shop mechanism.

Social media profiles, broadcasts, communications other than private messages, minor ancillary features and Machine-to-Machine (M2M) metadata, as well as data processing activities in the context of employment, should be excluded from the ePR.

Overall, the ePR must be more accessible to all stakeholders. Definitions and terms should be simplified and the different categories of data classified more consistently. All data categories and on-device processing activities must have consistent legal bases for security of networks and information, fraud prevention, performance of a contract, vital interests, compliance with a legal obligation and network management and optimisation. The compatible purpose exemption is key for innovation and must be consistent across all types of data and aligned with the GDPR. Also, algorithmic training should be explicitly recognized as a compatible purpose.

A ban on cookie walls would have a major impact on business models that depend on advertising revenue and should be removed. Similarly, the collection of consent at browser level for cookies should be removed as too disruptive of user experience. An exemption to software updates in the employment context must be introduced as organisations must be able to decide what security-critical software updates are needed to protect their IT security infrastructure. The ePR should provide for a legitimate interest exemption to enable terminal equipment data to be processed for the benefit of third parties and society as a whole. The audience measurement exemption should be maintained and should be broad enough to enable service providers to understand how their services are used.

The provisions on direct marketing should exclude display of advertising on a website. The "own similar products and services" exception should include products and services from the same sector and apply across companies of the same group. The ePR should not leave Member States with the power to determine the position on consent to direct marketing with respect to legal persons.

29 September 2021

Summary of CIPL Recommendations

- Adopt the Council position that, depending on context, **legal entities** can be considered as users rather than providers of electronic communication services;
- Exclude from the scope of the ePR social **media profiles, broadcasts, communications other than private messages and minor ancillary features** of electronic communication services;
- Exclude data processing activities taking place in the context of **employment,** and in particular the obligation to require consent, from the scope of the ePR;
- Exclude **M2M data processing** from the scope of the ePR;
- Clarify the **interaction between the GDPR and the ePR** and adopt the Council position that electronic communication data processed after receipt by the end-user is not subject to the ePR but is subject to the GDPR;
- Adopt the Parliament approach that end-users should not be **reminded of the possibility to withdraw consent** at regular intervals;
- Provide for a simple and **consistent classification and definitions** of the different types of data covered by the ePR;
- Adopt a consistent and comprehensive approach to the **legal basis for security** for all types of data covered by the ePR;
- Acknowledge the **benefits** of processing **content data and metadata**;
- Provide for an exemption for data processing of electronic communication data for **fraud prevention**;
- Adopt the Council position that metadata can be processed for the **performance of a contract**;
- Provide that electronic communication data, including content data, can be processed for **vital interest purposes**;
- Provide for an exemption to process electronic communication data for **compliance with a legal obligation** that is broad enough to cover all legal obligations;
- Extend the **network management and optimisation** legal basis to cover both metadata and content data;
- Include a broad exemption for **compatible processing of metadata** and ensure alignment of the compatibility test with the GDPR;
- Explicitly recognise **algorithmic training** as a compatible purpose;
- Remove the restrictions on **cookie walls** and align with the GDPR's requirements on consent;

- Remove the references to **"dominant position"** to assess the validity of consent to cookies;
- Adopt the Council's position to remove the **by default-refusal approach to cookies at browser level**;
- Provide for an **exemption to consent to software updates** in the context of employment to enable organisations to protect their IT infrastructure and enable business continuity;
- Provide for an exemption to data processing from end-users' terminal equipment **to enable the use of PET and PPT**;
- Provide for **a legitimate interest exemption to enable** data processing from end-users' terminal equipment for the benefits of third-parties and society;
- Lower the threshold to use of the processing and storage capabilities of end-users' terminal equipment for the provision of a service by removing the **words "strictly" and "specifically"**;
- Adopt the Council version of the **audience measurement exemption** to obtain consent for device processing;
- Provide for the processing of end-users' terminal equipment for the purposes of **compliance with a legal obligation**;
- Align the requirements applicable to metadata to **connection data**;
- Extend the legal grounds for processing metadata for **network management and optimization, for security and for performance of a legal obligation** to connection data;
- Clarify that the **display of advertising on a website or within an information society service requested by the end-user** is outside of the scope of the ePR's **direct marketing** provisions;
- Do not leave member states with the choice to decide whether **opt-out consent is required for the delivery of direct marketing to legal persons**;
- Clarify that, in the context of direct marketing under the "soft opt-in" exemption, the notion of "**similar products and services"** includes all products and services that derive from the same sector and also covers the concept of **groups of companies**;
- Entrust **DPAs** with the oversight and enforcement of the ePR to leverage the **GDPR's OSS mechanism** and ensure **consistency and harmonisation**;
- Reduce potential enforcement overlap between the GDPR and the ePR to minimise the **risk of double jeopardy**;
- Provide for an effective cooperation mechanism with respect to **third country regulators**;
- Provide for a **harm-based approach** to e-PR enforcement;
- Adopt the Parliament's position of encouraging the **use of encryption** in the context of the ePR; and
- Provide that the ePR applies **24 months from the date of entry into force** to provide organisations with enough time to implement the new requirements.

