April 2021

DOT Europe Recommendations ahead of the

Trilogue Negotiations on the draft e-Privacy Regulation

Introduction

As the European Commission ("**the Commission**"), the European Parliament ("**the Parliament"**), and the Presidency of the Council of the European Union ("**the Council**") continue preparing for the upcoming trilogue negotiations on the draft e-Privacy Regulation ("**ePR**")[1], it is crucial to consider the time it has taken to come to this point.

Originally proposed by the Commission in January 2017, the over three years of negotiations have not only witnessed technological change, but also the entry into force of several key pieces of legislation, namely the European Electronic Communications Code ("**EECC**")[2] and the General Data Protection Regulation ("**GDPR**")[3]. This has created a very different legal landscape for the ePR to fit into, raising questions of applicability of the draft law to today's technological reality as well as coherence with these other pieces of legislation.

In this paper, we touch upon the areas of the draft ePR that we encourage negotiating parties to consider ahead of forming compromise amendments. The below document makes recommendations to strengthen the Commission's original proposal, while constantly emphasising alignment with the GDPR.

Scope – Transmission of Electronic Communications Data (Article 2(2))

Issue: It is essential to clearly define the scope of the draft ePR by **excluding electronic communications data ("ECD") processed after receipt by the end-user concerned**. If this is not done, there exists a significant risk that lawful and sensible processing activities would be unduly prohibited. To the extent that the further processing of such data requires any additional protections under EU law, there are existing applicable laws (notably the GDPR) that would provide the required additional protections.[4] Excluding ECD that have been received by the end-user from the scope of the draft ePR does not lead to any material reduction in the protections that are appropriate in relation to such data.

[1] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

[2] Directive (EU) 2018/1972 establishing the European Electronic Communications Code

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[4] All of the compliance obligations set out in Chapters II, III and V of the GDPR are likely to apply to ECD, to the extent that such data constitute personal data

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 2 626 1990

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

This is currently most clearly spelt out in the Council's amendments, which introduce the principle that the ePR should not apply to ECD processed after receipt by the end-user concerned[5]. As is noted in the Council text, receipt of ECD by the end-user implies that the end-user has gained control over such data[6]. Once the end-user has gained control, it is logical that the end-user should have the option of processing ECD as they see fit, without being subject to the restrictions and obligations set out in the draft ePR. Likewise, end-users should be free to mandate third-parties to process or store such ECD on their behalf without having to satisfy the compliance requirements of the draft ePR.

Recommendation: **We recommend that the co-legislators adopt and maintain the Council's proposal on the scope of the draft ePR**. Specifically, we recommend that Article 2(2) of the draft ePR should explicitly exclude from the scope of the draft ePR ECD that has been received by the intended end-user(s).

Scope – Minor Ancillary Services (Article 4(2))

Issue: The Commission and the Council state in Article 4(2) and Recitals 11, 11a, and 13 that the draft ePR will apply to minor ancillary features that are intrinsically linked to another services such as chats in documentation programmes or the case of online games. We understand that the Parliament also has the intention to include minor ancillary services into the scope of the draft ePR.

Including minor ancillary services into the scope of the draft ePR is inconsistent with the definition of an Interpersonal Communication Services ("**ICS**") as established in Article 2(5) of the EECC. It would impact the development of new digital services that come with features that are not core to the services, but do provide users with the ability to communicate with other users. This also runs counter to the EECC where ancillary features are specifically carved out of the definition of ICS.

Recommendation: We recommend that the co-legislators recognise that **minor ancillary services should be excluded from the scope of the draft ePR**, in accordance with the definition of an ICS as established in Article 2(5) of the EECC.

Permitted Processing of Electronic Communications Data (Articles 6 & 8)

The ability of service providers to process ECD and data collected from terminal equipment, is one of the core components of the draft ePR. DOT Europe has long advocated for closely aligning the legal basis for processing with those found in the GDPR[7]. **The original Commission proposal along with the amendments of the Parliament remain highly restrictive and would lead to a situation in which user consent would be required for the overwhelming majority of use cases**. This would create obstacles for the "domestic EU development" of promising technologies including those based on artificial

[5] See Article 2(2)(e) of the Council Text
[6] See Recitals 8a and 15a of the Council Text
[7] See Article 6 GDPR

intelligence ("**AI**") and the Internet of Things ("**IoT**"). We welcome the amendments of the Council, which introduce additional flexibility into the draft ePR, with a particularly focus on:

- Performance of an Electronic Communications Contract (Article 6b(1)(b))

Issue: The Council text introduces a legal basis which would permit (among other purposes) the processing of electronic communications metadata to the extent that such processing is necessary for the performance of an electronic communications services ("**ECS**") contract to which an end-user is a party. This provision allows for metadata processing that is necessary to provide agreed service features (other than mere transmission) in accordance with the terms of a contract. **The introduction of such a legal basis will be pivotal to ensuring that end-users are able to continue to receive a product experience they've come to expect.**

For example, many instant messaging services offer features such as predictive text including the ability for users to see whether a message has been read or received by the recipient(s). The Council's text would allow ECS' to continue offering such features without requiring (additional) consent from the end-user.

