Council of the European Union
General Secretariat

Brussels, 27 November 2025

WK 16133/2025 INIT

LIMITE

COPEN	**COSI**
CYBER	**IXIM**
ENFOPOL	**CATS**
JAI	**FREMP**
DATAPROTECT	**TELECOM**
	CT

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	Presidency
To:	Delegations
Subject:	Presidency Outcome Paper - Future rules on data retention in the European Union

Delegations will find in annex the Presidency Outcome Paper regarding Future rules on data retention in the European Union.

Presidency Outcome Paper

Future rules on data retention in the European Union

1) Introduction

On 25 September 2025, the Danish Presidency organised a meeting of the Working Party on Judicial Cooperation in Criminal Matters (COPEN). The purpose of the meeting was to continue discussions on a possible design for a future EU legal framework on data retention and to contribute to the Commission's impact assessment, by identifying the main priorities of the Member States in this area, in particular in light of the requirements laid down in the case-law of the Court of Justice of the European Union (CJEU).

During the meeting, the Commission provided an update on their work on the impact assessment, including a presentation of the preliminary results of the call for evidence and the public consultation. The Commission reported that the response rate to the general open consultation had been very high and thus a big success. On the targeted consultation, the Commission summarised the input received from Member States and asked for it to be supplemented by more information regarding electronic data used for criminal investigations. The Commission is planning to finalise the impact assessment in the first quarter of 2026. If the result of the impact assessment pointed in the direction of a legislative proposal, that proposal could, according to the Commission, be presented at the end of the first semester of 2026.

During the exchange of views, most Member States reiterated their support for future EU legislation in this area. In this regard, most Member States referred to the need to remain within the limits defined by the CJEU, while some stressed the need to go beyond mere codification of the case-law and thought that necessity and proportionality should be re-assessed in the light of evolving technologies and developments in the way crimes are committed. Many considered that the overall proportionality of the retention regime could only usefully be ensured through access level and through additional safeguards. Moreover, Member States emphasised that certain elements should remain within their national competence, such as the definition of what constitutes 'serious crime'. Also, aspects related to national security should be exempt from the scope of any future EU legislation on data retention. This would mean that national legislation on *storing* and *access* to retained traffic and location data for the purpose of safeguarding national security would have to be exempt from future EU legislation, regardless of which national authority requested access.

At the end of the meeting, the Presidency invited Member States to send their contributions in writing based on the guiding questions outlined in the Presidency's discussion paper, WK 11640/2025.

2) Background and context

For more than a decade, the European Union has not had a common set of rules regulating the retention of personal data for the purpose of the investigation, detection and prosecution of serious crime. On 8 April 2014, the Data Retention Directive in force at the time (Directive 2006/24/EC)[1] was declared invalid *ab initio* by the CJEU in the landmark judgment in joined cases C- 293/12 and C- 594/12, *Digital Rights Ireland and Others*.[2] In that judgment, the CJEU found that the Directive violated Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, i.e. the right to respect for private and family life and the right to the protection of personal data. Even though the CJEU found that the Directive had a legitimate aim, it did not pass the proportionality test, given that it covered in a generalised manner all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation, or exception being made in the light of the necessary objective of fighting serious crime.

Since the Directive was declared invalid, the CJEU has developed and further refined its case-law on Member States' access to retained and stored data for the purpose of fighting serious crime.[3]

In the absence of a harmonised EU legal framework, Member States have had to navigate complex legal terrain to ensure that their national laws align with the CJEU's standards on necessity and proportionality, as well as privacy and data protection safeguards. In the Council, discussions of the consequences of the jurisprudence have taken place since 2014 in various fora, i.e. JHA Council meetings, but also in more detail in the COPEN Working Party.

---

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[2] Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12.