29 September 2021

Comments by the Centre for Information Policy Leadership on the Draft E-Privacy Regulation for the Purpose of the Trilogue Discussions

On 10 January 2017, the Commission adopted its proposal for an ePrivacy Regulation[1] (ePR). The ePR sets rules for the processing of electronic data and the protection of confidentiality of communications (Regulation on Privacy and Electronic Communications) and is intended to replace the existing Directive 2002/58/EC. The EU Parliament adopted a report on 20 October 2017 (Parliament Draft).[2] On 10 February 2021, the Council of the EU reached a common position (Council Draft).[3] In the context of the trilogue discussions, CIPL[4] welcomes the opportunity to provide comments on the different versions of the ePR. CIPL has been consistently advocating that the ePR to provide the flexibility necessary in the context of the changing digital environment while ensuring that individuals' rights are effectively protected.[5] Specifically, the ePR should:

- Include as guiding principle that the ePR should be interpreted **consistently with the GDPR**;
- Rely on the **GDPR's accountability and risk-based approaches,** which are based on assessing the likelihood and severity of harms for individuals and applying mitigation measures that are appropriate to the risk;
- Impose **additional obligations on the processing of electronic data** only where the GDPR does not provide the required level of protection in light of the risk posed to individuals;

[1] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
[2] Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
[3] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
[4] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.
[5] Factsheet on the key issues relating to the relationship between the proposed ePrivacy Regulation (ePR) and the GDPR (March 2018). Study prepared for CIPL by Normally on "How Will the ePrivacy Regulation affect the design of digital services and their user experiences?" (May 2018). Study prepared for CIPL by Brinkhof Advocaten on "EPR vis-à-vis GDPR, A Comparative Analysis of the ePrivacy Regulation and the GDPR" (July 2018). CIPL's Legal note on the ePrivacy Regulation and the EU Charter of Fundamental Rights (November 2018).

- Align with the GDPR's **legal bases for processing** to facilitate compliance for organisations that are already familiar with the GDPR, its associated regulatory guidance and relevant case law;

- Designate **data protection authorities** (DPAs) as sole regulators to ensure a consistent approach through the **one-stop-shop** (OSS) mechanism under the oversight of the European Data Protection Board (EDPB);

- Ensure the ePR enables the development of **privacy-enhancing and privacy-preserving technologies** that need to leverage on-device machine learning;

- Avoid conflicts with the **Data Governance Act** (DGA) that seeks to promote data sharing activities; and

- Avoid overlap with the **Digital Markets Act** (DMA), in particular regarding provisions on the validity of consent in relation to situations where there is an imbalance of power between the end-user and the service provider.

CIPL also highlights that **companies** (including European-based companies and SMEs) **generally struggle to comply with the increased level of regulation in the EU**. In fact, most organisations, including the most mature, are still dealing with implementing the right programs and controls to enable compliance with the GDPR. In addition, certain aspects of the ePR proposal do not take sufficient account of the technological and practical reality, leaving companies faced with an entanglement of regulations. There is a high risk that the majority of these organisations will find it challenging to make the ePR effective in the short term.

The developments below highlight CIPL's preferred positions on the three proposed drafts that are most likely to address the recommendations above. They also identify some additional concerns.

1. Scope of the ePR

- **Application of the ePR to legal entities** - The scope of the ePR with regard to legal entities must be clarified. Legal entities should be classified as "users" rather than "providers" of electronic communication services if they are one of the communicating parties but use their own or third parties' communication channels. For instance, a company should be considered a "user" rather than a "provider" of electronic communication services if using its own chat functions for customer communication, for employee communications via in-house communication channels provided by the company, or if metadata gathered from customer IoT applications is used as part of a contract with such customer. In these cases, such company uses third-party or in-house communication channels as an end-user only and does not provide an electronic communication service to an undefined number of persons. The same applies to payment service providers that process transactions relying on the electronic communications networks as end users (as defined in Article 2 (14) of European Electronic Communications Code (EECC)). They do not provide these

networks, nor do they provide publicly available electronic communication services**. Therefore Recitals (8aa), (11aa) and (12) as well Article 2(2)(c) in the Council Draft should prevail.**

- **Exclusion of social media profiles** - Recital 13 of the Parliament Draft states that the ePR's confidentiality provisions should apply to closed social media profiles and groups that end-users have restricted or defined as private. This conflicts with the EECC's definition of electronic communications services or interpersonal communication services.[6] This is also impractical as social media users generally do not have an expectation of confidentiality in these contexts. In practice, it would be very difficult to determine the threshold for inclusion in the definition of "closed," especially since the status of a group as open or closed can be easily changed. **Recital (11aa) of the Council Draft specifically excludes broadcast communications made through online games from the definition of interpersonal communications. This exclusion should be extended to cover social media profiles, broadcasts and communications other than private messages.**

- **Exclusion of minor ancillary features** - CIPL **recommends that minor ancillary features** such as services for collaboration, minor chat functions (for instance a chat function in a video game) and the joint editing of files and documents are excluded from the scope of the ePR. This would be in line with the EECC[7] and would allow for innovation with respect to features that are not core to the services being provided.