Recommendation: We recommend that the co-legislators adopt and maintain the Council's proposal on **performance of a contract as a valid justification for the processing of electronic communications metadata**, as set out in Article 6b(1)(b) of the Council text.

- Compatible further processing of electronic communications metadata (Article 6c)

Issue: The Council text introduces a legal basis for compatible further processing of electronic communications metadata. This is an essential provision to allow for innovation in the electronic communications space. It clarifies that such data may be processed in pseudonymised form for further purposes providing that the processing meets the conditions of the legal basis, which align with the corresponding GDPR provision.[8] **Without the flexibility and adaptability to permit such processing for compatible purposes, there is a material risk that the draft ePR may hinder technological innovation.**

For example, an ECS would like to introduce a new feature or technically improve its services, but first needs to understand the impact of the product changes on the performance on their service. To do this, the ECS would need to be able to access communications metadata to measure, for example, the impact of the speed of transmissions, or the number of failed attempts to send big files. The Council's proposal provides a helpful legal basis to conduct such activities necessary to improve the service of an ECS.

Recommendation: We recommend that the co-legislators adopt and maintain the Council's proposal on **permitted processing of electronic communications metadata for compatible purposes**, as set out in Article 6c of the Council text.

[8] See Article 6(4) GDPR

- Vital Interest (Article 6(b)(1)(d))

Issue: The Council text introduces a vital interest legal basis for the processing of electronic communications metadata. The introduction of this legal basis is important for protecting end-users and the wider public. This includes preventing and navigating emergency situations that have a high impact on public safety or health. The Council rightfully explicitly recognises the **importance of processing in the vital interest for humanitarian purposes**, including for monitoring epidemics or in humanitarian emergencies, in particular natural and man-made disasters.

Recommendation: We recommend that the co-legislators adopt and maintain the Council's proposal for a vital interest legal basis, as set out in Article 6(b)(1)(d) and Recital 17(a).

- Security Purposes (Article 6(1)(c))

Issue: ECS' are currently under obligation to implement appropriate technical and organisation measures to ensure a level of security appropriate to the risk within the EECC[9] and the GDPR[10]. The Council introduces language[11] that explicitly recognises these applications and introduces a legal basis for the processing of ECD to prevent security risks or attacks on end-users' terminal equipment. The Council rightfully provides service providers the much-needed **legal certainty** to ensure they can **process ECD to implement technical and organisation measures to ensure a level of security appropriate to the risk of their service**.

For example, the analysis of ECD associated with malware transmitted using an ECS that is specifically targeting end-user's terminal equipment may not otherwise present a security risk to the ECS itself, and would not be permissible under the Commission or the Parliament texts.

Recommendation: We recommend that the co-legislators adopt and maintain the Council's proposal to process ECD to prevent security risks or attacks on end-users' terminal equipment, as set out in Article 6(1)(c).

- Audience Measurement (Article 8(1)(d))

Issue: The Council text introduces a more progressive approach to the issue of audience measurement. This is an important addition for many services providers as the measurement of audiences is a legitimate and necessary aim. Such measurement enables services providers to accurately understand the ways in which their services are being used, including understanding whether new features are working as intended, along with being able to accurately assess end-user engagement. The purpose of audience measurement is to look for patterns/trends and to report aggregated analysis, and not individual results. It is **an essential activity for businesses, including SMEs, to grow their businesses across the EU Single Market**.

[9] See Article 40 EECC
[10] See Article 32 GDPR
[11] See Recital 15(aaa) in the Council Text

For example, companies with a commercial weblog use audience measurement to measure the number of people who have visited their website, and the time for which people have visited specific pages on their website. This way, they can understand what kind of topics, or design features, of their website are of the most interest to their audience. With such insight, they can improve the content or design of their weblog to stay relevant to their audience.

Recommendation: We recommend that the co-legislators adopt and maintain the Council's proposal on audience measurement, as set out in Article 8(1)(d).

Privacy settings of Electronic Communications Software (Article 10)

Issue: The Commission proposal states that electronic communications software should present end-users with privacy settings allowing them to accept or reject the storage or access of information on their terminal equipment. The Parliament added the requirement that electronic communications software shall configure the software so that privacy is protected, and that cross-domain access of information on terminal equipment by third parties is prohibited by default. The Council suggested deleting this provision.
It is clear that Article 10 was very much **drafted with browsers in mind and with limited assessment of how it might work in the vastly different mobile ecosystem**. Having electronic communications software operate as a mandatory gatekeeper is likely to disrupt the functionality of services and disproportionately empower certain actors. This is particularly concerning with the Parliament text. Creating a regime with such a restrictive approach will lead to a disrupted experience in that the electronic communications software would gain control over what is "strictly necessary" or not.