[3] Judgment of 6 October 2020, *La Quadrature du Net I*, C-511/18, C-512/18 and C-520/18, paragraph 168 (conditions for general and indiscriminate retention of traffic and location data). Judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, paragraph 67 (conditions for access to civil identity data). Judgment of 30 April 2024, *La Quadrature du Net II*, C-470/21, paragraphs 101-103 (conditions for access to information on IP addresses).
Judgment of 20 September 2022, *SpaceNet*, C-793/19 and C-794/19, paragraphs 104, 114,119, 120.
Judgment of 2 March 2021, *Prokuratuur*, C-746/18, paragraph 50.
Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, paragraphs 52-57.
Judgment of 30 April 2024, *La Quadrature du Net II*, C-470/21, paragraph 97.
Judgment of 30 April 2024, *Tribunale di Bolzano*, C-178/22, paragraphs 19, 22, 38, 49, 58, 62.

In June 2023, the Swedish Presidency, together with the European Commission, launched a High-Level Group on access to data for effective law enforcement (HLG), aiming to stimulate the discussion and open it to other relevant stakeholders. The HLG issued its concluding report in November 2024[4], in which the HLG confirmed that one of the main areas of access to data for law enforcement purposes is data retention. This was reiterated by the Council conclusions of 12 December 2024 on access to data for effective law enforcement, which invited the Commission to present a roadmap for the implementation of relevant measures to ensure the lawful and effective access to data for law enforcement.[5] Furthermore, in its conclusions of 26 June 2025, the European Council invited the EU Institutions and the Member States to take further action to strengthen law enforcement and judicial cooperation, including on effective access to data for law enforcement purposes.[6]

On 24 June 2025, the Commission presented a roadmap for lawful and effective access to data for law enforcement ('the Roadmap').[7] It is in the context of the implementation of this Roadmap that the Commission is carrying out an impact assessment on data retention.

During the discussions at the informal delegates' meeting of the Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS) in Copenhagen on 1-2 September 2025, many delegates stressed the importance of a timely Commission proposal for a harmonised set of rules on data retention in order to ensure that law enforcement authorities across the EU have effective access to data when investigating and prosecuting organised crime.

Within this context, the work done in the COPEN Working Party during the Danish Presidency has focused on contributing to this goal, by ensuring that the Member States' approaches and priorities are identified and taken into account in the Commission's impact assessment, following up on the work done by the Polish Presidency and in full coordination with the other communities concerned by the topic of access to data for law enforcement (i.e. the Standing Committee on operational cooperation on internal security (COSI) and the Horizontal Working Party on Cyber Issues (HWPCIs)).

[4] 15941/2/24 REV2.
[5] 16448/24.
[6] EUCO 12/25.
[7] 10806/25.

3) Summary of the Member States' remarks

Following the COPEN Working Party meeting on 25 September 2025, the Danish Presidency has received written contributions from fifteen Member States[8] and the EU Counter-Terrorism Coordinator (EU-CTC) with reference to the questions outlined in the Presidency discussion paper prepared for that meeting (WK 11640/2025). The contributions have been compiled in their full length in document WK 13500/25 and were distributed to Member States on 31 October 2025. In the following, the Presidency seeks to summarise both the written contributions and the oral comments made during the meeting in order to provide an overview of the Member States' main positions in this area. Hence, the summary reflects the Presidency's reading of and selection from the inputs provided and does not in any way prejudge the official or final position of Member States.

Support for a new legislative framework

Member States highlight that **stored traffic and location data are particularly relevant for the effective investigation and prosecution of criminal offences that leave few traces other than such data (e.g. cases regarding the acquisition, dissemination, transmission or making available online of child sexual abuse material[9]), and thereby minimise the risk of systemic impunity**. With relevant data, investigators can get a clear picture of the criminal offences committed. They emphasise that evidence **is not always incriminating**, but in many cases, it is exculpatory and can lead to an acquittal. For this reason, some Member States believe it is appropriate to provide for new rules which include general data retention and which are accepted by the CJEU.

[8] BG, CZ, IE, IT, LT, LV, AT, PL, PT, ES, SK, FI, SE, HU, and SI.

[9] Judgment of 6 October 2020, *La Quadrature du Net and Others*, C- 511/18, C- 512/18 and C- 520/18, paragraphs 153 and 154. Judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C- 140/20, paragraphs 73 and 74.