- **Exclusion of data processing in the context of employment** - CIPL recommends that the ePR provides a clear exemption for employment-related processing, in particular from the **requirement to obtain consent** under the Regulation. The Parliament and Council Drafts focus primarily on consumers. However, a large amount of processing takes place on employee devices, and employers should not have to force consent from their workforce. This would also contradict with the DPAs' longstanding position that consent is not a valid legal basis for processing data in the context of an employment relationship as employees are generally not in a position to give free consent.[8]

- **Machine-to-machine data processing** - The sharing of M2M metadata can create significant socio-economic benefits, improve productivity and reduce the environmental impact of human activities in line with the EU's policy objectives under the digital and green transitions. Excluding M2M communications from the ePR's scope would **facilitate the data uses and sharing activities** necessary to achieve these aims (such as through the use of wind turbines and animal

[6] See Article 2(4) of Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[7] See Article 2(5) of Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code: "interpersonal communications service […] does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service."
[8] See WP 249, Opinion 2/2017 on data processing at work, adopted on 8 June 2017.

monitoring). In addition, obtaining consent for the purposes of M2M metadata use can be challenging and unduly burdensome as the specific nature of consent limits the extent to which insights can be generated. **CIPL recommends excluding use of M2M data from the ePR's scope.**

2. Interaction of the ePR with the GDPR

- **Scope of the ePR** - CIPL recommends that some clarifications are provided with respect to the scope of the ePR. In particular, it should be made clear when it applies (i.e., to data in transit), when it ceases to apply and when the GDPR starts to apply. **Article 2(2)(e) in the Council draft, which confirms that electronic communication data processed after receipt by the end-user are not within the ePR's scope and are instead governed by the GDPR, should be retained**. The extension of confidentiality to data collected from terminal equipment suggested under Article 5 of the Parliament draft should not be adopted.

- **Definitions** - Although the ePR provides that the definitions of the GDPR apply in the context of the GDPR, the ePR should clarify that terms such as **anonymisation** and **pseudonymisation** are defined and used in an identical manner both in the GDPR and the ePR.

- **Relationship between the ePR and the GDPR** - Finally, CIPL underlines that the relationship between the e-Privacy Directive and the GDPR is based on the principle of *lex specialis derogate legi generali*. As far as legal bases for processing are concerned, the EDPB has confirmed that Article 5(3) of the ePrivacy Directive shall take precedence over Article 6 of the GDPR with regard to the activity of storing or gaining access to information stored in the terminal equipment of a user, but that any processing of personal data which is not specifically governed by the e-Privacy Directive (or for which the e-Privacy Directive does not contain a "special rule") remains subject to the provisions of the GDPR, and "there shall only be a derogation from the general rule insofar as the law governing a specific subject matter contains a special rule."[9] **The ePR should maintain a similar approach**.

3. Definition of Electronic Communications Data

- **Consistency of definitions** - CIPL underlines that, overall, the draft ePR includes a vast number of definitions which are overwhelming and make an already complex technological landscape even more incomprehensible to end-users. There are, for instance, some subtle differences between electronic communication metadata and terminal equipment information. In Article 4(3)(c), data used to trace and identify the source and destination of a communication belongs to the metadata category and is therefore subject to the rules governing metadata. CIPL believes that such data could however belong also to the "terminal equipment information" category. **CIPL calls for**

[9] See paragraphs 38 and 41 of Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. See also Recital 173 of the GDPR and Recital 10 of the e-Privacy Directive.

simplification and consistency of terms and definitions.

- **Reminder to withdraw consent** - Article 4a(3) of the Council Draft provides that end-users that have consented to the processing of electronic communication data shall be reminded of the possibility to withdraw consent at least every 12 months, unless the end-user requests not to receive such reminders. The Parliament Draft removes the reference to regular reminders provided in the Commission's Draft. While end-users must have the right to withdraw consent concerning the processing of electronic communication data at any time, regular reminders risk confusing end-users with respect to this right. End-users already receive a large amount of information daily regarding their data protection rights. If these regular reminders were added, a situation might arise where end-users inadvertently withdraw their consent "as a precaution" leading to certain functions being reset and no longer available to them. **The Parliament approach that reminders are not required should be adopted**.

