June 18 2025

Contribution for the impact assessment on retention of data by service providers for criminal proceedings

As German Mobile Network Operators, we are pleased to provide our views on the data retention rules in the European Union.

In a nutshell: any regulatory intervention from the EU should be in line with the respective jurisdiction of the European Court of Justice (ECJ) and be coherent with existing national laws.

Our input to the call for evidence is composed of six (6) high-level principles on: 1) specifications on data to be stored, 2) retention period, 3) data security requirements, 4) data provisioning, 5) cost compensation and 6) coherence of EU requirements and national laws.

1. Specification of data to be stored

It is important to be very precise about which data categories should be in the scope of a potential EU framework. The ECJ has set very strict limits, which must be observed in the interest of legal certainty and the protection of fundamental rights. The storage of traffic data without a specific reason is generally illegal. According to the jurisprudence of the ECJ, storage is permissible only for IP addresses (and the associated information to uniquely identify a customer), and even then, only to the necessary extent to prevent severe crimes. Additionally, uniform data specifications **should be based on international standards.**

2. Retention period

To reduce the significant regulatory costs for the storage of (continuously increasing) data, any retention period **should be limited to what is absolutely necessary**.

3. Data security requirements

Technical security requirements for data retention **should be proportionate**. Telecommunications providers are already subject to EU regulations that protect data from unauthorized access (e.g. NIS2, CER, DORA, etc.). Therefore, any new requirements for data security in the context of data retention rules should only be considered where a clear risk is identified. In particular, it must be possible for telecommunications providers to adapt new technologies that might even improve data security without conflicting with technically outdated regulations set out by EU provisions for data retention.

4. Data provisioning

There **should be a clear legal basis for the provisioning** of the stored data. This would have to meet high standards of constitutional law and fundamental rights of protection. It must also take into account existing European regulations such as the E-Evidence Regulation. The data should be provided by using ETSI-Standards. Providers should be appropriately compensated for data retention and the provisioning of data.

5. Cost compensation

Any type of EU-level data retention framework should include a mandatory cost compensation scheme for service providers across the EU.

6. Coherence of EU requirements and national laws

Due to the wide variety of national regulations already in place in Member States, it is of utmost importance that any European approach on data retention is in alignment with existing national laws – to this end, a complete mapping of the current rules across all Member States would be a good first step to identify areas, if any, where existing regulations would allow for harmonization at EU level. Any **EU approach towards data retention should be aligned with national laws**.