Council of the European Union
General Secretariat

Brussels, 31 October 2025

WK 13500/2025 INIT

LIMITE

COPEN
CYBER
ENFOPOL
JAI
DATAPROTECT

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

WORKING DOCUMENT

From: To:	General Secretariat of the Council Delegations
N° prev. doc.:	WK 11640/2025
Subject:	Future rules on data retention in the European Union - Compilation of comments

Delegations may find in the Annex the comments received from Member States and the EU Counter Terrorism Coordinator on the above.

Contents

BULGARIA

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?**

We find that the scope of the new legislative proposal should include all providers that offer communication services or internet access, not just the so-called OTT providers, which are mandatory since their market share in terms of message transmission is particularly significant. This also applies to providers that provide VPN services. As an absolute minimum, user data, including payment data, as well as traffic data regarding the source and destination/address of messages, including IP addresses and the relevant data that allow their distinction in cases where dynamic IP addresses are used, must be stored.

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?**

Domain and hosting providers and email service providers should certainly fall within the scope of the proposal. Consideration could also be given to including payment service providers, cryptocurrency traders, etc.

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?

We find that location data (mobile operator cells) should continue to be stored for the purposes of conducting search operations and rescuing people, and the application of this tool to support the competent authorities in Bulgaria demonstrates a high degree of effectiveness.

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?

With regard to the targeted retention of data, we would like to point out the following: it is unreasonable to expect that it is possible (even from a technical point of view) for service providers to automatically retain only data that is initially suspected of being linked to a specific criminal activity. This is because, unless otherwise provided, the data should be deleted immediately after the transmission of the message has been completed. Even if the investigating authorities subsequently issue an order to retain such data in the context of criminal proceedings initiated on the basis of other information, valuable information that could be crucial to the outcome of the case will be lost.

The same reasoning is even more valid with regard to the retention of data protected by national provisions on professional secrecy, since at the time of retention the service provider would not be able to assess which data are of such a nature. Similar arguments could be put forward with a view to limiting the retention of data to certain categories of persons or to a certain geographical area, since such an approach would open the door wide to abuse by persons with criminal intent (for example, calls could only be made from areas outside the scope of the providers' obligations, telephone numbers could be registered to persons who do not fall within the scope of the data retention obligation, etc.).

Targeted data retention is also difficult to implement for technical reasons. When targeted retention is based on a geographical criterion, it should be borne in mind that the location of the cells of mobile operators is individual for each operator, and their coverage is not tied to a predefined geographical area. In addition, information about the location of the relevant cell is not automatically included in the collected data - providers are able to establish the link between the cell to which the data relates and the geographical location of this cell only in a specific case - in connection with a request from the competent judicial or investigative authorities.

Therefore, we consider the concept of "restricted data retention" to be far more appropriate, which is based on the retention of a limited number of data categories for a shorter period of time while adhering to strict access conditions.

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?

In Bulgaria, the competent investigative authorities do not have access to data that providers store for other purposes, such as marketing, after the six-month retention period for the purposes of combating crime has expired. In this sense, the “quick freeze” model can only be a complementary tool, as it concerns data from a previous moment (“past” data) that has already been stored by service providers on another basis. This method does not guarantee that the competent authorities will have data for the purposes of investigating a serious criminal act. This is because the above-mentioned other basis must have been present on the basis of which the providers stored the data, and it is quite possible that such a basis did not exist.

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?

In this regard, account should be taken of the case-law of the Court of Justice, according to which the obligations of providers to retain data for the purposes of protecting national security fall within the scope of Directive 2002/58/EC.

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?

We cannot give a clear answer regarding the length of the retention periods. However, it should be borne in mind that according to statistics, the majority of data is requested within the first four months of its generation, so this could be a starting point. In addition, an option could be considered where there would be a differentiation of the retention periods depending on the type of data. Regarding the possibility of introducing renewable retention orders, it should be noted that this model is not traditional and typical for the continental criminal justice system. However, flexibility in setting the periods in a future legislative act is preferable.

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?

According to the Bulgarian Constitution and the practice of our Constitutional Court, traffic and location data may be stored and collected only for the purposes of combating serious crime, therefore access to them in other cases is impossible. The same conclusion is also found in the practice of the Court of Justice of the European Union.

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)?

We find it logical that the basic requirements for access should be regulated in the possible legislative proposal - permission from a court or independent jurisdiction after a reasoned request, the data being related to the subject of the investigation.

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?

We do not see a need to regulate standardized formats and communication channels, since the main purpose of the instrument will be to regulate issues related to data retention, and it is a question of interaction between a national authority and a provider established on its territory, i.e. so-called "domestic" cases. The hypotheses of cross-border cooperation are anyway regulated in Regulation (EU) 2023/1543 on electronic evidence with all the details specified in the question itself.

CZECHIA

In general, for CZ it is essential to **resolve current situation** in relation to the strict criteria aimed at **limiting general data retention.**

Moreover, CZ believes that the conclusions of the High-Level Group on Access to Data cannot be meaningfully implemented without **amending the ePrivacy Directive to clearly define the limits of law enforcement and judicial authorities' access to certain types of data,** rather than treating such access merely as an exception to the right to privacy.

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?

It would certainly be beneficial for the potential new legislation to be **technologically neutral** so that for example **also OTTs providers would be required to retain data**, as much as this is technically possible. In this context, however, it will also be necessary **to consider the costs** that such new obligation for these electronic services would represent, because depending on the scope and duration of data retention, and given the amount of metadata, it can be assumed that high costs could be incurred by the obliged entities.

When searching for a missing person, it is essential to have location data quickly, essentially in real-time. In these cases, the Police Department conducting the search contacts the Police Presidium's operations center, and the procedure in these cases is very much based on cooperation. This purpose should be included in potential new instrument, but its concrete terms in this respect must be thoroughly discussed.

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?