4. Security (Articles 6, 6a, 6b, 8)

- While the Commission, Council and Parliament Drafts all recognise the importance of processing data for network and information security purposes, the approach of the ePR is neither consistent nor comprehensive across the different types of data. In the Council Draft, for example, content and metadata can be processed for security of electronic communication networks and services and devices but not for the security of applications or for the security of data that run on them or information systems beyond the networks themselves. As provided in Article 8(2), connection data cannot be used for security purposes at all. Under the current Drafts, for example, an entertainment venue running a wireless network for use by the public would not be able to quarantine devices that are behaving abnormally on the network or detect rogue access points used by attackers to launch attacks against their customers. **All data categories and processing capabilities should have a consistent and comprehensive legal basis for security of networks, information and information systems.**

5. Processing of Metadata and Content Data (Articles 6, 6a, 6b)

- **Benefits of processing content data and metadata** - Processing of electronic communications data and metadata, with the appropriate privacy safeguards, is vital to the delivery of a range of digital services. For example, when aggregated and anonymised, such data can be used by car manufacturers in order to provide insights into car performance, charging practices and customer preferences with respect to comfort and car features. This not only benefits consumers, but can also create cleaner, safer cars that benefit society more widely. The processing of such data can also assist in the fight against climate change by helping energy companies monitor wind turbines and farmers ensure the productivity of livestock and machinery (usually in remote areas without fixed line connection). In the telecom sector, anonymised data insights can generate better value for customers. The utilisation of network bandwidth varies depending on geographical area and time of day. Just as the price of electricity varies depending on the region and time, dynamic rate

plans and resulting price cuts could be offered to customers depending on network utilisation in certain geographical areas. Customers in the respective network areas could be generically notified on a pseudonymised basis (without being identifiable) to receive offers for price savings due to lower network utilization as well as for other tariff recommendations.

- **Data processing for fraud prevention** - CIPL welcomes the inclusion of an exemption relating to cookies under Article 8 of the Council Draft that explicitly refers to fraud prevention. However, this exemption is not mirrored under Article 6 with respect to electronic communication data. Instead, there is only a limited exemption from consent to prevent security risks or attacks. Given the limited risks involved and the type of data (metadata), there should be a consistent exemption for fraud detection and prevention purposes across the text of the ePR. In the telecoms field, for example, the use of metadata is crucial for the detection of trends in fraud tactics such as those using SMS text. This in turn helps operators create machine learning tools to address the issue. Similarly, in the financial sector, the use of data to detect and prevent fraud is critical to ensure the security of payments of individuals, as well as the security of the whole financial ecosystem.

- **Data processing for the performance of a contract** - The ePR should provide sufficient flexibility for organisations to process metadata for purposes such as performance of a contract, such as for paying affiliates. This would also enable the provision of services with innovative features that benefit the end-user without requiring consent, such as "read receipt" notifications in messaging services. If this is not permitted, in practice consent could be required in order for the service provider to perform contractual obligations for the end-user, which means that any consent provided likely would not be "freely given." This exemption would also assist service providers in combatting potentially harmful behavior on messaging services, such as scamming, bullying or harassment. These purposes likely would not fall under the "vital interests" exemption, but may fall under the contractual necessity exemption. Requiring consent would prevent the service provider from tackling these issues as abusers likely would not consent to the use of the metadata associated with their communications. AI and machine learning solutions can also be deployed for these purposes, which is ultimately more privacy and safety preserving for individuals. **CIPL therefore recommends that the Council's approach under 6b(1)(b) be adopted**.

- **Data processing for vital interests** - The vital interest legal basis is also key to process electronic communication data for the safety of users. This includes preventing and navigating emergency situations that have a high impact on public safety or public health. The Council Draft rightfully explicitly recognises the importance of processing data in the vital interest for humanitarian purposes, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters. **This legal basis should be retained under Article 6(b)(1)(d) and Recital 17(a).** Vital interest and public interest and safety are also appropriate legal grounds for processing content data, particularly in the smart city or transport realm. Connected roadways infrastructure, for example, is covered by the ePR as it is a service offered to an unspecified group of end-users in a public space. Electronic communication data is used frequently, including for traffic signal prioritisation (for emergency or public vehicles) or

optimisation (for traffic management), vehicle-to-vehicle communication, traffic incident management, smart parking, road and road structure conditions and maintenance and dynamic rerouting. Content data may include video and sensor data on number, speed and location of vehicles. Given the lack of available interface with end-users in the vehicles, none of the proffered legal bases for processing content data (service provision, network, service or device security, legal obligation or consent) is currently available or appropriate. **The vital interest legal basis should be extended to all electronic communications data, including content, and ideally complemented by a public interest or safety legal basis.**

- **Data processing for compliance with a legal obligation** - CIPL welcomes the inclusion of compliance with a legal obligation as an exemption to the requirement for consent in the Council Draft under Article 6(1)(d). However, the exemption is limited to certain purposes, such as crime prevention or maintenance of public security. This creates a gap and may lead potentially to **conflicting obligations** for providers of electronic communication services. For example, under the Payments Services Directive 2 (PSD2), processing of personal data is permitted for fraud prevention purposes. The PSD2 also mandates Strong Customer Authentication, which requires data processing for such purposes. The security and stability of the payment system should not be dependent on individuals' consent. Obtaining explicit consent for activities mandated by law and regulatory standards is not desirable, meaningful nor practical as fraudsters would not consent. **The ePR should therefore broaden the exemption so that it avoids the need for consent when processing is required for the purpose of compliance with a legal obligation** generally, not just in selected areas.