Most Member States **express support for a new legislative framework at EU level,** highlighting the need for harmonised rules to address the fragmentation after the 2006 Directive was declared invalid in 2014. However, this support is expressed **with cautionary remarks** concerning the need to incorporate **elements to guarantee proportionality and necessity as well as robust safeguards against abuse**. **Some Member States** emphasise the limitations imposed in particular by the *Digital Rights Ireland* judgment and the need to avoid indiscriminate retention, while a few Member States **explain that they do not have a formal position yet on the need for new legislation on data retention at EU level. The EU-CTC** is in favour of **establishing a harmonised EU regime on data retention that is technology-neutral and future-proof** and advocates for the use of standardised formats for data retention.

Most Member States recall that safeguarding national security falls within the remit of their competence and this area should therefore be excluded from the scope of any future EU legal framework on data retention. According to certain Member States, the framework should be defined in such a way as not to impede the exercise of their competence in the area of national security. This implies that national legislation on *storing* and *access* to retained traffic and location data for the purpose of safeguarding national security should be exempt from future EU legislation, regardless of which national authority requests access.

In addition, some Member States also mention **the importance of aligning future data retention rules with existing EU regulations** which provide law enforcement authorities access to retained data, mainly the e-Evidence Regulation[10], but also others, such as regulation in the field of consumer protection.[11]

Scope of service providers

Regarding the service providers that should be covered by the obligation to retain data, most Member States express **general support for future legislation to have the broadest possible scope** of application, including the possibility of adapting the list to future technological and market developments.

[10] 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.
[11] Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the enforcement of consumer protection laws, recital 7, Article 9(2), and Article 42.

More concretely, some Member States and the EU-CTC agree that **over-the-top (OTT) services should be subject to retention obligations** due to their dominance in communications (approximately 97% of mobile messages are currently sent via OTTs, with traditional SMS and MMS making up only about 3% of messages[12]). Nevertheless, some Member States mentioned that the impact which such an extension would have on OTT business models and that the related costs should be taken into account. Further to the general reference to OTTs, Member States provided detail on a wide range of service providers to be included in a future legal framework, such as domain name registries, hosting providers, file sharing and cloud storage services, payment service providers, providers of VPN services, cryptocurrency traders, e-commerce and financial platforms intermediaries, taxi and food delivery services and gaming platforms, as well as car manufacturers, most of which are already included in the scope of the e-Evidence Regulation.

Regarding alignment of services with the e-Evidence Regulation, several Member States point out that it would be useful to include at least the same scope of services in a future legal framework on data retention to ensure the full effectiveness of access rules under the e-Evidence Regulation.

Data to be retained

Regarding the data to be retained, most Member States mention that data to identify a user should be the minimum data category to be included in future legislation, such as subscriber data and IP addresses. Furthermore, metadata associated with communications (traffic and location data) should be included, **with content data clearly excluded**. Some Member States also mention data to identify the destination and service recipient's communication equipment in order to determine the location of mobile communication equipment.

As regards the possibility of imposing a **general and indiscriminate data retention obligation on telecommunication providers in order to locate missing persons, most Member States consider that** location data is crucial in such cases, with some expressing support for including a general and indiscriminate retention of such data for the purposes of conducting search operations and rescuing people, given how highly effective this is, while others consider that such a retention obligation would need to be finely tuned since not all cases of missing persons involve a potential criminal offence.

[12] Roadmap for lawful and effective access to data for law enforcement.

Targeted retention

On the **benefits** of targeted data retention for traffic and location data, Member States noted that the aim of targeting measures would be to provide **proportionality** and to limit interference with individuals' privacy, as data should only be retained according to clearly defined criteria, **in line with the CJEU's case-law.**

On the **shortcomings,** Member States generally agree **that targeted data retention based on geographical criteria would be** technically challenging **to implement (and even impossible for some)**, due to the current configuration of providers' networks, which does not allow for restriction of data retention to a pre-defined area, while being very costly for service providers. In addition, Member States consider that **targeted data retention would be insufficient to achieve a good outcome for the investigations**, since law enforcement authorities will not always know in advance by whom, when, and where a crime is going to be committed.

