

WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.



POSITION PAPER

on the Call for Evidence for an Impact Assessment on Retention of Data by Service Providers for Criminal Proceedings

Berlin, 18.06.2025

On April 21, the European Commission published a call for evidence for an impact assessment on the retention of data by electronic communication service providers for criminal proceedings. The objective of this initiative is to examine the possible introduction of a harmonised EU framework for data retention, aiming to improve the availability of non-content communication data such as metadata and subscriber information for law enforcement and judicial authorities.

According to the Commission, the absence of an EU-wide legal framework has led to divergent national regulations, resulting in legal uncertainty for service providers and potential obstacles for cross-border cooperation in criminal investigations. The initiative is part of the broader agenda outlined in the "ProtectEU: a European Internal Security Strategy" communication and responds to recommendations from the High-Level Group on Access to Data for Effective Law Enforcement.

The impact assessment will explore different policy options, including both legislative and non-legislative measures, and evaluate their potential effects on fundamental rights, the internal market, and public security. Key considerations include the proportionality and necessity of data retention obligations, the scope of the data to be retained, and appropriate safeguards for access.

eco would like to take this opportunity to comment on the consultation and respond to the debate with the following points:

1. Previous Case Law

Storing communication data without cause significantly encroaches on fundamental rights. As established in the Digital Rights Ireland ([C-293/12](#)) and La Quadrature du Net ([C-511/18](#)) judgments, metadata can reveal extensive details about one's private life, including the creation of comprehensive movement and social profiles. The CJEU has emphasized that data retention interferes with fundamental rights and is subject to strict constitutional standards, not merely a measure to secure data.

eco recalls the landmark judgments of the CJEU in cases [C-793/19](#) and [C-794/19](#), which clearly define the strict limitations placed on data retention within the EU. In line with these rulings, eco emphasizes that any form of blanket or indiscriminate



WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.



data retention constitutes a serious violation of the fundamental rights of EU citizens, particularly the right to privacy and the confidentiality of electronic communications. Together with its member company Space.net, eco has previously played a pivotal role in successfully challenging unlawful data retention practices in the EU. Should the European co-legislators once again seek to undermine these essential rights, eco stands ready to oppose such measures through all available legal means.

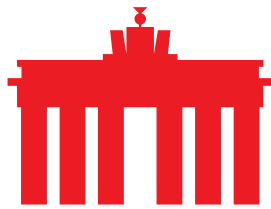
2. Access to Data for Law Enforcement

With the adoption of the European e-Evidence Package ([\(EU\) 2023/1543](#) and [\(EU\) 2023/1544](#)), the EU introduced new instruments in 2023 to enable criminal authorities to lawfully access electronic evidence. These measures complement and, in part, replace the existing framework of Mutual Legal Assistance Treaties (MLATs). The implementation of this legislation is currently underway across the Member States. From the perspective of the Internet industry, there is no identifiable need for additional instruments or further reform at this stage. Each new legislative initiative imposes significant compliance burdens on companies, reduces operational capacity, and introduces legal uncertainty, both in terms of implementation and alignment with fundamental rights and consumer protection standards. It is therefore essential that the recently adopted legal framework be thoroughly implemented and evaluated before any further legislative or regulatory steps are considered.

3. Risks and Disadvantages of Data Retention

The susceptibility of stored data to misuse and errors is a factor that cannot be ignored. The longer and larger the amount of communication data stored, the higher the risk of data misuse, security gaps and false conclusions when using the data. Therefore, the CJEU emphasizes that storage itself must be secured by clear legal requirements and technical protective measures. In practice, however, many national regulations have not met these requirements.

Furthermore, there is a significant lack of empirical evidence demonstrating that data retention without cause significantly contributes to the fight against serious crime. The actual benefits and relationship to the cost of data retention should be critically examined. Efficient law enforcement is possible without blanket data retention. This can be achieved primarily through targeted measures in individual cases or through temporally and objectively limited safeguards.



WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.



4. Conclusion

Even with its most recent ruling, the CJEU has made it clear once again that IP addresses may only be stored if the strictest technical, legal, and organizational requirements are met. These requirements include the effective separation of data categories, strict purpose limitation, independent monitoring, and protection against profiling. Therefore, data retention “without cause” within the framework of EU law is impossible to implement legally.

Data retention without cause is legally risky and questionable in terms of fundamental rights, as well as disproportionate in terms of security policy. Rather than mass surveillance of European citizens, targeted, constitutional measures for criminal prosecution that align with the Charter of Fundamental Rights are needed. The CJEU provides clear guidelines for this with its differentiated case law.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.