- **Data processing for network management and optimisation** - CIPL welcomes the inclusion of a legal ground for metadata processing for network management and optimisation under Article 6b(1)(a). It should be recognised, however, that providers also use automated tools to scan communications – i.e., content data – for purposes that go beyond security of the network or service, such as to prevent data loss. These activities would be better served by **extending the network management legal basis to all electronic communications data.**

6. Compatible Purpose Exemption (Article 6c and Article 8(1)(g))

- **Scope of exemption** - The **compatible purposes exemption** is not included in the Commission proposal nor in the Parliament Draft. This exemption is key for innovation. For example, in the telecoms sector, aggregated and anonymised mobility insights produced on the basis of pseudonymous data from telecommunications networks represent a great example of human-centered digitisation, allowing socio-economic insights without profiling or intrusion on privacy.[10]

[10] Secondary use of metadata is critical to the development of new services and enhancement of the efficiency of telecommunication networks. This has been recognised by the Committee on the Internal Market and Consumer Protection in its Opinion 2017/0003(COD) https://www.europarl.europa.eu/doceo/document/IMCO-PA-604857_EN.pdf. "The rapporteur considers that processing of previously collected data for compatible purposes,

The Council's inclusion of a compatible purposes exemption for metadata under Article 6c is therefore essential. Without the flexibility and adaptability to permit the processing of electronic communication metadata for compatible purposes, there is a material risk that the ePR would inadvertently stifle technological innovation and prevent the development and improvement of new and existing services within the EU. Furthermore, sharing of data is often necessary in order to develop new services. In many cases, a single operator will not have access to all the technology that is needed, e.g., for network improvements, fraud management or customer value initiatives. Operators may need to share data with third parties to develop new services in the "proof-of-concept" or development phase. It is therefore important that the compatible purposes legal basis is broad enough to enable data sharing with the relevant technology providers. These kinds of activities may not be permitted under the current limited form of the compatible purposes basis, and the text should therefore be amended and further aligned with the GDPR in this regard.

- **Algorithmic training** - Because of the growing relevance of artificial intelligence (AI), CIPL also recommends that **algorithmic training be explicitly recognized as a compatible purpose.** In the telecoms sector for instance, AI systems are required to combat fraud and protect consumers from fraud scams. There is no appropriate legal basis to rely on for the training phase of AI used for these purposes other than compatible purposes. Consent is inappropriate as low or irregular opt-ins and withdrawal of consent result in low-quality datasets, and the exploratory nature of AI means that repeated consents would be needed. It is also generally not possible to collect consent that would be considered specific, informed and unambiguous in the context of AI and machine learning.

- **Consistent definition** - For consistency purposes, the conditions to process personal data under the compatible purpose exemption (metadata in Article 6c and collection of data from end-users' terminal equipment in Article 8(1)(g)) should align with one another and ideally with the GDPR's legal basis for compatible further processing (Article 6(4) of the GDPR). **The GDPR is version is more flexible and strikes the right balance between protecting privacy and allowing for innovation**.

7. Business Software Updates and Cookies (Article 8)

- **Cookie walls** - A ban on cookie walls would have a major impact on business models that depend on advertising revenue, which could in turn impact the diversity of online media. The GDPR already provides for sufficient safeguards around the validity of consent, including a requirement for consent to be "freely given." As such, the restrictions around the use of cookie walls in the Parliament Draft should be removed, and the ePR should instead align with the GDPR's requirements with respect to consent and not impose additional requirements. The ePR should

such as the development of services that ultimately provide added value for the end-users and their user-experience, public authorities and businesses should be allowed."

also remove the references under the Council draft to **"dominant positions"** undermining the validity of consent. This is a competition law concept that is irrelevant in the data protection field. DPAs would not have the relevant competences and skills to determine whether or not a cookie wall is compliant under these restrictions.

- **Consent at browser level** - The process of collection of consent at browser level under Article 10 in the Commission proposal and the Parliament Draft is disruptive to the user experience and should be removed. Article 10 proposes that electronic communications software should present end-users with privacy settings allowing them to accept or reject cookies. The Parliament Draft adds the requirement for electronic communications software providers to configure software so that privacy is protected, and a default prohibitive approach is adopted with respect to cookies. The Council has suggested deleting this provision. Having a restrictive, default-refusal approach with respect to functionality cookies will disrupt the user experience and leave electronic communications software providers to determine whether a cookie is "strictly necessary" or not, which is not within their remit and could compromise service provision and security for end-users. Therefore, **the Council approach should be retained**.

