GSMA – Connect Europe views on the European Data Union Strategy

The GSMA and Connect Europe welcome the European Commission's initiative to develop a comprehensive European Data Union Strategy. As representatives of the telecom sector, we recognize the transformative potential of data in driving innovation, enhancing competitiveness, and supporting the development of Artificial Intelligence (AI) and digital services across the EU. However, we also acknowledge the complex regulatory landscape that has emerged from the proliferation of data-related legislation. While these frameworks aim to promote data sharing and reuse by fostering trust and safeguarding rights, their overlapping scopes and fragmented implementation might create legal uncertainty and operational burdens.

This is why we welcome the Data Union Strategy as an opportunity to simplify and streamline the data regulatory framework where it hinders the competitiveness and innovation potential of European companies. In this context, addressing redundancies of sector-specific rules with the horizontal framework is a priority for our sector. Simplifying the data privacy framework for telecom operators would lift the unnecessary burden that limits our sector's innovation and bridge the regulatory asymmetry with companies that are not subject to the same rules. This would also achieve another key objective of the Strategy, which is making more data from our industry available for AI.

Current regulatory framework

ePrivacy rules

The GSMA and Connect Europe call for the repeal of the ePrivacy Directive (2002/58/EC), which no longer reflects the realities of today's digital ecosystem. The Directive's sector-specific approach has resulted in regulatory asymmetries, placing disproportionate obligations on telecom operators compared to other digital service providers. This imbalance stifles innovation and creates unnecessary compliance burdens, especially in areas like data processing and fraud prevention.

In many instances, the General Data Protection Regulation (GDPR) already provides a comprehensive, horizontal framework for personal data protection, including robust provisions on transparency, accountability, and security. In contrast, ePrivacy regime introduces duplicative and outdated obligations.

The implementation of the ePrivacy Directive has varied significantly across Member States, resulting in a fragmented regulatory landscape that generates legal uncertainty across markets. Additionally, the Directive imposes obligations on telecom operators that do not apply to other digital service providers, creating regulatory asymmetries that place telecom operators at a competitive disadvantage and distort the level playing field within the digital single market.

As a consequence, the current framework limits the adoption of the large-scale innovative services, such as the [GSMA Open Gateway] initiative, advanced anti-fraud technologies that could significantly enhance consumer protection.

While calling for the Directive's repeal, the GSMA and Connect Europe emphasize the importance of preserving the principle of confidentiality of communications (Article 5 (1) and (2)) and integrating it into a harmonised legal framework encompassing all communication providers, technologies and usages, potentially through the forthcoming Digital Networks Act (DNA) or a similarly comprehensive EU initiative.

A repeal of the ePrivacy Directive would eliminate these inconsistencies and support the development of a more coherent, agile, and innovation-conducive regulatory environment, while ensuring the continued protection of users' privacy through integration of key safeguards into a harmonised legal framework.

Data Act

As the Data Act is implemented across Europe, the GSMA and Connect Europe support its goals of enhancing B2B data access, cloud switching, and interoperability, crucial steps toward improved data sharing and the emergence of a competitive cloud market within the EU.

On B2B and B2C data sharing, we encourage the Commission to consult with industry on upcoming guidelines on compensation. In addition, further clarity on which products and services are in scope is also needed, particularly in relation to certain services within the IoT connectivity value chain. The massive volumes of data generated by IoT devices require sophisticated data management, storage, processing, and analytics capabilities, which can be expensive and complex to implement. Significantly simplifying cross-border deployments, by reducing legal complexities and compliance burdens, alongside the adoption of open standards and interoperability protocols for IoT devices, would help prevent vendor lock-in.

We are concerned B2G data sharing provisions could hinder innovation in European data analytics by enabling overly broad access to privately held data in vaguely defined situations. Telecom operators already collaborate with public authorities during emergencies. Ambiguous "exceptional need" provisions risk undermining trust and innovation. Additionally, one persistent issue for telecom operators is the absence of a fair compensation mechanism for the costs incurred in complying with government data access requests, particularly in emergency situations, which adds to the operational burden of B2G data sharing. A mandatory EU-level compensation scheme, guaranteed by Member States, should be established to cover the investments and procedural adaptations required of service providers. Such a mechanism would also serve as a price signal to promote efficiency and proportionality, encouraging authorities to limit their requests to essential cases and to make accurate requests. Therefore, in the implementation of the Data Act, ensuring that B2G data access is used in a targeted manner only when market-based solutions fail should be key. Continued good-faith negotiations between public bodies and private firms are essential. Overreach could harm emerging European data analytics services. We urge policymakers to foster cooperation throughout implementation to maximize benefits and avoid negative impacts.