CZ **does not consider targeted retention based on personal or geographical criteria sufficient tool** to investigate and combat serious crime. Its shortcomings have been discussed already quite extensively. According to our findings, this is technically demanding, costly, and not very effective for law enforcement. CZ is thus of the view that potential new legislation should **not prejudge such targeted retention as the only acceptable solution**. Our goal should be **a system that allows for an adequately graduated interference with the right to privacy**, but based on the fact that we do not know who and when will become the perpetrator or the victim.

We can imagine **limitation in terms of data categories** - data traffic generates a large amount of data and it is in our view not necessary to retain it all for use by law enforcement bodies. In addition, there is the issue of costs.

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?

CZ **does not consider quick freeze as alternative to general data retention regimes**. It can work especially when the crime is detected very soon after it is committed and the police knows the criteria and parameters according to which the orders can be targeted. As for the broader scope of use set out by the case-law of the ECJ, i.e. for example cases where the commission of an offence may reasonably be expected, this would be useful only in small percentage of cases. Data freezing also requires a speed that some companies are unable to provide.

In CZ, the vast majority of requests (about 90%) are sent to large companies that have data retention obligation (O2, T-Mobile, Vodafone). Cooperation with providers who do not have data retention obligation is of course less effective. The **level of data** which **they retain for their own purposes varies** and differs in the length of retention and the amount of data retained. In accordance with the Criminal Procedure Code, providers shall release the data they have at their disposal, i.e. if they retain any data for their own needs, they are obliged to release it. Especially with ISP companies that do not have a retention obligation, it is clear that **not all data is always available, especially in the required quality.**

After all, the obligation to retain data was established precisely with regard to the fact that companies either retain a different range of data for their own purposes, or retain data identical to law enforcement requirements, but not for a sufficiently long period. For example, information from BTS stations is erased very quickly depending on the operation of a particular BTS, while this is important data for law enforcement.

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?

In our view, data retention for the purposes of safeguarding **national security should be left for the Member states.**

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?

Data retention is of course **necessary in the case of crimes committed largely online**. But this is not the only case. Analysis of telecommunications data can lead to the acquisition of important evidence about the movements of the perpetrator or the victim, the presence of the perpetrator in a certain place, the contacts of the perpetrator, etc. It is therefore often **also** necessary in investigations of **other serious crimes, including serious violent crimes**. For example, when investigating murders, the police can often learn retrospectively through telecommunications data about how the victims lived and with whom they were in contact. At the beginning of the investigation, these data are often the only tangible source of information that can lead to the identification of the perpetrator, documentation of mutual ties, etc. If these data were not available, it would be impossible to file charges and bring the perpetrator to justice in many such cases.

According to CZ, it would be appropriate to **establish a general range of crimes given by the criminal rate**, which would **indicate certain seriousness of the crime**, **and a list of crimes** with a lower criminal rate, which would concern crimes **committed largely online** (stalking, hate crime, etc.), where the criminal rate would not be so high, but the lack of data would practically make the investigation impossible.

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?

As regards access to data, we can imagine regulation of the **requirement for prior authorisation by a court or an independent administrative authority** in cases of serious interference following a reasoned request.

It is possible to imagine a **differentiated access to data** by the law enforcement authorities depending on the nature of the retained data. The specific conditions for access should depend on what data is requested and for what purposes.

IRELAND

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?

Ireland is strongly in favour of requiring OTTs to retain traffic data. As far as practically possible, there should be, a level playing field across all service providers, whether they are traditional telecommunications providers or OTTs, with some limited differentiation based on their different models of service delivery.

A) The ability to access Metadata—such as IP logs, registration data, device identifiers, and login timestamp are crucial in most investigations for attribution and timeline reconstruction. With the inability to lawfully access content due to the challenge of encryption, metadata is reassuming increased significance in intelligence led investigations.

B) It would be useful to align the scope of a data retention instrument with the scope of services covered by the e-evidence regulation. There is significant overlap between data covered by the preservation and production order system in e-evidence and the type of data likely to be covered in a data retention instrument.

   Other Providers under e-Evidence Regulation: Domain name registrars, hosting providers, and e-commerce intermediaries should also retain identifying and transactional data to combat fraud, cyber-enabled crime, and child exploitation in particular. These services also impact on other areas of crime but those three areas are the most prevalent.

C) Missing Persons: The inability to impose general retention limits the capacity to locate vulnerable or missing persons promptly. Access to historic cell-site or IP data is often decisive in time-critical humanitarian cases.

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?

The targeted retention of data is somewhat useful but insufficient on its own. The ability to predict in advance the geographical area or the person who will commit a crime in advance is limited.

A) Benefits: There is a reduced privacy impact and the approach is enshrined in case law.

Shortcomings: There is a risk of data gaps meaning that resources may be wasted. There may also be inconsistent application of criteria. The approach hampers early-stage investigations when suspects are unknown meaning that time will be lost in time sensitive investigations where there is a potential risk to life.

B) Alternative Criteria:
A data-category-based model **may** provide the necessary proportionality while maintaining the ability to utilise data more meaningfully in investigations.

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?

Quick-freeze powers add value but are not a substitute for standing retention. They are reactive, not preventive. The event will generally have to have taken place before the quick freeze is utilised. This causes significant risk as time is lost in the initial phase of an investigation. Other evidential strands may be lost to law enforcement due to such delays.

A) Use of Existing Data: We access data retained for commercial or billing purposes; however, such data are often too limited in scope and duration. For serious offences, supplementary retained data (e.g. IP logs beyond 30 days) are usually required for successful investigations.

Greater transparency from service providers around exactly what data they hold for market and billing purposes may make this more effective. This is an important action in the lawful access roadmap (recommendation 17).

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?