- **Harmonisation** - In order to avoid divergent categorisations of cookie consent mechanisms and lack of common interpretation, regulators should be encouraged to release consistent guidance on how cookies should be categorised at the EU level.

- **Consent to software updates** - Article 8 of the Council Draft requires the consent of the end-user for software updates. But when the end-user is a legal entity, further clarification is needed to ensure that the legal entity can give consent to software updates on behalf of their employee on terminal equipment owned or managed by the employer or otherwise used in the context of employment. Almost every company today uses connected terminal equipment for business purposes. Industry, retail, health services – all sectors work with tablets, laptops or smartphones to process customer data, control robots or generate medical files. The software needed for this must always be updated to the version which meets the company's needs so that digitised processes can function seamlessly in offices, factories and hospitals. To ensure this seamless functioning, companies – as end-users – must be able to decide what security-critical software updates need to be made in order to be able to protect their IT security infrastructure and beyond. As end-users, companies and legal entities must therefore be able to give consent to a software update. Where the use of in-house devices is concerned, legal entities must be able to carry out security updates, provided that the provisions of GDPR and rules on employee protection are complied with.

8. Exemptions to data processing from end-users' terminal equipment (Article 8)

- **PET and PPT exemption** - The Drafts currently have a binary approach – either technology is considered safe or unsafe. This means that privacy-preserving technology is treated the same way as privacy-intrusive technology (requiring consent), which is counterintuitive given the aims of the

ePR. CIPL recommends that the ePR permit a risk-based, rather than binary, approach. Alternatively, if the law wants to ensure better privacy, **an exception to enable use of privacy enhancing (PET) or privacy preserving technologies (PPT)** should be specifically included under Article 8 and Recitals 20 and 21 of the ePR.

- **Legitimate interest exemption** - In addition, some form of "legitimate interest" exemption should be included in the ePR. Currently, **data cannot be used for the benefit of anyone other than the user to whom a service is directly provided** (under the service provision exemption). In a brand to consumer relationship, for example, the processing of personal data should be based on a brands' legitimate interest in getting to know their customers' preferences in order to be able to offer products and services that better meet the needs of their customers generally. Similarly, in the context of connected cars, allowing data to be used for service improvement and safety more generally would benefit everyone. It should be noted that, in this context, where one person withholds consent to processing, this may actually have an impact on the safety of others. Safety concerns provide a more general justification for processing in other areas, such as with respect to children's communications and data. **CIPL recommends that this concept is extended to cover circumstances where data use would have a significant impact on the safety of other users of a service or society as a whole.**

- **Necessity threshold** - With respect to the service provision exemption provided under Article 8(c), the threshold of "strictly technically necessary"/ "strictly necessary" is high and in practice will require additional user consent in order to be able to use all the functionalities of a specifically requested service. Use of the processing and storage capabilities of end-user terminal equipment and collection of information from that equipment should be permitted without the end-user's consent if it is necessary for the provision of services requested by the customer. The current thresholds mean that the functionalities required for providing a user-friendly and safe service require additional consent, which undermines the purpose of this exemption. For example, some cookies are used to assist in fraud prevention. These do not fall under the exemption as drafted, but should not require consent. Similarly, if an insurer provides telematics-based motor insurance that depends on the processing of data from terminal equipment (e.g., via mobile phone apps or connected vehicles), the ePR should not require them to seek additional consent from the customer that requested the product. **As such, CIPL recommends removing the words "strictly" and "specifically" from the Council drafting of Article 8(1)(c).** This would bring the wording of the ePR in line with the GDPR's contractual necessity legal basis.

- **Audience measurement exemption** - As currently drafted, the audience measurement exemption is unnecessarily restrictive and does not permit data sharing with third-party providers carrying out measurement on behalf of the organisation. Audience measurement is a legitimate and necessary purpose for processing data as it allows service providers to understand how their services are used and whether their features are working and to establish user engagement. These activities are not designed to monitor individuals. They are designed to look at patterns and trends at an *aggregate level* and are essential for organisations in many instances. Because the data is

aggregated, there is a minimal impact on individuals. For example, bloggers often use third-party providers and tools to measure visits to their website and levels of interaction with website features. This helps them improve their content and design, benefitting their users. In some instances the data is not only helpful but critical. In addition, in order to accurately bill advertisers, cookies that measure how often advertisements are shown must be used by publishers**. As such, the Council's version of the audience measurement exemption should be adopted.** Frequency capping that avoids that individuals be presented with the same advertisement several times should also be included as a specific exemption.

- **Legal obligation** - The grounds for processing electronic communications data to meet a legal obligation should also be extended to device processing and storage capabilities or information collected from the device. For example, several national laws currently provide the possibility for authorities to require the placement of software enabling surveillance on a device for counter-terrorism purposes. **The legal obligation ground for processing should also be available in the context of processing on end-user terminal equipment**.

