Council of the European Union
General Secretariat

**Brussels, 17 September 2025**

**WK 11640/2025 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.*

**MEETING DOCUMENT**

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

In view of the ongoing discussions on a future legal framework for data retention in the European Union, the Presidency invites delegations to engage in a structured exchange of views at the COPEN meeting on 25 September 2025.

The purpose of the discussion is to gather input from Member States on their operational needs, challenges and best practices in relation to data retention and access to data for the purposes of investigating, and prosecuting serious crime. This input will also serve as an important contribution to the Commission's ongoing work and help shape any future legislative initiative in this area.

After the meeting, delegations are invited to submit their contributions in writing **no later than 10 October 2025** . The Presidency will then compile all the written contributions in a document to be shared in due time.

# Future Rules on Data Retention in the European Union

**Presidency Paper**

## 1. Introduction

For more than a decade, the European Union has not had a common set of rules regulating the retention of data. On 8 April 2014, the data retention directive in force at the time (Directive 2006/24/EC) was declared invalid by the European Court of Justice (hereinafter "the CJEU") in the landmark judgment in Joined Cases C- 293/12 and C- 594/12, *Digital Rights Ireland and Others*. In this case, the CJEU found that the Directive violated Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter"), 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, as the Directive, according to the Court, in a generalised manner covered all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation, or exception being made in light of the necessary objective of fighting serious crime.

Since the annulment of the Directive in *Digital Rights Ireland and Others*, the CJEU has developed and further nuanced its case-law on the Member States' access to retain and store data for the purpose of fighting serious crime. Several Member States have taken independent legislative actions to regulate data retention. In the absence of a harmonised EU legal framework, Member States have had to navigate a complex legal terrain to ensure that their national laws align with the Court's standards on necessity, proportionality, and privacy safeguards.

At the last meeting in COPEN (Data Retention) on 19 May 2025, the Polish Presidency followed up on the recommendations of the High-Level Expert Group on Access to Data with regard to data retention and initiated a discussion on the way forward. On that meeting, the vast majority of Member States expressed support – or at least openness – towards a future EU legislative proposal on data retention and encouraged the Commission to proceed with an impact assessment in relation to such a proposal. At the same time, many Member States emphasized that their support to a future EU initiative on data retention came with certain reservations and that a future legislative proposal would have to provide sufficient tools and leave the necessary margin of discretion to the law enforcement and prosecution authorities while at the same time respecting fundamental rights and the case-law of the CJEU. In this regard, some Member States specifically mentioned that a directive laying down minimum rules would, in their view, be the appropriate legislative instrument.

On 24 June 2025, the Commission presented a Roadmap stipulating the way forward to ensure that law enforcement authorities in the EU have effective and lawful access to data. As part of the roadmap, the Commission stated that it will carry out an impact assessment with a view to a future proposal for a new EU legal framework on data retention. In that context, the Commission published a call for evidence, launched a public consultation and invited Member States to provide further views, facts and figures in reply to a targeted consultation. The finalisation of the impact assessment is currently foreseen towards Q1 of 2026.

During the discussions at the informal 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 Member States 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.

The Danish Presidency has organised a COPEN (Data Retention) meeting on 25 September 2025. The purpose of this meeting is to continue the discussion 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 CJEU. For that purpose, this paper seeks to outline the main criteria set out by the CJEU to be followed when regulating retention and access to non-content communication data for investigation purposes.