Retention periods must balance necessity with proportionality. Ireland suggests that 12 months represents an appropriate balance for general and indiscriminate retention for the purpose of combatting crimes threatening national security. However, it should be acknowledged that complex investigations can take place over a number of years with timelines of up to 2 years not being unusual.

A) Ireland believes that future EU rules on data retention should not cover national security and that member states should continue to regulate in this area.
Ireland's national police force, An Garda Síochána, is responsible for both upholding national security and investigating crime. As such, we are acutely aware of the potential for unintended consequences of the imposition of legislating for law enforcement needs only. Any EU instrument on data retention for crime must ensure that there are not requirements imposed which potentially impact on the ability of each member state to protect their National security.

B) Differentiation: There is scope to differentiate on data category, with less intrusive forms of data being held longer than more intrusive forms.

C) c. Fixed vs Range: A fixed retention period provides for greater consistency and harmonisation. Providing a range may introduce some uncertainty around what is necessary and proportionate.

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?

Retained communications data are vital across multiple categories of serious crime.

A) Key Offences: Terrorism, organised crime, homicide, child sexual exploitation, human trafficking, cybercrime, and corruption.

B) Risk of Impunity: Cyber-enabled and transnational offences often leave no physical evidence—without data retention, offenders remain untraceable.

C) Coverage: All cyber-dependent and cyber-enabled offences should be included, given their reliance on electronic infrastructure for execution and concealment

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?

EU law should set common minimum access safeguards to ensure legality and mutual trust. It is also our strong view that the High Level Groups recommendations on the use of SPOC [Single Point of Contact] processes should be encouraged or indeed regulated for in any potential solution. This allows for the minimum access safeguards and the principles of proportionality and necessity to be encapsulated in internal access processes in both law enforcement authorities and providers.

A) Necessity and Authorisation: Access should be limited to serious offences, subject to prior judicial or independent authorisation, consistent with CJEU case-law.

B) Procedural Harmonisation: Standardised request formats, secure channels, and defined response timelines—aligned with e-Evidence Regulation—would improve efficiency, traceability, and legal certainty for both providers and law enforcement.

In summary, Ireland supports a balanced, legally robust retention framework that ensures the availability, integrity, and accessibility of communications data necessary to protect citizens, while respecting privacy and proportionality under EU law.

It is our position that the current situation is imbalanced and promotes the protection of privacy over the rights of the victim. Law enforcement across the EU is struggling with the ability to properly investigate offences where lawful access to communications data is a key factor in the investigation of the offence. As more crime continues to be conducted in the digital space, it is imperative that this balance is realigned.

ITALY

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]

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.

[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.
[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.

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 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]

---

[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.
[13] Judgment of 30 April 2024, Case C-470/21, *La Quadrature du Net II*, paragraphs 86-89, 92, and 131-132.

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]

[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.

- 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 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]

[21] Judgment of 5 April 2022, Case C-140/20, *G.D.*, paragraph 105.
[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?

Excluding OTTs from the list of obligated entities would prevent the legislation from achieving its intended purpose. As a matter of fact, daily activities are now pervaded by services that rely on the Internet; therefore, excluding a significant portion of providers, such as OTTs, would greatly reduce the traceability of a range of criminal activities. It would also leave the door open to evasive manoeuvres by criminals, who would turn to providers (and related communication channels) that are exempt from the retention obligation.

Moreover, any selection of obligated service providers should be carefully considered and adequately justified to avoid resulting in unlawful unequal treatment, which could also affect the functioning of the market.

It is therefore recommended to support the broadest possible scope of application of the future legislation, which includes OTTs among the service providers subject to the obligations, while also providing for the possibility of adapting the list to future technological and market developments.

    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?

Without prejudice to what has been set out under a), it is considered appropriate to ensure consistency with the e-evidence regulation by including all operators covered by it. The successful execution of a data retention or production order issued pursuant to that Regulation will depend on the actual existence of the data in the provider's possession at the time of receipt of the order, which can only be guaranteed for an adequate period by introducing a retention obligation.

Consideration should also be given to the possibility of including other providers, as suggested by some delegations during the COPEN meeting of 25 September 2025 (e.g. cryptocurrency providers, car manufacturers, etc.).

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?

Support is expressed for the generalised retention of traffic data for the purpose of locating missing persons, given the importance that such data may have for a quick location.

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?

The most frequently invoked advantage of "targeted" retention for investigative and crime prevention purposes is the reduction of the risk of unauthorised access to retained data. However, while targeted retention aims at reducing the quantity of retained data and consequently the risk of compromised or unauthorised access, as well as at containing the costs for service providers, this outcome is apparently not to be taken for granted, considering that service providers already voluntarily retain data for operational, contractual, commercial, financial, and other purposes.

Furthermore, the choice of limitation criteria appears rather complex. Subjective criteria, based on the characteristics of the data subject, are hard to implement and imply a high risk of discrimination. Geographic criteria, referred to in the case law of the EU Court of Justice, present technical challenges for defining areas due, for example, to the different locations of cell towers and the variable geographical areas they may cover, with possible repercussions on the effectiveness of investigations. Moreover, when based on crime statistics (e.g. identifying areas at high risk of crime), they require extremely reliable detection systems and highly significant data, which are not always available and may be affected by unreported crime, depending also on the type of offence. This could lead to consequences in the opposite direction of what is desired. For example, violent crimes leave clear traces and are easily located; financial and white-collar crimes, instead, have a more complex commission process, are less tied to a specific territory, and have a high number of unreported cases. The result would be increased attention and retention obligations for more evident crimes, while investigative tools would be reduced for crimes that are more difficult to detect and prove.

It should also be noted that limiting the retention obligation to areas where crimes are more likely to be committed would risk excluding the retention of all data related to preparatory activities, which may well take place far from the place where the offence is perpetrated. There is also a risk of circumvention by criminal organisations, which could identify and avoid the areas covered by the retention obligation, thus concentrating their activities elsewhere. Similar remarks can be made with respect to the criteria based on proximity to critical infrastructure.