Moreover, retention based on geographical or personal criteria could be easily circumvented e.g. by criminals using other persons' identities or shifting their criminal activities to areas not covered by data retention obligations. Targeted data retention limited to data of persons with a criminal history would not account for first-time offenders as well as foreign offenders (not included in national databases). Furthermore, reliance on criminal statistics would risk not accounting for areas where crimes are prepared or concealed or for crimes that cannot easily be linked to a certain location such as financial crimes. As a consequence, such targeted retention would not meet the needs to effectively investigate a number of crimes including organised crime, cybercrimes or terrorism.

For some Member States, targeted retention could also raise **constitutional issues because of risks of discrimination and the presumption of innocence.** Some Member States also expressed concerns that applying such targeted retention would lead to unequal protection of victims depending on where the crime is committed (e.g. murder in a remote area outside the targeted geographical area) and potentially hamper the early stages of investigations in relation to unknown suspects. In these cases, the lack of data to identify a potential perpetrator could result in delays in time-sensitive investigations where there is a potential risk to life.

Several Member States also point to the high complexity of designing and implementing such a targeted retention regime, which would need to define all relevant criteria capturing future criminal behaviour based on historical data and would need to be constantly updated (creating additional burden for companies).

Instead, several Member States and the EU-CTC recommend working on a system that allows for an adequately graduated and differentiated retention regime, with **limitations defined in terms of data categories and retention periods**, accompanied by strengthened security requirements and strict access rules and purpose limitations, user information, complaint mechanisms and legal remedies as well as general oversight. Some Member States also point out that the CJEU has not ruled out the use of criteria other than those mentioned (i.e. geographical or personal) to define data retention obligations.

Expedited retention orders (quick freeze)

While Member States recognise expedited retention (known as a 'quick freeze'), **as a relevant tool** allowing for the immediate preservation of data upon notification of a crime, it is considered **insufficient to guarantee a good outcome for an investigation**. **Quick-freeze obligations should therefore complement, but not replace, a data retention regime.**

The reasoning behind this is that the **tool is reactive, not preventive**. The event under investigation would have to have taken place before the quick freeze is utilised. Furthermore, in the absence of a general retention obligation, the risk that the request might arrive when the data has already been deleted increases exponentially.

Some Member States would support the regulation of quick-freeze measures in an EU instrument, with some considering that regulation of **quick freeze should cover not only the scope of data to be accessed, but also the conditions imposed on the requesting authority**, taking into account the degree of interference with privacy.

Use of traffic and location data retained for marketing and billing purposes

In some Member States, the preservation regime relies on **service providers storing data for commercial purposes.** In others, law enforcement authorities may only access this type of data from telecommunication providers, and in certain Member States, data retained for marketing and billing purposes serves as the basis for requests directed at providers **not subject to the general data retention obligation, such as operators outside the traditional telecom sector.** A common feature of these regimes is that the retention period can be very short, typically between a few days or weeks, or three to six months, depending on the Member State, and the data available may be incomplete.

Some Member States indicate that companies either retain a **different range of data** for their own purposes, or retain data necessary for criminal investigations, **but not for a sufficiently long period or of a sufficient quality**. Thus, some of the data (e.g. data kept for marketing purposes) have only limited evidential value and may only prove useful in certain categories of offence, such as online or credit fraud. In other cases, service providers do not store relevant data at all since they are not required for billing purposes (e.g. when offering unlimited calls or in relation to pre-paid services). Overall, Member States consider that data held by service providers for purely business purposes are **insufficient to enable the effective investigation and prosecution** of all types of serious crime. For the purposes of effective criminal investigations, the definition and scope of data to be retained should reflect the investigative needs in terms of identifying the perpetrator and establishing who communicated with whom, when, where and how.