## 2. The requirements set out in the case-law of the CJEU

The CJEU annulled the 2006 data retention directive[1] considering that the generalised and indiscriminate retention of all electronic communication data (excluding content data) was disproportionate and therefore in breach of Articles 7 and 8 as well as Article 52(1) of the Charter because of:

- Retention obligations not providing for any differentiation, limitation, or exception in light of the necessary objective of fighting serious crime[2];
- Lack of access rules which would limit access to clearly defined crimes and without access being subject to judicial authorisation[3];
- Retention period being set at a range between 6 months and 2 years without differentiation based on the usefulness of the data and without setting out clear criteria as to how to set the retention period within that range to ensure that the retention period is limited to what is strictly necessary[4];
- Insufficient safeguards against unauthorised access and abuse (leaving technical and operational measures to ensure data security and integrity in the hands of service providers) and no obligation to store data in the EU or to delete data once the retention period expired.[5]

[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, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraphs 57-59.
[3] Judgment of 8 April 2014, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraphs 60-62: Referring to the lack of a) objective criteria limiting access to data to what is strictly necessary for the investigation of offences which may be considered to be sufficiently serious to justify serious interference; b) substantive and procedural conditions governing access, including a requirement that access and subsequent use of the data must be restricted to the purpose of investigating precisely defined serious offences; c) lack of objective criterion by which the number of persons authorised to access and subsequently use the retained data is limited to what is strictly necessary; d) lack of requirement to make access depending on prior review by a court or independent administrative body.
[4] Judgment of 8 April 2014, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraph 63 and 64.
[5] Judgment of 8 April 2014, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraphs 66-68.

In subsequent jurisprudence, the CJEU assessed national data retention and access rules under Article 15(1) of the e-Privacy Directive[6] in light of Articles 7, 8, 11 and 52(1) of the Charter.

It has considered the following **retention regimes** to be permissible:

1) **General and indiscriminate retention of traffic and location data** can be justified by the legitimate aim of protecting national security where there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat to national security, which is shown to be genuine and present or foreseeable.[7] The duration of retention must not exceed a foreseeable period of time and must be limited in time to what is strictly necessary. Although it is conceivable that an order requiring providers of electronic communications services to retain data may be renewed, such data retention must be subject to limitations and be controlled by strict safeguards to ensure effective protection against abuse. Thus, according to the CJEU's case-law, the retention may not be of a systematic nature.[8]

2) **Targeted retention of traffic and location data** can be justified by the legitimate aim of combating serious crime. For retention to be targeted, it must be based on objective and non-discriminatory criteria. While the CJEU elaborated in more detail on the personal and geographic criteria[9], it also recognised that targeted retention could result from other criteria, including by limiting the categories of data to be retained or means of communication subject to retention obligations. Furthermore, it considered that Member States could use other criteria provided that such criteria would establish a connection between the data to be retained and the purpose of fighting serious crime. [10] Such targeted retention must be limited in time to what is strictly necessary, but may be extended. [11]

3) **General and indiscriminate retention of IP addresses assigned to the source of an internet connection** for the purpose of combating criminal offences in general and for a period that is limited to what is strictly necessary. For the general retention of IP addresses to be permissible, the service provider must ensure that the data cannot be combined with other traffic and location data (water-tight separation).[12] Law enforcement and prosecution authorities can in principle get access to such data without the requirement of prior review where IP addresses have been stored separately from other data and where the interference with the fundamental rights concerned by access by a public authority cannot be classified as

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[7] Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net I*, paragraph 137.
[8] Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net I*, paragraph 138.
[9] Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net I*, paragraphs 147-151.
[10] Judgment of 5 April 2022, Case C-140/20, *G.D.*, paragraph 83: Explicitly clarifying that other criteria for targeting data to be retained are not excluded.
[11] Judgment of 21 December 2016, Case C-203/15, *Tele2*, paragraphs 108-111: Referring to the possibility to limit the scope of the data retention obligations, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.
[12] Judgment of 30 April 2024, Case C-470/21 *La Quadrature du Net II*, paragraphs 101-103.

serious, as it is the case for access to data relating to the civil identity of users of electronic communications for the sole purpose of identifying the user concerned, and without it being possible for those data to be associated with information on the communications made.[13]

4) **General and indiscriminate retention of data relating to the civil identity of users of electronic communication systems**, without specific requirements or limitations concerning the retention period and no prior authorisation by a judicial authority or independent administrative authority being required. However, the Court has provided that measures should ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.[14]