As for the selective criterion based on the seriousness of the offence, it implies that mandatory retention would only concern the data collected after a suspicion of criminal activity (whether committed, ongoing, or at least in the preliminary stage) has arisen, which the service provider would also need to be informed of to identify the triggering of its obligation. Before that moment, the criterion would not be applicable. Therefore, it is a suitable criterion for limiting future access to data by law enforcement or judicial authorities, rather than a prerequisite obligation of retention.

It should be pointed out, however, that the Court of Justice of the EU has not ruled out the use of criteria other than those listed above to define data retention.

The future EU legislation could therefore impose a retention obligation whose limits are defined by an adequate retention period (to be determined), differentiated according to the specific type and sensitivity of the traffic data considered, and supported by enhanced cybersecurity measures. Such an obligation could be sufficiently defined to pass the scrutiny of the Court of Justice without limiting the effectiveness of investigative and crime prevention activities.

b. Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?

Without prejudice to what has been outlined above in reply to the previous question, the general premise appears to be that the **purpose of the draft directive** is to require all Member States to make provision for a **minimum retention obligation**. The principle should be that of **minimum harmonisation**: Member States are required to introduce a retention obligation that is **at least** as extensive as that provided for in the directive, obviously respecting a fair balance of the interests and rights at stake, notably among the various fundamental rights involved. This should **not** result in the adoption of common legislation that slavishly incorporates the criteria and limitations suggested in the case law of the Court of Justice to date by crystallising them into general rules, both because such criteria appear excessively restrictive and hardly practicable, thus undermining the effectiveness of investigations, and because the case law takes into account individual domestic set of rules on a case-by-case basis, in relation to the technology existing at a given historical moment and is therefore already obsolete from various points of view.

As mentioned, the need to minimise the potential risks that mandatory retention may pose to the protection of data subjects' fundamental rights could be efficiently pursued by requiring service providers to adopt enhanced measures that ensure a high level of security for retained data against possible abuses, unauthorised access, profiling, or loss and damage (e.g. technical security measures, high-level training and reliability of involved employees, etc.). Therefore, **a possible solution could be to impose a generalised retention obligation for certain types of non-content data, for a limited period (to be defined), accompanied by strengthened security requirements.**

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?

Rapid retention (quick freeze) is certainly an added value, but it **may not be considered a substitute for systematic retention**, as it requires at least the existence of a suspicion of an offence. Therefore, in the absence of a general retention obligation, the risk that a quick freeze order arrives too late, when the data has already been deleted, increases exponentially.

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?

Data not available.

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?

Retention obligations imposed for defence and national security purposes should not be covered by the new directive; they indeed should be expressly excluded from its scope, remaining within the competence of every single Member State.

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?

See previous answer.

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?

As already remarked, limitations on the retention obligation based on the type and size of providers, or on the seriousness of offences (which is only triggered after a suspicion of criminal activity arises), may not be shared.

As to limited retention periods according to the type of data, this kind of assessment requires information on the types of data that are most indispensable for investigations in practice, but this type of information is not available at the moment.

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?

Imposing a sufficiently long minimum retention period in all EU States, adequately covering broad categories of traffic data and service providers, and allowing for extensions at a national level, would help ensure effective action against crime, which is increasingly transnational in nature.

Ensuring a retention obligation for at least a defined minimum period prevents the service provider, who already legitimately holds and retains traffic data for commercial, operational, technical, or other reasons related to its business, from deleting it at any time, either spontaneously or at the request of the data subject, thus risking jeopardising potential investigations.

However, this period should be designed as a **minimum** mandatory retention **period** to be ensured by States, **rather than** as a maximum limit.

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?

The answer to this question requires data and evaluations derived from investigative and judicial practice, which are not available at the moment.

In any case, it is worth reiterating that if the retention obligation is made dependent upon a connection with a specific offence (or offences of a certain seriousness), the retention obligation would be anchored to the existence of a suspicion of criminal activity, thus excluding all data already in the provider's possession beforehand, as a result of its normal activity. This would entail a huge limitation and could undermine the effectiveness of subsequent investigations. Therefore, such a criterion should be avoided for defining mandatory retention. On the other hand, that criterion appears more suitable for limiting subsequent access to data by authorities, which necessarily occurs when at least a suspicion of criminal activity has arisen.

a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?

See previous answer.

b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

See previous answer.

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?

If the draft directive includes provisions on access, these should also be limited to minimum harmonisation in compliance with the principles of subsidiarity and proportionality. Therefore, the conditions indicated as essential by the Court of Justice would be sufficient (purpose of investigating into enough serious offences, procedural safeguards including authorisations by judicial authorities, strict necessity and proportionality of the data requested to the specific investigative purpose).

LITHUANIA

Comments from the Police Department under the Ministry of the Interior of the Republic of Lithuania

1) Scope of service providers: Do you consider that OTTs (over-the-top services) should be required to retain traffic data?

Yes, Lithuania agrees that OTT services should be included in the data retention framework. Considering that these services are increasingly used for electronic communication, the data they hold can be highly important for criminal investigations. Data retention is essential to ensure effective law enforcement.

a. Which service providers and which services or data held by these service providers would you consider to be particularly relevant for criminal investigations?

Particularly important service providers include:

• Email services (e.g., Gmail, Outlook),

• Instant messaging and voice/video call services (e.g., WhatsApp, Signal, Telegram, Skype),

• Social media platforms (e.g., Facebook, Instagram, X),

• File sharing and storage services (e.g., Google Drive, Dropbox).

Key metadata attributes:

• IP addresses,

• Login and logout times,

• Device identifiers,

• Location information,

• Contact lists,

• Message sending and receiving timestamps.

This data helps identify suspects' connections, activity patterns, locations, and potential timeframes of criminal activity.

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?

