Connect Europe and GSMA comments on the Digital Omnibus Proposal
April 2026

Connect Europe and the GSMA, the industry associations representing telecoms operators in Europe, welcome the European Commission's focus on regulatory simplification and competitiveness, and take note of the initiatives proposed through the Digital Omnibus proposal. In our view, it is an extraordinarily important moment to deliver on these goals, particularly as the telecommunications sector faces significant changes, namely brought by the Digital Networks Act (DNA) and Cybersecurity Act review (CSA2). However, while we welcome the reduction of unnecessary red tape in certain areas, there remains much more to be done to truly support Europe's digital ecosystem and allow its core players to focus on continuing to provide the quality of connectivity the continent's citizens and businesses need and expect.

Several significant areas of regulatory burden remain unaddressed within the proposal, and others require further clarification, which we believe deserve urgent attention. This includes aspects related to the continued effects of the ePrivacy Directive, the proposal for an EU-single entry point for incident notification and the proposed targeted amendments to the General Data Protection Regulation (GDPR). In this paper, we underline our main messages in this respect and invite you to take note of what remains to be problematic for the European telecommunications sector. Making these changes will support our mutual goal of uplifting European businesses and cutting regulatory overlaps, resulting in an improved framework that centres innovation and competitiveness as core principles.

1. ***The ePrivacy Directive:*** *The ePrivacy Directive is outdated and must be repealed. The principle of confidentiality of communications should be maintained and integrated into horizontal legislation.*
2. ***The EU Single-Entry Point for Incident Notification:*** *The proposed Single-Entry Point must ensure that incidents may be reported at national level and only once, in accordance with best practice and cybersecurity legal provisions. It should not create further burdensome procedures rather than simplifying existing ones.*
3. ***The GDPR:*** *The risk-based approach of the GDPR should be respected, and its core principles maintained. Targeted adjustments on personal data are necessary to align with the 2025 ruling by the CJEU recognising the role of privacy-protecting techniques.*

1. The ePrivacy Directive

Immediate repeal of the ePrivacy Directive

European telecommunications providers continue to struggle with the fragmented and duplicitous nature of the ePrivacy Directive, with the Directive's legal obligations applying exclusively to telecom operators, thus placing operators at a comparative disadvantage. As such, we reiterate our call for the **repeal of the ePrivacy Directive in its entirety**, and the **incorporation of the principle of the confidentiality of communications into horizontal EU law that would foster innovation and better protect personal data**.

The ePrivacy Directive has explicit impacts on the telecommunications industry, with full implementation marred by disproportionate obligations, fragmented legal application and legislative

inconsistencies with existing EU law. More specifically, the Directive (particularly Articles 6 and 9) imposes unique legal requirements exclusively on telecommunications operators that do not apply to other digital service providers. This creates regulatory asymmetries that place telecom operators at a competitive disadvantage, distorting the level playing field within the digital single market, maintaining stricter rules solely for telecommunications providers over other sectors. Furthermore, the implementation of the ePrivacy Directive has varied significantly across EU Member States, resulting in a fragmented regulatory landscape that generates legal uncertainty across markets. As a consequence of this, the current legal framework casts limitations on the adoption of the large-scale innovative services, such as authentication APIs in initiatives like Open Gateway[1], or advanced anti-fraud and security-related technologies such as anti-spam filters that could otherwise add significant benefits to enhancing consumer protection. It also questions the management of operators' data in the context of AI transformation.

It should be recalled that the ePrivacy Directive was conceived in the context of the 2002 environment of linear communications and basic terminal equipment, and cannot natively accommodate today's multi-channel, cross-platform, cloud-based and AI-driven communications models. Retaining the ePrivacy within this modern context perpetuates a dual regime that is conceptually inconsistent and highly challenging to operate in. Moreover, the Digital Omnibus proposal, instead of repealing the ePrivacy Directive, introduces narrow derogations and exceptions by means of other legal acts and legislative measures (Child Sexual Abuse Material, eEvidence, Article 88a, the Third Payment Services Directive, etc.), and introduces Article 88a GDPR as a *lex specialis* for access to and storage of personal data in terminal equipment, while residual Article 5.3 of the ePrivacy Directive remains for non-personal data. This produces an inverted and counter intuitive situation: a more permissive, risk-based GDPR regime applies to personal data, while the stricter Article 5.3 long survives for non-personal data. Instead of simplifying, the coexistence of Article 88a and Article 5.3 multiplies interpretative questions and enforcement uncertainty. Likewise, the GDPR's risk-based approach is solely implemented in relation to the processing of personal data in the terminal of natural persons, but not in relation to traffic data, although both processing was regulated similarly under the ePrivacy Directive. This leads to the telecom sector in Europe being the only sector still subject to the more restrictive and discriminatory approach set out within the ePrivacy Directive and thus, unable to benefit from the simplification efforts proposed by the European Commission.

As a consequence of this, there remains a risk of fragmentation during the transitional period where Article 5.3 remains fully operational in national laws until amended, while Article 88a will apply directly under the GDPR, potentially exposing data controllers to overlapping, or even contradictory, obligations.

2. The Single-Entry Point for Incident Notification

Connect Europe and GSMA take note of the Digital Omnibus's proposal for a single-entry point (SEP) for reporting, which could present an opportunity to simplify the reporting process for cybersecurity incidents. We support the ambition behind the tool and see a strong need to improve on the status quo, both to reduce unnecessary bureaucracy but also to adequately support legal clarity and security incident management. However, clarity is still needed to ensure that incidents only need to be reported once, and it should not create further burdensome procedures instead of simplifying existing ones.

