Connect Europe & GSMA Comments on the Call for Evidence regarding Retention of Data by Service Providers for Criminal Proceedings

June 2025

As representatives of telecom operators, Connect Europe and GSMA welcome the possibility to comment on the European Commission's call for evidence for an impact assessment on retention of data by service providers for criminal proceedings. Protecting user data and confidentiality, while ensuring effective cooperation with law enforcement authorities, is essential for the safe and balanced functioning of a digital society. However, the current data retention regulatory framework presents several compliance challenges for telecom operators, which we would like to take this opportunity to highlight.

General remarks

Telecom operators have had to deal with several iterations of data retention obligations over the years – from the initial EU Directive of 2006 to the ECJ decision, and to member states developing their own approaches. These changes have already imposed considerable investments and operational costs on telcos.

This also resulted in today's fragmented situation across EU Member States in a number of ways. Firstly, a legal framework exists in some Member States but is either absent or not effectively applied in others. Additionally, there are a wide variety of definitions for metadata and the types of data to be retained. Retention periods can also be strikingly different, ranging from 6 to 72 months. Due to these divergences, it can be challenging to draw commonalities in the impact of data retention laws (or the absence thereof) on the European telecom industry. With that in mind, and considering the EU's ambitions for regulatory simplification, any changes should bring tangible improvements and to the current situation. For example, any new rules should avoid being prescriptive about operational requirements, such as how or where the data is stored, as long as it is stored within the EU/EEA.

The most significant impact of data retention law is related to the differing retention periods for data collected and retained for business purposes, in compliance with the GDPR and the ePrivacy Directive, compared to those retained for law enforcement purposes. This has resulted in significant costs for operators to purchase storage equipment, redefine the system architecture, and hire personnel. Data retained for business purposes is related to billing, operation or maintenance, network security, and commercial purposes. Other data – like location data – that are not relevant for business purposes are stored for much shorter timeframes. However, there are significant variations across operators and countries. Additionally, the GDPR has affected the situation by driving the implementation of data minimization.

The majority of requests are targeted at individual subscribers or devices, with relatively few bulk requests. Bulk requests can be problematic because Law Enforcement Authorities (LEAs) often do not fully appreciate the magnitude of the data they will receive and how it will benefit their investigations.

Access typically involves automated systems and the use of Single Points of Contact (SPOCs) for the majority of access requests. These interfaces should be easy to use and not require costly adaptations

for operators. The exchange is typically based on the ETSI request-response standard, which speeds up responses and significantly reduces access refusal rates (e.g., when a LEA contacts the wrong operator or when the requested data is no longer available).

Any data retention approach should also be proportionate. Only data that has already been processed and stored for billing, commercial, or other legitimate business purposes should be retained, as any additional requirements could have significant technical and financial implications.

Future challenges

In view of this backdrop, several future challenges should be considered moving forward.

The biggest future challenge is the considerable uncertainty surrounding the stability of national laws, many of which do not align with CJEU jurisprudence.

Furthermore, Europe's mobile data consumption per user is expected to grow from 15 GB per month in 2022 to 75 GB per month by 2030, representing an annual growth rate of 25%. Fixed data consumption per household is projected to increase from 225 GB per month in 2022 to 900 GB per month by 2030, with an annual growth rate of 20%[1].

Internet of Things (IoT) connections are expected to increase to around 707 million by 2030, growing by 6,5% year-on-year since 2023[2]. Edge computing is also a growing area. It distributes cloud infrastructure closer to the user, rather than relying on a centralized cloud. With more data generated, there are more queries and consequently more data to retain. This will result in a need for additional investment in equipment, storage capacity, and IT architecture to sustain the anticipated data volumes.

There is also an ongoing change in telecom network architecture, with a clear shift toward 5G and a virtualized, software-defined, and cloud-dependent infrastructure. Networks will be delivered by an ecosystem of operators, cloud providers, managed service providers, OTTs, and others, where functions can be operated in the cloud and outsourced from telecom providers to other actors in the value chain. This evolution may impact data storage strategies.

Encryption and other technologies may also pose challenges to data requests. 5G provides enhanced encryption compared to 4G. Additionally, technologies like DNS over HTTPS and Apple Private Relay make ISPs 'blind' to data traffic. This creates further challenges in meeting LEA requests.

As mentioned in the call for evidence, "*most national data retention laws only apply to traditional telecommunication platforms, and do not cover communication providers offering their services via the internet, which constitute currently the most used communication services*". Traditional telecom services like voice and texting remain important, but phone calls and SMS are increasingly replaced by online apps. For example, active users of messaging apps are expected to match mobile device penetration in Europe by 2025, while SMS use has dropped by 60% between 2013 and 2023. Therefore, the roles of different players in the electronic communications market have been rapidly evolving.

[1] Arthur D. Little, The evolution of data growth in Europe (2023)
[2] Connect Europe and Analysys Mason, State of Digital Communications (2025)

Recommendations

Any new regulation should avoid imposing additional costs or requiring a re-engineering of telecom operators' processes and systems. To effectively address the various challenges in the data retention landscape, we see a few key areas for improvement:

- **Need for harmonized, simplified, and future-proof rules** that ensure legal certainty, consider market developments and the growth of data volumes, and ensure cooperation with LEAs while protecting fundamental rights.
- **Level playing field and technological neutrality** should be ensured to cover all the relevant means of communications in the fast-evolving digital economy.
- **Necessity and proportionality** are principles that must be fully adhered to in any data retention legal framework, in line with the ECJ's jurisprudence. Data retained by operators to comply with legal retention obligations should be minimized and limited to what is strictly necessary, with a critical review of which categories of data are truly essential, given the expected surge in data traffic. Data retention should only concern traffic and location data, not content.
- **Industry-led technical solutions**, such as LEA SPOCs and communication standards based on ETSI, should support the implementation of legal obligations to the extent feasible within current technical and operational frameworks.
- **Ensuring stability for existing solutions** to safeguard the investment already made in implementing national data retention requirements.
- **A mandatory cost compensation mechanism should be established at EU level** to cover investments and measures taken by service providers. Member States should guarantee this compensation, considering the expected data growth and required modifications to the existing solutions and procedures. This would also serve as a 'price signal' to promote efficiency and proportionality, encouraging LEAs to limit their requests to important cases and to make accurate requests.