Yes, information society service providers such as:

• Cloud storage services (e.g., Google Drive, OneDrive),

• Domain name registries,

• Content hosting platforms (e.g., YouTube, TikTok),

• E-commerce platforms (e.g., Amazon, eBay),

• Cryptocurrency exchanges.

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?

Yes, Lithuania supports the possibility of applying a general data retention obligation to telecommunications service providers in certain exceptional cases, such as the search for missing persons. In today's era of electronic devices, almost every individual uses a mobile phone that generates location data. A person may go missing for various reasons — becoming a victim of a crime or an accident — and such an event can occur anywhere, regardless of the individual. In these situations, the availability of data can be a decisive factor in enabling a rapid and effective response. However, such access should be strictly regulated and limited in purpose and duration to ensure compliance with the principle of proportionality.

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?

Benefits:

• Proportionality – Targeted data retention allows limiting interference with individuals' privacy, as data are collected only according to clearly defined criteria. However, the impact of this advantage is limited, since the metadata set alone does not significantly restrict personal freedoms. To derive a comprehensive picture of an individual's private life from metadata, additional economic and human resources are required – analytical capabilities, contextual information, and cross-referenced data sources.

Shortcomings:

• Need for investment by service providers – Service providers will have to continuously adapt to evolving law enforcement requirements, which demands additional investments in infrastructure, data management systems, and storage capacity. Moreover, they may often be unable to react swiftly to new or specific data retention requests, especially if such requirements change frequently or are technologically complex.

• Need for law enforcement resources – Crime is a dynamic phenomenon, constantly evolving with technology, social trends, and the geopolitical situation. Law enforcement authorities will need to continuously invest in crime analysis, risk area identification, and geographic attribute monitoring to ensure that targeted retention remains relevant and effective. Furthermore, the dangerous nature of certain crimes – particularly organized, cyber, or terrorist activities – requires rapid response and data availability, which may be limited under a targeted retention model.

• Risk of data loss – If a service provider does not retain certain categories of data or if the retention period is too short, critical information for investigations may be lost.

• Risk of concealment – Criminals may exploit gaps in the targeted retention system by using concealment strategies, alternative communication channels, or operating outside monitored geographic areas, thereby avoiding surveillance.

We consider that it is practically impossible to effectively differentiate or restrict data retention obligations according to other criteria, since it is not feasible to precisely assess the geography of crime, identify service providers specifically used for criminal purposes, or predict where relevant data may arise. The loss of such data would have a highly negative impact on criminal investigations, given that electronic communications data are crucial in the majority of criminal cases.

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?

The expedited data preservation mechanism is significant and beneficial. This measure allows data to be temporarily "frozen" while law enforcement authorities submit a formal request for its disclosure. It is particularly important in cases where data may be quickly deleted or altered, and its preservation is essential for the continuation of an investigation. This is especially relevant in combating cybercrime, terrorism, child exploitation, and other serious offences where speed and data availability are critically important.

It is important to note that expedited preservation is usually applied once a specific incident is already known — when law enforcement authorities have a reasonable suspicion of a crime and seek to preserve data until a full investigation can begin. For example, under Regulation (EU) 2023/1543, a judicial authority in one EU Member State may instruct a service provider in another Member State to temporarily preserve IP addresses, user identification data, emails, messages, or other communication data until an official production order is issued.

Although expedited data preservation is a valuable tool, its applicability is limited because it operates only when law enforcement already has information about a committed offence or reasonable grounds to suspect an imminent one. In other words, "freezing" is a reactive rather than a preventive measure — it cannot be applied proactively when the time or location of a crime is unknown.

Since crime is a dynamic and unpredictable phenomenon, it is impossible to accurately predict in advance what types of crimes will occur, in which locations, or which data will be required. This is particularly true for cybercrime, human trafficking, terrorism, and organised crime, where activities often take place covertly, across multiple jurisdictions, and through anonymous digital channels.

Therefore, while expedited data preservation helps to secure information in known cases, it cannot replace a systematic, pre-defined data retention mechanism that ensures law enforcement has access to essential data even in unexpected or complex investigations.

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?

Operators collect only the minimal data necessary for their commercial activities — typically login times, IP addresses, session duration and billing information — but these data are not sufficient for successful and comprehensive criminal investigations.

Law enforcement, by contrast, requires additional data, such as:

• the time of SIM-card activation,

• information needed to identify and determine the source of a communication,

• information needed to determine the destination endpoint of a communication,

• information needed to identify the communication equipment or the entity that identifies it,

• data related to internet access, email and VoIP calls,

• data necessary to determine the location of mobile communication equipment.

Without these data, investigations become fragmented, which severely complicates the identification of perpetrators or their victims, the determination of locations, the analysis of activity patterns, and the clarification of other circumstances of the crime. In such cases there is a risk that the crime will remain unsolved or that the investigation will take a disproportionately long time. Therefore, an expedited preservation mechanism is necessary to ensure that not only commercial but also operational data — which might be deleted or rendered unavailable if not promptly "frozen" — are preserved.

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?

When determining the data retention period, it is appropriate to take into account the current geopolitical situation, which is tense and unstable. Member States are facing constant threats, including hybrid attacks, cyber incidents, information operations, and even physical actions targeting critical infrastructure. Hostile states and organizations use various methods — including the use of SIM cards for geolocation purposes — to monitor, manipulate, or influence activities within the EU territory.

Such threats are often difficult to predict, long-term, and systemic; therefore, Member States should have the possibility to apply longer data retention periods when necessary to safeguard national security. However, these periods must be strictly limited and based on objective criteria in order to maintain the principle of proportionality.

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?

National security matters are sensitive and depend on the specific threats faced by each Member State. Therefore, EU rules should not directly cover general and indiscriminate data retention in this area. These competences should remain with the Member States, which are best placed to assess their own security needs and apply appropriate data retention measures.

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?