5) **Expedited retention of traffic and location data held by service providers**, for the purpose of combating serious crimes subject to effective judicial review and limited to a specified period of time (which can be extended**).** The CJEU clarified that such orders can be issued early on in the criminal investigations[15], not limited to situations where a crime has already been committed but also where the commission of offences may reasonably be expected[16], does not have to be limited to suspects identified in advance but can include other persons whose data are able to shed light on the crime in question[17], and can be issued also in relation to specific geographic areas, including places where a person, possibly the victim of a serious crime, has disappeared.[18]

The CJEU has also clarified the requirements governing **access to data**:

- General requirement that access to retained data must be subject to substantive and procedural conditions to ensure that access is limited to what is necessary and proportionate.
- Legislation governing access must be proportionate to the seriousness of the interference with the fundamental rights in question: serious interferences can be justified only by the objective of fighting crime which must also be defined as 'serious' while for non-serious interferences access is justified in relation to the fight against 'criminal offences' generally.[19]
- National authorities must ensure in each individual case that categories of data requested and the period in respect of which access to those data is sought are limited to what is strictly necessary for the investigation in question and that the requested data makes an effective contribution to combating crime.[20]
- Requested data must have a link (at least an indirect link) to the intended purpose of investigating criminal offences.[21] At least regarding traffic and location data, access can, as a

[13] Judgment of 30 April 2024, Case C-470/21, *La Quadrature du Net II*, paragraphs 86-89, 92, and 131-132.
[14] Judgement of 5 April 2022, Case C-140/20 *Commissioner of An Garda Síochána and Others*, paragraph 67
[15] Judgment of 20 September 2022, Joined cases C-793/19 and C-794/19, *SpaceNet*, paragraph 120.
[16] Judgment of 20 September 2022, Joined cases C-793/19 and C-794/19, *SpaceNet*, paragraph 114.
[17] Judgment of 20 September 2022, Joined cases C-793/19 and C-794/19, *SpaceNet*, paragraph 104.
[18] Judgment of 20 September 2022, Joined cases C-793/19 and C-794/19, *SpaceNet,* paragraph 119.
[19] Judgment of 2 October 2018, C-207/16, *Ministerio Fiscal*, paragraphs 52-57.
[20] Judgment of 2 March 2021, Case C-746/18, *Prokuratuur*, paragraph 50.
[21] Judgment of 5 April 2022, Case C-140/20, *G.D.*, paragraph 105.

general rule, only be granted in relation to individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. The objective of combating criminal offences in general can justify the grant of access to traffic and location data stored by the telecommunication providers for the purpose of marketing and billing services.[22]

Finally, it is important to recall some of the **basic considerations and principles in relation to the proportionality assessment that result from the relevant case-law**:

- Retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, as regards combating serious crime, the data whose retention is provided for must be capable of contributing to the prevention, detection or prosecution of serious offences.[23]
- The overall proportionality of data retention obligations and access rules depend on the level of interference with fundamental rights to privacy, protection of personal data and freedom of expression. Interferences with fundamental rights are considered serious where the data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and thus to establish a profile of the persons concerned. Where no such conclusions can be drawn, the interference with fundamental rights was considered not being serious (this was recognised by the CJEU in relation to civil identity data and IP addresses).[24]
- The overall proportionality assessment needs to weigh interferences with fundamental rights to privacy and protection of personal data with other general public interests as well as the rights of others. Such general interests include safeguarding security. Similarly, the CJEU recognised that, as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment.[25] Furthermore, the CJEU recognised that the risk of systemic impunity is a valid consideration when balancing the relevant rights and interests. This could lead to interests of data retention to ensure effective criminal justice taking precedent over privacy should the data concerned be the only equally effective means of identifying the potential perpetrator with alternative investigative means being potentially more intrusive.[26]