However, several Member States would prefer to keep **the possibility to request metadata that has already been retained for commercial purposes** or in order to comply with other obligations, such as data retained to fulfil security and quality requirements.

<u>Retention periods</u>

As for the question of **how to best determine retention periods in line with the case-law**, **most Member States advocate for a duration of one year and in any event not shorter than six months**. However, some Member States are in favour of longer retention periods for complex investigations or for very serious crimes, linking the retention obligations with strict conditions to access.

According to some Member States and the EU-CTC, retention periods should be designed as a **minimum mandatory period, rather than as a maximum limit**, thus allowing Member States to maintain longer retention periods where necessary.

Regarding the question of the advantages and disadvantages of one fixed retention period across the EU, allowing for the possibility of renewals at national level, or setting a range within which Member States may set shorter or longer retention periods, Member States generally recognise that uniform retention periods across the EU increase predictability and facilitate cross-border investigations while also ensuring that criminals cannot take advantage of lower retention periods in some Member States. While Member States prefer to maintain some flexibility (in particular to be able to maintain longer retention periods under national law), they recognise that a **range may introduce some uncertainty** as to what is necessary and proportionate. Other Member States **show openness to an interval-based model**, under which the EU would set minimum and maximum retention periods, allowing Member States to adjust them according to national needs, taking into account the type of data, their relevance to specific crime areas, the technical capabilities of service providers, and the practical needs of law enforcement.

On the possible **differentiation of retention periods according to the type of data**, most Member States are generally open to such an approach, while also pointing to an increase in complexity affecting the ability of service providers to implement it.

Scope of crimes

Most Member States stress that metadata could be relevant in relation to the investigation of practically all crimes. For the purposes of an EU data retention regime for traffic and location, they agree that such obligations could be limited **to the purposes of combating serious crime**. Types of crime mentioned in the contributions include combating fraud and serious economic and financial crimes, cyber-enabled and cyber-dependent crime, child exploitation, terrorism, homicide, human trafficking, cybercrime, corruption, organised crime, all crimes committed in cyberspace or using information and communication technology. Other crimes that were committed with the use of relevant means of communication are also mentioned in some of the contributions, such as offences against life and health and online sexual offences, kidnappings and disappearances, and threats to national security.

In addition, most Member States support the inclusion of crimes **committed largely online** (stalking, hate crime, etc.) even if the level of sanctions is moderate but the lack of data would practically **make the investigation impossible**. While most Member States consider that the lack of traffic and location data would risk systemic impunity in particular in relation to cyber-dependent and cyber-enabled crimes, similar risks are also identified in relation to other serious and organised crimes such as drugs trafficking, arms trafficking, human trafficking, terrorism, as well as kidnappings and disappearances and other serious offences against life and health.

On the other hand, some Member States advocate for **the broadest catalogue of offences possible** based on the list in Article 12(1)(d) of the e-Evidence Regulation (which includes all crimes with a penalty threshold of three years). Member States consider that EU legislation should not define the concept of 'serious crime'. In this regard, some Member States consider that **an offence catalogue would imply an EU-wide definition of 'serious crime',** interfering with national competences. Some Member States also note that a list of all possible offences would not be sufficient because of the changing *modus operandi* of criminals. Those Member States see the decisive points as being the **specific purpose of the investigation, the degree of interference, and strict, differentiated safeguards**.

Access rules and conditions

Some Member States emphasise that **EU provisions on access to retained data should be limited to minimum harmonisation** in compliance with the principles of subsidiarity and proportionality and with the other requirements set out by the CJEU, while other Member States point out that the system should be based on **general retention combined with robust access safeguards**.

A large majority of the **Member States state the need for robust access safeguards,** including prior authorisation by a court or independent administrative body for certain types of data, based on reasoned requests and subject to limitations reflecting the seriousness of the offence. Such access would be granted only for a specific purpose, with strict guarantees also applying to data sharing, and accompanied by strong security and data minimisation measures, in order to avoid, among other risks, the possibility of profiling.