9. Connection Data (Article 8.2)

- **Relation to metadata** - Data emitted by a device is necessary to enable such device to connect to another device or to a network. This architecture is a standard across wireless networks. Devices need to broadcast who and where they are and how they can connect in order to be found and connected to the network. Such connection data is a subset of metadata. It is the "who, what, where, when?" that enables communication to be established in the first place. However, the Council and Parliament Drafts currently classify connection data as an entirely independent category of data. While the Commission's Draft subjects connection data to the most relaxed set of requirements, the Council and Parliament Drafts are much more stringent. This is completely at odds with the metadata category (of which connection data are part) that have the broadest grounds for processing under the ePR. **CIPL recommends ePR revert to the Commission's original proposal for Article 8(2) and provide at minimum that Article 8(2) should be without prejudice to Articles 6 and 6b.**

- **Establishing and maintaining connection and network management and optimisation** - The Parliament Draft provides that reliance on this legal basis requires the *service to be requested* by the end-user. This provision endangers the entire architectural model of wireless technologies, which rely on devices to announce their presence to prospective networks in order for such networks to be discoverable by the end-users' devices. At face value, the Parliament Draft would restrict users to connect to networks they have preconfigured and therefore requested connection to – e.g., their home wi-fi. The Council Draft focuses on establishing or maintaining a connection – which is narrower than the "provision of the service" legal basis available to all other categories of data but at least does not include the user request requirement contained in the Parliament Draft. In addition, connection data is necessary for other purposes than just establishing a connection. In an airport wi-fi network used by passengers, for example, connection

data can be used for optimisation of the network to cope with high-volume traffic and promote under-utilised routers. **The legal grounds for processing metadata for network management and optimisation should be extended to connection data.**

- **Security** - In the Council and Parliament Drafts, connection data cannot be processed for security purposes, whereas such use is essential to the safe operation of the networks and the protection of their users. **The legal grounds for processing metadata for security purposes should be extended to connection data.**

- **Legal obligation** - In the Council and Parliament Drafts, connection data cannot be processed for the performance of a legal obligation, whereas such use is essential to comply with law enforcement data access requests. **The legal grounds for processing metadata for the performance of a legal obligation should be extended to connection data.**

10. Direct Marketing

- **Definition of direct marketing** - The reference to material "presented" to individuals under the definition of direct marketing communications in Article 4(3)(f) of the Parliament Draft should be removed in order to clarify that the display of advertising on a website or within an information society service requested by the end-user is not caught by the scope of the ePR's direct marketing provisions. The display of advertising is an important revenue stream for services that are provided to individuals for free. Removal of this revenue stream could prevent new and innovative businesses from entering the market as this is often the only way that small businesses can enter the market while offering services for free.

- **Consent of legal persons** - The distinction between business-to-business and business-to-consumer marketing should be explicitly maintained, with a reference to end-users who are "natural persons" under Article 16(1) of the ePR, as in the Council Draft. However, it should not be left to Member States to determine a position on consent with respect to legal persons. This will lead to disparity and a lack of consistency across the EU, and the varied implementation of the GDPR has demonstrated that this can present difficulties for organisations established in multiple EU Member States. CIPL recommends providing a definitive position in the ePR as to whether opt-in consent is required for the delivery of direct marketing to legal persons.

- **Similar products and services** - In order to provide legal certainty and resolve existing uncertainties that have arisen from case law (such as in German case law and doctrine[11]), the term "own similar products and services" should be defined under Article 16(2) or explained in the recitals of the ePR. It should be made clear that the phrase "own similar products and services"

[11] See jurisdiction by Kammergericht Berlin KG Beschl. v. 18.3.2011 – 5 W 59/11 at BeckRS 2011 and Oberlandesgericht München OLG München, Urteil vom 15.2.2018 – 29 U 2799/17 (LG MünchenI), as well as literature, especially Köhler/Bornkamm/Feddersen/Köhler, 39. Aufl. 2021, UWG § 7 Rn. 205 and MüKoUWG/ Leible, 3. Aufl. 2020, UWG § 7 Rn. 183-185

includes all products and services that derive from the same *sector*. For example, a food market should be able to send direct marketing for other food products and related services. The same goes for financial service providers, such as insurers.

- **Groups of companies** - The ability to advertise similar products under the "soft opt-in" exemption should not be limited to natural or legal persons but should also include groups of companies. The structure of a company should not affect the right to conduct direct advertising for similar products.