Anchoring the SEP at national level

Telecom operators must report security incidents and vulnerabilities through multiple different laws,

[1] GSMA Open Gateway

some of which have clear national contexts or national focuses. We strongly believe that administrative burdens should be reduced and support the aim to streamline reporting requirements across relevant legislation. In our view, the Digital Omnibus proposal for an EU single-entry point should be clearly anchored at national level for initial operational notifications, to effectively take stock of both the national and EU-level frameworks in incident reporting, considering the practical realities of incident management and cybersecurity. It should reflect the 'once-only' principle, meaning that just one notification would need to be submitted through a single-entry point in each EU Member State. The same report should then be made available to all relevant competent authorities, while fully respecting relevant requirements on IP and Trade Secrets stemming from national and EU law, as well as cybersecurity best practices in the handling and storing of such incident notification data.

Ensuring that there is clarity in this approach would reduce the complexity of cybersecurity and data incident management, allowing more resources to focus on incident resolution rather than on reporting the same incident multiple times. They will also improve awareness of incidents among relevant agencies and provide greater legal certainty for all parties involved through simpler and more consistent legislation and would prevent duplication in reporting at both EU and national levels, in line with the EU's objectives of simplifying the reporting framework.

Harmonising reporting between national and EU level
In order to avoid and remove overlapping and sectoral obligations, the European Commission should ensure that incident definitions, thresholds, reporting scopes, guidance and templates are fully harmonised and interoperable, to prevent duplication and inconsistent filings. The SEP must also ensure confidentiality, multilingual support, legal certainty, operational reliability, secure and auditable technical mechanisms, resilient fallback channels and clear liability rules to achieve its goals, and function as a true simplification tool rather than an additional layer of compliance. In this regard, the European Commission could provide guidance and a roadmap, to support the smooth implementation of the SEP.

3. The GDPR

Connect Europe and the GSMA support the GDPR's overall risk-based approach and strongly believe that its core principles must be maintained. Having said that, the Digital Omnibus sets forward targeted revisions to the GDPR, including reviewing the definition of personal data, making changes on personal data for AI training, amending how special category data (Article 9 GDPR) is processed, and making changes to data access requests and transparency obligations, that are much welcome. While supportive of some changes, we believe that the proposed changes are targeted, without a radical change to the main elements of the GDPR as a whole. Additionally, we believe that there are still areas where clarification is needed to make the proposal as effective as possible. We share our comments on the most relevant changes for our sector below.

Interactions with the AI Act
The Omnibus would also allow the use of the principle of legitimate interest[2] as a legal basis for the processing of personal data for AI model development and training. In our view, this would be a welcome change and could support European companies in the uptake of trustworthy AI, so long as this processing adheres to clear safeguards. Although we consider that such legitimate interest should be further extended to include any type of processing of personal data performed to develop any type of technologies (not just AI), since the real nature of such legitimate interest is to balance data

[2] GDPR Article 6(1)(f)

protection rights with innovation.

Risk-based approach of the GPDR

Connect Europe and GSMA support the risk-based approach of the GDPR, which allows compliance obligations to be tailored to the respective level of risk presented. However, overly rigid views on how this can be achieved have undermined this approach. In our view, further clarification and harmonisation is needed regarding risk evaluation and enforcement criteria across EU Member States. This should, in our view, encompass factors such as scale, sensitivity, safeguards, and likelihood of harm. We believe this more refined approach would significantly reduce administrative burden, ensure better allocation of companies' resources and better position EU companies to innovate and compete globally. Equally, we consider it essential that the Digital Omnibus explicitly incorporates a risk-based and proportionate approach to international data transfers.

Harmonising legal interpretation, including on personal data

Connect Europe and GSMA support the Commission's intended targeted simplification of the GDPR, specifically the measures related to personal data protection. However, we would like to underline a number of issues that persist, especially when it comes to the goal of a simpler and more harmonised framework. While we support the foundational principles governing data protection, particularly related to personal data protection, the telecoms sector has struggled with fragmented interpretation across EU Member States. As such, while the GDPR's intention is to harmonise interpretations on personal data protection across the EU, the current implementation foresees the potential for twenty-seven unique interpretations across each EU Member State and thus leads to fragmentation over legal certainty.

We note the Commission's proposals on personal data, better aligning the legal framework with the 2025 ruling of the Court of the Justice of the EU (CJEU)[3] and understanding that personal data should be treated as such strictly in the event that a data recipient has the technical means to re-identify an individual, and thus, representing a clear concern to an individual's fundamental rights. We therefore agree with the Commission's proposal that in the event personal data has been sufficiently pseudonymised and there are no technical measures by which a data recipient can re-identify an individual through that pseudonymised data, it should not be treated as personal data under the GDPR. At the same time, we consider that the definition can still include a few more clarifications, including a more detailed explanation on the distinction between controllers and processors. In this sense, we consider that when a data controller makes available previously de-identified and/ or pseudonymous data to third parties not having reasonable like means to reidentify a data subject, such sharing should not be considered as a sharing of personal data, neither from the perspective of the originator nor from the recipient. We also consider that the concept of "*reasonable expectations of the data subject*" should be clearly explained and linked to the controller's ability to identify an individual. Finally, there should be further clarifications or examples that exclude specific non-identifiable technical data from the definition of personal data.

Further simplification

Another potential area for simplification is the management of long supply and subcontracting chains. Article 28(2) of the GDPR requires prior authorisation for the replacement or appointment of a sub-processor, which is not easy to implement in standardised processes. In practice, the "opportunity to object" effectively translates into the possibility of terminating the contract. Prior authorisation could instead be replaced by a simple information obligation in which the subcontractor guarantees the same level of security (i.e., where it is subject to EU legislation or to other instruments provided for by the GDPR, such as standard contractual clauses).

[3] EDPS v. SRB (C-413/23 P)