CCIA Europe Response to the European Commission's Public Consultation

Assessing the Impact of Data-Retention Rules on Service Providers

September 2025

The Computer & Communications Industry Association (CCIA Europe) welcomes the European Commission's initiative to harmonise data-retention rules across the EU, and appreciates this opportunity to provide input in response to the Commission's consultation. The tech sector believes that a unified framework could help address the longstanding regulatory fragmentation, which currently imposes a disproportionate compliance burden on cross-border service providers. Any future proposal, however, must be evidence-based, proportionate, and focused on clearly defined objectives.

I. Apply a proportionate clear scope for data retention

The current patchwork of national data-retention regimes creates legal uncertainty and operational inefficiencies for companies doing business in multiple EU Member States. CCIA Europe believes that a harmonised framework of regulations, rather than voluntary measures, are necessary to provide certainty to service providers and users across the EU.

Such a harmonised framework of regulations can only work if it is grounded in evidence and built on best practices. To ensure a proportionate and clear scope, retention periods should be justified by clear necessity and calibrated to the specific risks they are meant to address. Accordingly, data-retention obligations should apply only to data covered under Article 6 of the ePrivacy Directive.

CCIA Europe recognises the importance of targeted measures to detect and investigate serious crimes such as terrorist activity, drug trafficking, cybercrime, or child sexual abuse material (CSAM). However, the legal basis, purpose for retaining metadata, and categories of metadata must be explicitly defined in consultation with service providers. Indeed, the application of data-retention obligations should be tied to an existing EU-wide definition of 'serious crime'. Vague or open-ended mandates risk introducing legal ambiguity for service providers and users alike.

Additionally, ensuring fair competition for number-independent interpersonal communication services (NI-ICS) requires a tailored approach to data retention. Any new data-retention rules should not be a blanket extension of systems designed for traditional telecom operators. Failing to distinguish between over-the-top (OTT) services and telecom operators overlooks fundamental differences in their business models, technologies, data flows, and user relationships. Forcing uniform retention rules on OTTs would only add unnecessary costs, suppress innovation, and deliver little, if any, real benefit for privacy or security.

II. Streamline data requests and usage

Legal harmonisation should be matched by practical progress in how retained data is accessed. A truly effective framework must cover all types of data retention, including in the areas of criminal justice and national security, while carefully respecting the limits of EU competences. To make this work, the Commission should collaborate closely with Member States to ensure law enforcement authorities adopt modern, interoperable tools for requesting and using data.

As the Commission's Directorate-General for Migration and Home Affairs has observed, the current situation remains highly fragmented with some authorities still relying on paper-based requests – creating delays, inefficiencies, and unnecessary burdens for law enforcement and service providers. CCIA Europe considers that coordinated action is needed to standardise and digitise these procedures while ensuring that appropriate safeguards, accountability, and oversight mechanisms are in place.

III. Avoid mandating technical criteria

To prevent disproportionate barriers to entry of the single market, any data-retention legislation should leave technical considerations for compliance to service providers.

The scope of the forthcoming framework must remain limited to data retention and explicitly exclude requirements to weaken or bypass end-to-end encryption, or any other security protections for that matter. End-to-end encryption is a foundational security measure that protects systems, users, businesses, public institutions, and infrastructure from malicious actors. Encryption's importance is already acknowledged in EU legislation currently in application, including the NIS2 Directive[1] or the e-Evidence Regulation.[2]

Mandating decryption capabilities or requiring providers to weaken other security measures in the interest of law enforcement's access to data would not only compromise user privacy and data integrity, but also risk introducing systemic vulnerabilities across the entire digital ecosystem. That is why CCIA Europe strongly urges the Commission to reaffirm its commitment to end-to-end encryption and ensure that any new retention rules remain aligned with the existing legislative framework and respect this critical safeguard.

IV. Guaranteeing coherence and judicial oversight

It is essential that any new legislation align with fundamental rights under the Charter of Fundamental Rights, the case law of the Court of Justice of the European Union (CJEU) and

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), available here: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-Evidence Regulation), available here: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

the European Court of Human Rights (ECHR)[3], as well as EU data protection rules, including the General Data Protection Regulation's principle of data minimisation.[4] Future data-retention rules should also clarify that service providers are not obliged to collect or request additional data beyond what is already gathered in the course of providing their services.

Moreover, to ensure appropriate and effective oversight, any national decision imposing a data-retention order or access to retained data by national authorities should be subject to effective prior review by a judicial or independent administrative body, with the right of appeal and right of redress for impacted parties. Only competent national authorities should have the power to obtain such orders.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.eu, x.com/CCIAeurope, or linkedin.com/showcase/cciaeurope to learn more.

For more information, please contact:
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org

[3] Joined Cases C-793/19 and C-794/19, Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH, Judgment of the Court (Grand Chamber) of 20 September 2022, ECLI:EU:C:2022:702, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0793.

[4] Article 5(1)(c) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available here: https://eur-lex.europa.eu/eli/reg/2016/679/oj