Some Member States mention that **access to traffic and location data should be subject to additional criteria in specific cases.** These include situations where digital evidence is essential for identifying the perpetrator, where serious harm to life, health, human dignity or major economic damage is involved, where the data is at risk of being lost, where less intrusive measures have failed to elucidate the offence, or where the case has a cross-border dimension that makes it difficult to obtain evidence quickly by other means.

Some Member States pointed out that when designing a new data retention regime in accordance with the case-law of the CJEU, account should be taken of the fact that **the CJEU's judgments were delivered in specific factual contexts.** They therefore argue that a new EU data retention regime should not rely on a literal application of those rulings to individual cases, but rather on an assessment of the **principle of proportionality** in line with the CJEU's general guidelines as they result from the application of the Charter, combined with **appropriate mechanisms for oversight** by independent bodies or judicial authorities to ensure full protection of fundamental rights.

On this matter, some Member States also point out that access to communication metadata is subject to the condition of **probable cause, reasonable grounds or a criminal context.**

Regarding alignment with the e-Evidence Regulation regarding conditions for access, several Member States support mirroring some of its elements, such as standardised formats for access requests, secure communication channels and guarantees of access depending on the type of data at stake, while adapting them to the specific needs of data retention for law enforcement purposes in order to ensure transparency, data protection and more efficient operation. More specifically, some Member States advocate for standards in line with those of the European Telecommunications Standards Institute (ETSI). Such standards would enhance the efficiency of information sharing and provide greater legal certainty for service providers, while also allowing them to contribute to the design so that the standards better reflect their technical needs. **The EU-CTC also sees value in defining standardised formats** for a harmonised categorisation of data to be retained and accessed, but also for establishing secure channels for the exchange between competent authorities and service providers.

Some Member States explain, however, that the e-Evidence Regulation only standardises to a limited extent, and that new standards of data transmission could potentially incur significant costs. These Member States **do not see a need to regulate standardised formats and communication channels**. They argue that the main purpose of an EU instrument should be to regulate data retention in situations involving interactions between national authorities and providers established within their territory, i.e. domestic cases, since cross-border cooperation scenarios are already addressed by the e-Evidence Regulation.

Finally, some Member States highlight the fact that it would be important to bear in mind the recommendations of the HLG regarding the **enforcement of sanctions** against electronic and other communications service providers which do not comply with requirements regarding the retention and provision of data.

On the other hand, some Member States stress that access rules at EU level should not interfere with national rules on the admissibility of data.

4) Conclusion

If a data retention framework were to be defined, a primary hurdle would be reconciling the demands of effective law enforcement, on the one hand, with the protection of fundamental rights, as interpreted by CJEU jurisprudence, on the other. In this regard, most Member States highlight the need for a framework that avoids indiscriminate retention, prioritises judicial oversight based on the sensitivity of the data at stake, and incorporates robust safeguards against abuse. The Commission must navigate this complex legal and political landscape by focusing on differentiated retention obligations, establishing a clear definition of crimes that justify access, and adopting strict rules to regulate such access. It should contain harmonised procedures to ensure compliance with CJEU case-law while providing a practically effective solution. Moreover, it is emphasised that national legislation on *storing* and *access* to retained traffic and location data for the purpose of safeguarding national security should be exempt from future EU legislation, regardless of which national authority requests access.

5) Next steps

Taking into account the views of Member States and given the need to respond to law enforcement requirements while fully respecting individuals' fundamental rights, the COPEN Working Party will continue to follow up on the specific activities related to data retention in the Roadmap, and when appropriate, with the support of the Commission, the justice and home affairs agencies and other relevant stakeholders. However, at this stage, priority will be given to awaiting the outcome of the impact assessment before considering further steps. The contributions of other Council preparatory bodies to the work on access to data for effective law enforcement within their respective mandates will be coordinated by the Presidency to avoid overlaps.[13]

[13] Including CATS, COPEN, DATAPROTECT, FREMP, HWPCI and LEWP, not excluding the possible involvement of other preparatory bodies of the Council.