[22] Judgment of 30 April 2024, Case C-470/21 *La Quadrature du Net II*, paragraph 98.
[23] Judgment of 8 April 2014, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, paragraph 59, and Judgment of 6 October 2020, Joined Cases C- 511/18, C- 512/18 and C- 520/18, *La Quadrature du Net I*, paragraph 133.
[24] Judgment of 30 April 2024, Case C-470/21, *La Quadrature du Net II*, paragraphs 86-89, 92, and 131-132.
[25] Judgment of 6 October 2020, Joined Cases C- 511/18, C- 512/18 and C- 520/18, *La Quadrature du Net I*, paragraph 126.
[26] Judgment of 30 April 2024, Case C-470/21 *La Quadrature du Net II*, paragraphs 119-122.

## 3. Exchange of views

In light of the above, the Presidency encourages Member States to provide their assessment of implementing the CJEU's jurisprudence in national law. Moreover, Member States are invited to share their views on how the requirements set out in the case-law can be translated into EU rules on data retention with a view to maintain and enhance capabilities of investigating and prosecuting crimes while being limited to what is necessary and proportionate.

In particular, the Presidency invites the Member States to address the following questions as a basis for our discussion:

1) **Scope of service providers:** Do you consider that OTTs (over-the-top services) should be required to retain traffic data?
    a. Which service providers and which services or data held by these service providers would you consider to be particularly relevant for criminal investigations?
    b. Are there other service providers covered by the e-Evidence Regulation (which includes in addition to electronic communication services also information society services as well as domain name registers) on which requiring the retention data would be particularly necessary for combating serious crime?
    c. Do you miss the possibility to impose a general and indiscriminate data retention obligation on telecommunication providers in order to locate missing persons, whose location is unknown to the authorities?

2) **Targeted/limited/differentiated retention regime for traffic and location data**: Do you consider targeted retention (based on personal or geographical criteria) a sufficient tool to investigate and combat serious crime?
    a. What are its benefits and shortcomings?
    b. Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?

3) **Expedited retention orders (Quick freeze):** Do you consider the possibility to order expedited retention of data in the possession of service providers as an added value, taking into account the scope as set out by the case-law and which may go beyond what Member States have implemented in relation to quick freeze provisions?
    a. In your Member State, how actively do the law enforcement and prosecution authorities make use of traffic and location data, which telecommunication providers are, in any case, storing for marketing and billing services? Is this data enough for them to successfully conduct their investigations?

4) **Retention periods:** In your opinion, for how long can a Member State extend the fixed period of general and indiscriminate data retention for the purpose of combating crimes threatening national security? This must be understood in the light of the continuing threat of terrorism which, given the geopolitical situation, is directed against Member States in the EU. How can we best determine retention periods in line with the case-law ensuring that such periods are limited to what is strictly necessary?

a. Should future EU rules on data retention not cover general and indiscriminate data retention in terms of national security in order to leave it for Member States to regulate this specific area?

b. How would you distinguish retention periods depending on the kind of data or service provider, relevance for criminal investigations or any other distinguishing criterion?
c. What are, in your view, the advantages and disadvantages of one fixed retention period across the EU, allowing for the possibility of renewals at the national level, or setting a range within which Member States may set shorter or longer retention periods?

5) **Scope of crimes for which availability of communication data is particularly relevant:** Which are the crimes where you would consider that availability of traffic and location data is particularly relevant for their effective investigation and prosecution?
   a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?
   b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

6) **Access rules and conditions**: To what extent should EU law regulate access conditions for data subject to EU retention obligations?
   a. Should access conditions be limited to what is strictly necessary under the case-law (including, in particular, the requirement that access and further use of data is limited to the purpose of investigating offences that can be regarded as sufficiently serious to justify serious interferences, as well as the requirement of prior authorisation by a court or independent administrative body in cases of serious interferences, following a reasoned request)?
   b. Should access conditions and rules also cover other requirements for national access to data retained by nationally established service providers, similar to those established in the e-Evidence Regulation such as standardised formats for access requests and submissions, time limits and use of secure communication channels?