Considering the points outlined above, the establishment and practical implementation of such criteria are complex and inherently limited. This would require continuous investment in analytical systems, strengthening of law enforcement capacities, technical adjustments by service providers, and a

consistent risk assessment mechanism. Moreover, crime is a dynamic phenomenon, making it often impossible to predetermine which data will be needed and in what circumstances.

Therefore, it would be reasonable to apply a universal data retention system in which all essential data are stored, while access to them is strictly regulated. It should be clearly defined:

• who can access the data (institutions, officials),

• for what purposes (only for the investigation of specific, sufficiently serious crimes),

• to what extent (only the data necessary for the specific investigation).

Such a model would allow the preservation of information essential for investigations while ensuring the protection of fundamental rights and adherence to the principle of proportionality.

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?

Advantages:

• Legal clarity and consistency – a uniform retention period across the EU would ensure a coherent approach to data protection and law enforcement capabilities.

• Facilitated cross-border cooperation – particularly important in transnational cases where data availability depends on another country's retention policy.

• Prevention of abuse – criminals would not be able to deliberately choose service providers in countries with more lenient or shorter data retention regimes. A unified EU-level standard would reduce opportunities to exploit legal differences for criminal purposes.

Disadvantages:

• Insufficient flexibility – a single retention period may be too short for some Member States facing higher threats, or too long for others where the risk is lower.

• Potential data loss – if the period is too short, law enforcement may lose critical data, especially in long-term investigations.

We would like considering an interval-based model, under which the EU would set minimum and maximum retention periods, while Member States could adjust them according to national needs. This model should be based on the actual information needs of criminal investigations, 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.

Such an approach would help to maintain a balance between effective crime prevention and the protection of fundamental rights.

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?

Traffic and location data are important in more than 90% of criminal investigations, and are critical in the majority of those cases, because electronic services have become an integral part of everyday life in modern society. Communication, financial transactions, social connections, information

searches and even physical movement often occur via digital channels that are generated and recorded by various service providers.

The prevalence of electronic services includes:

• Mobile communications and the internet,

• Social networks and messaging platforms,

• Cloud storage and email,

• Navigation and geolocation systems,

• Electronic payments and banking transactions,

• Smart devices and apps.

Because of this digital environment, traffic and location data have become the primary source enabling law enforcement to reconstruct the sequence of events, identify suspects, determine their whereabouts, contacts and activity patterns. Without these data, even traditional crimes — such as theft, violent offences, sexual offences or fraud — become difficult to resolve.

a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?

A significant threat is posed by criminal activities covering a wide range of offences — from corruption, smuggling, illicit asset acquisition, financial crimes, human trafficking, and the illegal possession of weapons or narcotic substances, to document forgery, unlawful influence on public officials, and other acts harmful to state interests and public security.

In addition to traditional threats, hybrid threats are playing an increasingly important role, targeting critical infrastructure, including energy, communications, transport, and public administration systems. Such threats often involve coordinated actions that combine cyber, informational, economic, and physical attacks.

b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

The identification and investigation of criminal offences should not be limited solely to cyberspace or the use of digital tools. Modern crimes are often carried out in a complex manner, employing various means and channels — both in the physical and digital domains.

Therefore, it is essential to ensure that criminal activities are assessed broadly, covering all their aspects — from planning and execution to evidence collection and suspect identification — regardless of whether the crime was committed using digital tools or traditional methods.

This approach should apply to all types of offences, not just cybercrime. It includes:

• economic crimes (e.g., fraud, illicit enrichment),

• corruption-related offences,

• crimes against public administration,

• crimes against individuals,

• crimes against property,

• human trafficking, illicit drug trafficking, and others.

It is crucial that law enforcement authorities have the capacity and competence to investigate various types of crimes comprehensively, identify perpetrators, and ensure accountability. This not only strengthens public trust in the justice system but also reduces the sense of impunity, which is one of the factors encouraging criminal behaviour.

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)?

EU law should clearly establish that access to data subject to EU data retention requirements must be strictly proportionate, based on a legitimate purpose, and limited to what is necessary. In line with the case law of the Court of Justice of the European Union, access should be permitted only when:

• Investigating crimes that are considered sufficiently serious to justify a significant interference with an individual's privacy.

• There is a well-founded request clearly specifying the need for the data and the purpose of the investigation.

• Prior authorization has been obtained from an independent authority — a court or an administrative supervisory body — particularly in cases of serious interference.

Such requirements are essential to ensure that data access is not used for excessive or disproportionate purposes and that the rights of data subjects are adequately protected. They also contribute to reducing impunity by enabling the effective investigation of serious criminal offences while maintaining a solid legal basis and oversight.

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?

It is possible to support the idea that EU law should establish common principles governing national access to data, particularly when it concerns OTT service providers (e.g., messaging, email, and cloud services). In such cases, it would be effective to apply standardized request formats, clear deadlines, and secure communication requirements in order to ensure transparency, data protection, and the efficient operation of law enforcement authorities.

In contrast, in the case of traditional telecommunications operators, the existing practices are often already sufficiently developed and regulated at the national level. Therefore, any additional regulation could be applied more flexibly, taking into account specific situations and practical needs.

Comments from the Prosecutor Generals' Office of the Republic of Lithuania

1) Scope of service providers: Do you consider that Otas (over-the-top services) should be required to retain traffic data?
Yes.

a. Which service providers and which services or data held by these service providers would you consider to be particularly relevant for criminal investigations?
The future regulation should cover all service providers that have access to date, including OTT (over-the-top services). The data held by electronic communications network and service providers, as specified in the annex to the Law on Electronic Communications of the Republic of Lithuania, is particularly important for criminal investigations:

- data necessary to identify the source of the communication;
- data necessary to identify the destination of the communication;
- data necessary to identify the date, time, and duration of the communication;
- data necessary to identify the type of communication;
- data necessary to identify the service recipient's communication equipment;
- data necessary to determine the location of mobile communication equipment;
- data necessary to determine and record the content of the communication.