Provisions on switching and interoperability can open up Europe's cloud market to make it more competitive. Where the European Commission will develop guidelines on interoperability requirements and provisions, and also on third-party access to non-personal data; we again encourage open dialogue with industry, for example through existing expert groups, taking into account existing international or European standards.

International dimension of data

The global digital economy relies on cross-border flows of data to deliver crucial social and economic benefits to individuals, businesses and governments. Cross-border data flows play a key role in innovation, competition and economic and social development. However, divergent regulatory regimes, rising data localization requirements in third countries, as well as growing geopolitical tensions, are creating significant compliance burdens and operational uncertainty for companies.

Cross-border flows of personal data are currently governed by a range of international, regional, and national instruments aimed at protecting individual privacy, national security, and local economic interests. While many of these frameworks are based on shared privacy principles, they do not constitute an interoperable regulatory system that reflects the realities, challenges, and opportunities of a globally connected digital environment. In practice, national security-driven localisation requirements, such as those mandating that Network and Security Operations Centres be located within national borders, further fragment the Single Market. These measures increase costs and limit the use of shared infrastructure and expertise. [1] Telecom operators deploying cross-border infrastructures or seeking to operate distributed network functions face significant obstacles due to divergent national requirements on asset localization and restrictions on remote network access. [2]

In particular, data localization requirements that lack a well-defined and justified legal basis can place a growing burden on telecom operators. These measures may hinder

[1] https://www.gsma.com/about-us/regions/europe/gsma_resources/the-gsma-responds-to-the-european-commission-white-paper-how-to-master-europes-digital-infrastructure-needs/
[2] See for more details A Simplification Agenda for European Telecoms, ADL Study, 2025

innovation, and may create operational inefficiencies. They may also impose operational and financial costs, especially when navigating divergent legal requirements across multiple jurisdictions.

It is therefore essential to establish interoperable and accountable frameworks for cross-border data flows that align with privacy and regulatory standards. Any restrictions should be limited to what is necessary to achieve legitimate public policy objectives and to avoid unauthorised access to data by third countries and must remain proportionate, and transparent.

In that context, we advocate for a balanced approach that upholds high standards of data privacy and security while enabling trusted, balanced, and efficient cross-border data flows. It is important to establish clear and interoperable rules that facilitate such flows with the EU's key trading partners, such as the United States, China, the United Kingdom, Switzerland, and Turkey, as identified in the European Commission's International Digital Strategy, as well as with countries that have an adequacy agreement with the EU.

However, the EU should also promote a more balanced flow of data globally. Currently, there are substantial asymmetries not only in the way that data is regulated but also in the global distribution of data flows. Mario Draghi speaks of a 'data value loss' (i.e. the amount of EU data transferred to third countries) of around 90%, with a long-term risk of loss of industrial know-how[3]. Addressing these imbalances should not result in additional regulatory burden for companies. Furthermore, this issue needs to be addressed, especially in light of the crucial role of data for digital competitiveness. One way to address this is to insist more on reciprocity in international relations when it comes to data flows.

Unlocking AI potential through harmonized regulation and data access

AI is increasingly central to the EU's digital transformation and data economy. This is why a clear and consistent guidance from the European Commission is essential to ensure a harmonized interpretation and application of AI-related rules across Member States. Without such guidance, there is a risk of fragmented implementation, legal uncertainty, and unintended barriers to innovation.

As AI systems rely heavily on large, diverse, and high-quality datasets, the development of a robust European Data Union must ensure that data is accessible in a way that supports trustworthy AI innovation. A key aspect of this is enabling the use of data for AI training, which often involves copyrighted or proprietary content. To strike the right balance between innovation and rights protection, the EU should re-examine existing

[3] The future of European competitiveness Part B | In-depth analysis and recommendation, Mario Draghi, 2024, page 67.

legal regimes, particularly copyright law, to clarify the conditions under which data can be used for training purposes.

In this regard, it is essential to ensure that any use of data for AI development and innovation respects intellectual property rights. The Data Union Strategy should explicitly acknowledge that promoting data availability must go hand in hand with safeguarding the rights of creators and rightsholders, in full coherence with the EU copyright framework.