11. Enforcement of ePR (Chapter IV)

- **Leverage the DPAs** - While the Commission and Parliament Drafts import the GDPR one-stop-shop (OSS) mechanism, the Council Draft permits entrustment of enforcement power to separate supervisory authorities, subject only to a cooperation obligation with one another and with the EU Commission. The creation of different avenues for enforcement between the ePR and the GDPR is impractical, especially given the overlap between the GDPR and the e-Privacy regimes. It may lead to the creation of different thresholds for initiating investigations or overlapping investigations with different drivers. Enforcement should be specifically given to the regulator responsible for the GDPR (i.e., the DPAs), and the GDPR's OSS mechanism should be applied under the ePR. This would help to ensure that service providers and users face a consistent and uniform interpretation of the ePR and would enable businesses to leverage their existing relationship with their Lead DPA under the GDPR. This position is fully supported by the EDPB, which has stated that "[o]versight of privacy provisions under the ePrivacy Regulation should be entrusted to the competent supervisory authorities under the GDPR [the DPAs] to further support consistency."[12]

- **Reduce potential enforcement overlap** - The potential for overlap in enforcement between the GDPR and the e-Privacy Directive has been raised by Advocate General Bobek, who identified that (1) the e-Privacy Directive and the GDPR may apply at the same time, or may not, depending on the actual provision that has been allegedly breached; and (2) the OSS does not apply to the e-Privacy Directive.[13] This potential overlap of enforcement regimes between the GDPR and the future ePR is a sensitive area in which the possibility of double jeopardy – an unacceptable outcome incompatible with basic legal rights and the rule of law as set forth both in the GDPR and the EU Charter of Fundamental Rights – remains a threat to organisations. The interface between the two regimes is very close, though the requirements of the laws are, at times, inconsistent with one another. There are cases which could potentially be treated as falling into either regime but result in different outcomes depending on whether the GDPR or the e-Privacy Directive is applied. In one case against Facebook, the Belgian DPA alleges unlawful collection and use of information by means of cookies on the basis of the national Belgian law implementing Directive 95/46[14] (later

[12] See EDPB Statement 03/2021 on the e-Privacy Regulation of 9 March 2021.
[13] See Case C-645/19 Facebook v Gegevensbeschermingsautoriteit. See Opinion of the Advocate General Bobek.
[14] https://www.dataprotectionauthority.be/the-judgment-in-the-facebook-case

replaced by the GDPR). The French DPA takes a different approach in a case against Google and Amazon by sanctioning the lack of transparency and consent on the placing of cookies on the basis of French law implementing the e-Privacy Directive.[15] If the ePR fails to align with the GDPR OSS, organisations will have to deal with both the competent lead DPA under the GDPR in relation to the GDPR-related aspects of a matter and a national DPA that takes parallel actions in respect of the e-Privacy aspects, even though the factual issues may be the same or relate to the same processing.[16]

- **Improve harmonisation** - Now that e-Privacy is changing from a Directive to a Regulation that is directly applicable in all Member States, it will be necessary for the OSS apply to ensure the harmonisation objectives of the ePR are met at all stages, including at the enforcement level, to avoid recreating the fragmentation that the ePR is seeking to address. The absence of OSS in the e-Privacy landscape would go against the principle of the free movement of services by creating clear inefficiencies that might also have the effect of excluding smaller operators from creating EU-wide services. Finally, it is critical that GDPR OSS efficacy be improved so that it serves as a blueprint for other upcoming digital initiatives where organisations would benefit in having a single point of contact or interlocutor on enforcement matters, such as the draft AI Act,[17] the draft Digital Services Act[18] or the draft Data Governance Act.[19]

- **International cooperation** - CIPL recommends the inclusion of a specific and effective cooperation mechanism with respect to third-country regulators, particularly the UK ICO.

12. Remedies (Article 21)

- **Harm-based approach** - Under its current version, Article 21.1 of the ePR essentially allows anyone to bring proceedings following an infringement, even where they have not been adversely affected. This article should be clarified and narrowed. If it were retained, it risks enabling all natural and legal persons, including competitors, to bring cease and desist claims before courts for alleged infringements of the ePR without evidencing any harm. This could result in anti-competitive behavior and vexatious, frivolous and abusive litigation. This is in line with neither the GDPR's approach to standing in Article 79 GDPR nor the general principles of harm.

[15] https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core ; https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland

[16] See for instance the case launched by France Digitale against Apple handled by the CNIL under the e-Privacy Directive. This follows a similar case handled by the Irish DPC on the basis of the GDPR. https://www.hebergementwebs.com/apple/apple-vs-france-digitale-the-cnil-takes-up-the-case

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[18] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

13. Encryption

- **Security of data** - The use of encryption as a means of protecting end-users and preventing misuse of systems and data is essential in the development of secure and reliable technologies and is important to end-users. Encouraging the use of encryption is also consistent with the GDPR, which promotes the use of encryption and explicitly recognises that it can be valuable for the purposes of ensuring security of data and limiting the impact of data breaches. **CIPL therefore recommends adoption of the Parliament's Draft on encouraging the use of encryption in the context of ePR, as set out in Article 17(1a), Recital 26(a) and Recital 37.**

14. Application of the ePR

- **Reasonable delay** - The Council Draft's provision under Article 29 that the ePR applies **24 months from the date of entry into force should prevail**. This will provide organisations with enough time to thoroughly implement new requirements under the Regulation.

If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, or Markus Heyder, mheyder@huntonAK.com.