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?
Yes, such requirements would be particularly significant for companies providing Internet domain name and IP numbering services, as this data is important for identifying perpetrators of offences and the technologies they use.

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?
The obligation to store data on missing persons should also apply. The current legal regulation in Lithuania is essentially adequate, but the limited and insufficient data retention periods specified in the legislation pose problems, as they may hinder the search for missing persons and the rapid determination of their whereabouts.

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?
We believe that such regime would be insufficient.

a. What are its benefits and shortcomings?
The main benefit is that the obligation of service providers to store data, as laid down in legislation, ensures that such data will be available for investigation. However, a significant shortcoming is that the limited retention regime in certain cases hinders both the prevention and investigation of offences, as it is not always possible to predict in advance where a crime will be committed and who may commit it.

b. Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?

Limitations may be imposed according to data categories or types of service providers. However, retention volumes should not be limited – it would be more reasonable to restrict only access to data, taking into account the severity and nature of the offence. A differentiated storage regime based on personal or geographical criteria is difficult to implement, as it is often impossible to predict in advance the location of crimes or their possible perpetrators.

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?
Yes, this option is an added value, but it cannot replace advance data storage – it is only an additional measure in certain cases.

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?
The law enforcement and prosecution authorities make use of traffic and location data rather often for crime investigation and perpetrator identification. The added value of these data is very important. However, the data which telecommunication providers are storing for marketing and billing services are insufficient for a successful investigation – more detailed data are needed to fully uncover criminal offences.

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?
Currently, the data retention periods specified in legislation in certain cases hinder the combating of crimes threatening national and public security as the perpetrators of such crimes are often only identified after the specified retention periods have expired. In consideration that some of the most dangerous crimes are not even subject to a statute of limitations, it is necessary to ensure a significantly longer data retention period, particularly in the fight against terrorism, war crimes, or organised crime. In our opinion, data should be stored for at least 10 years, only the access to these data should be restricted based on the severity of crimes under investigation.

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?
Yes, this area should be regulated by Member States, as national security issues are closely linked to the threats and needs of a particular state.

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?
Retention periods could vary depending on the severity and nature of the offence. We believe that, with court sanction, it should be possible to access all data for up to one year when searching for missing persons and investigating all criminal offences punishable by arrest or imprisonment, up to 3 years – when investigating criminal offences punishable by imprisonment of 3 years or more, up to 10 years – when investigating criminal offences related to terrorism and organised crime, war crimes or crimes against humanity, or for which imprisonment for 10 years or more is provided.

Different periods could be applied depending on the data categories and their importance to the investigation.

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?
A uniform minimum retention period across the EU would provide greater legal clarity and ensure that all Member States have access to the same categories of data. This would facilitate and accelerate mutual cooperation, preventing criminals from taking advantage of less stringent legal regulations in individual Member States. At the same time, Member States should be allowed to set longer retention periods in line with their national needs.

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?
The availability of such data is particularly important in investigating crimes related to national security and organised crime, the consequences of which involve loss of life or destruction of critical infrastructure.

a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?
The greatest risk of systemic impunity is posed by crimes committed in cyberspace (crimes against the security of electronic data, proper functioning of the state's energy and other infrastructure, fraud, etc.), as well as the distribution of narcotic and psychotropic substances, smuggling, contract violent crimes, terrorism, and other crimes committed in the context of organised crime.

b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?
Yes, this should cover all crimes committed in cyberspace or using technology, as well as other crimes that were committed with the use of relevant means of communication. In addition, the conditions for accessing such data should be regulated uniformly across the EU, with mandatory court authorisation and access linked to the severity and dangerousness of the crime.

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)?
Yes, access to retained data must be strictly limited so that it is proportionate and consistent with the goals of the investigation of crimes based on their dangerousness. Such access should only be linked to sufficiently serious crimes that justify a serious restriction of a person's rights. It is essential to require prior authorisation from a court or independent administrative authority when deciding on access on the basis of 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?

No, such technical access conditions should not be regulated at EU level. However, the application of different directives and regulations should be harmonised in matters related to the investigation of criminal offences, giving priority to those European Union legal acts that regulate processes related to criminal prosecution, as well as the use and retention of data

It should also be noted that the regulation concerning the possible use of certain data obtained and used in criminal investigations should be reviewed with a view to allowing their use in other proceedings related to the application of disciplinary liability, fair competition, public procurement, as well as the assessment of transactions and investors, where such matters are connected to the national security interests of the state and similar concerns.

Comment from the State Security Department of the Republic of Lithuania

In view of the specific nature of the area of national security and the principle enshrined in European Union law that Member States are responsible for safeguarding their national security, Member States should remain free to determine the retention periods for data on electronic communications in order to combat threats to national security. For this reason, European Union legislation should not regulate data retention periods that are general and indiscriminate to all Member States.

LATVIA

Latvia supports finding a solution for data retention and accessibility for law enforcement authorities that (depending on the category and severity of the offense) ensures at least the minimum necessary data availability to investigate or prevent each violation/offense. This is especially relevant for offenses committed fully or partially in cyberspace, provided that the offense is punishable under national law and the authority is legally obliged to investigate and prosecute.

The general principle is clear, namely, for less serious crimes, there should be a possibility to request at least the minimum necessary data with minimal impact on privacy. For serious crimes there should be a possibility to request more data if needed. However, applying these principles in detail may lead to differences in implementation across Member States, so it would be useful to establish unified guidelines.

Latvia also supports aligning data retention regulations with other EU-level regulations that provide law enforcement access to retained data. This includes harmonizing regulations regarding access to data flows [traffic data] or location data for investigating administrative offenses, such as in the field of consumer protection, as provided in Regulation (EU) 2017/2394. According to Recital 7, Article 9(2), and Article 42 of Regulation (EU) 2017/2394, Member States are obliged to ensure the relevant minimum powers for competent authorities. These powers include tracking data flows [traffic data], identifying involved persons, and determining website owners.