The explicit objective of **the draft ePR's technology neutrality must be upheld**. Codifying into law how products should engage with their users, which limits companies' freedom to innovate and develop the most efficient way to interact with people, is anything but future proof.

Recommendation: DOT Europe recommends that the potential impact of Article 10 is taken into account and **the Article be amended to be more technology-neutral** as part of trilogue negotiations.

Supervisory Authorities and Enforcement (Articles 18-20)

Issue: The Commission proposal states that the monitoring and application of the draft ePR should be conducted by the supervisory authorities appointed by each EU Member State under the GDPR[12], with responsibility for ensuring a consistent application of the draft ePR falling to the European Data Protection Board ("**EDPB**")[13]. Furthermore, the Commission proposal imposes an obligation on supervisory authorities to cooperate with one another in respect of the consistent application of the

[12] See Recital 39 and Article 18 of the Commission Text
[13] See Article 19 of the Commission Text

draft ePR[14], and effectively imports the one-stop-shop ("**OSS**")[15] mechanism from the GDPR. The Parliament text replicates this approach, with the addition of helpful clarifications regarding the roles of supervisory authorities.[16]

The implementation of an OSS mechanism in the draft ePR is vital to the long-term success of the Regulation. As has been amply demonstrated since May 2018, the equivalent mechanism in the GDPR has ensured that data controllers (in most cases) deal with a single lead supervisory authority. This has helped to ensure that data controllers face a consistent and uniform interpretation of the GDPR and has also enabled businesses to establish a working relationship with their lead supervisory authority.

The alternative would be to fracture the regulatory system. Without an OSS, there is a significant risk that businesses would face an inconsistent application of the draft ePR and would be subject to parallel regulatory and enforcement actions by multiple supervisory authorities. This would deter business investment in Europe.

Recommendation: We recommend that the co-legislators adopt the statement, "*Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis"*, as set out in Article 18(1) of the Commission and Parliament texts. This approach is essential to ensuring consistency between the GDPR and the draft ePR in respect to enforcement and regulatory oversight.

Legal Standing of Entities to Bring Proceedings (Article 21)

Issue: The phrasing of Article 21(2), in the Commission, Parliament and Council texts, leaves the interpretation open that natural and legal persons do not need to be adversely affected by infringements of the draft ePR in order to bring legal proceedings against a service provider. This risks enabling all natural and legal persons, including competitors, to bring cease and desist claims before courts for alleged infringements of the draft ePR without evidencing any harm and its attribution to the relevant person and the draft ePR infringement.

This could cause numerous unfounded proceedings by anyone who wants to bring a case forward. If not corrected, anti-competitive behaviour, and frivolous/abusive litigation could be expected, as any business could bring proceedings against other businesses, without having been adversely impacted. This is neither in line with the GDPR's approach to standing[17] nor with the general principles of harm.

[14] See Article 20 of the Commission Text
[15] See Article 18(1) of the Commission Text: "*Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis*
[16] See Amendment 143 of the Parliament Text
[17] See Article 79 GDPR

Recommendation: **We recommend that the co-legislators clarify in Article 21(2) that other natural and legal persons will also need to have been adversely affected by infringements of the draft ePR** in order to be able to bring forth proceedings. If the co-legislator intended to include representation, it must align this provision with Article 80 GDPR.

Encryption and Privacy-Enhancing Technologies (Article 17)

Issue: Encouraging the use of end-to-end encryption ("**E2EE**")[18] and creating incentives for privacy preserving technologies can be a valuable contribution to protecting users. However, we would caution against mandating the use of specific technologies, such as E2EE. Service providers should be free to implement the privacy-preserving technology which achieve the most appropriate level of security taking account of the potential harm to the customer and which achieve the objectives of the ePR.

We also believe the draft ePR should mirror the approach of the GDPR, by providing encouragement and incentives for companies to incorporate privacy-by-design and privacy-enhancing technologies ("**PETs**") into their operations. This can provide better protection and an enhanced user experience, without compromising on innovation and the benefits of advertising-based business models. Creating incentives for the use of privacy-preserving technologies would reflect the objectives of the draft ePR, make it future-proof and technology-neutral while strengthening the trust of users in the Internet and the use of digital services.

For example, the ePR should **incentivise the use of privacy-preserving technologies** that would still allow for online advertising that underpins business models that have contributed to the open access to quality information, innovative services and communication on the web.

Recommendation: We recommend that the co-legislators support the use of PETs, such as E2EE, into their operations, but refrain from imposing certain technologies on companies. Companies should be free to choose the best available PET taking account of the risk to customers. This will ensure a future-proof legislative regime.

[18] See Amendment 29 of the Parliament Text