Currently, there are uncertainties regarding whether retained data can be used in administrative offense proceedings or investigations of less serious criminal offenses. There is active discussion about the admissibility of using retained data for investigating certain administrative offenses, especially when denying access to data would compromise investigation and result in automatic impunity.

Latvia supports a solution that ensures both user rights protection and the ability to investigate punishable crimes and offenses. If law enforcement authorities are obliged to investigate crimes and offenses and it is established that access to specific data from the retained dataset is necessary for investigation and detection, then the possibility to request the minimum necessary data must be provided. The volume of requested data should be proportionate to the severity of the offense under investigation.

Latvia supports choosing a solution that is technically feasible and proportionate to the benefit. A solution that is technically unfeasible or prone to errors and is considered to be ineffective from the law enforcement perspective—leading to an increase in unsolved cases—would not be supported. Privacy rights must be balanced with the right to justice for victims of criminal offenses. Guarantees and controls for data processing must be provided, thereby improving the regulation where deficiencies were found.

Latvia's answers to questions posed in document WK **11640/2025** INIT:

1. Scope of Service Providers

Q: Should OTT (over-the-top) service providers be required to retain traffic data?

A: Yes.

a. Which service providers and which of their services or data do you consider particularly important for criminal investigations?

- A requirement should be established to retain a minimum set of metadata (IP addresses, user/account ID, login data), with a clear exclusion of content retention.

b. Are there other service providers covered by the e-Evidence Regulation (which includes information society services and domain name registries in addition to electronic communications services) for whom data retention requirements would be particularly necessary in combating serious crimes?

- Not identified.

c. Do you lack the ability to impose a general and non-differentiated data retention obligation on telecommunications service providers to locate missing persons whose whereabouts are unknown to authorities?

- A unified understanding is needed that such an option is permissible / lawful / proportionate.

---

2. Targeted/Limited/Differentiated Retention of Traffic and Location Data

Q: Do you consider targeted data retention (based on personal or geographic criteria) a sufficient tool to investigate and combat serious crimes?

A: No, targeted data retention is technically impossible with the existing technical equipment of electronic communications service providers. Its implementation would lead to the possibility of errors, incomplete data, ineffective work of law enforcement authorities.

a. What are the benefits and drawbacks of such an approach?

- Differentiated data retention entails error risks and data unavailability. A significant drawback is that retaining dynamic IP addresses requires retaining traffic data as well. Therefore, traffic data cannot be retained for a shorter period than dynamic IP addresses, which the ECJ rulings allow to be retained longer.

b. Could data retention obligations be meaningfully limited based on other criteria, such as data categories or service providers?

- [Response not provided]

---

3. Emergency Data Retention Orders ("Quick Freeze")

Q: Do you consider the ability to issue urgent data retention orders for data held by service providers to be of added value, considering the scope defined in case law, which may exceed what Member States have implemented regarding "quick freeze" provisions?

A: The quick freeze mechanism is an effective tool to prevent significant data loss, ensuring data is retained until court approval is obtained. It should be used as a mandatory EU instrument to prevent data loss.

a. How actively do law enforcement and prosecution authorities in your Member State use traffic (load) data and location data that electronic communications service providers retain for marketing and billing purposes? Are these data sufficient for successful investigations?

- The most common issues in operational practice relate to the short-term availability and deletion of data, and the unavailability of data from OTT platforms. For example, insufficient retention periods often hinder murder investigations, where obtained information could lead to new investigative directions, but the lack of retained data (due to deletion) makes verification difficult. Retention periods vary by provider, typically ranging from 1 to 3 months. Law enforcement authorities have indicated that such limited timeframes are insufficient for investigating complex and serious crimes.

4. Data Retention Periods

Q: In your opinion, how long could a Member State extend the general and non-differentiated data retention period to combat crimes threatening national security? This should be assessed considering ongoing terrorism threats targeting EU Member States due to the geopolitical situation. What is the best way to define retention periods so they comply with case law and are limited to what is strictly necessary?

a. Should future EU data retention rules exclude general and non-differentiated data retention for national security purposes, leaving this specific area to Member States?

- Yes, Latvia agrees that data retention for national security purposes could be excluded from EU regulation.

b. How would you differentiate retention periods based on the type of data or service provider, relevance to criminal investigations, or other criteria?

- Latvia does not support solutions with differentiated retention periods if they involve separate retention of dynamic IP addresses and traffic data. Service providers indicate that it is technically impossible to separate these in a way that dynamic IP addresses could be used without traffic data.

c. What are the pros and cons of setting a fixed retention period across the EU with the possibility of extension at the national level, or defining an interval within which Member States can set shorter or longer retention periods?

- The most important aspect of a unified retention period is technical feasibility, which service providers can currently ensure. A solution that requires differentiated retention of various data categories over different periods introduces error risks or even technical infeasibility.

---

5. Types of Crimes Where Access to Communication Data Is Especially Important

Q: Which crimes do you consider require access to traffic and location data for effective investigation and prosecution?

- Crimes committed in cyberspace.

a. Which crimes pose a systemic impunity risk due to the lack of traffic and location data?

- Crimes committed in cyberspace.

b. Should this include all cyber-enabled or cyber-dependent crimes, or only some of them, or other types of crimes?

- Access to minimally necessary data should also be ensured for other crimes, with prior control by a court or administrative authority. For example:
    - **5.b.1.** In competition law violations, location data may be needed to identify significant breaches that could be equivalent to criminal offenses.
    - **5.b.2.** In consumer protection, since January 17, 2020, Regulation (EU) 2017/2394 applies across the EU. Article 9(2)(b) of the Regulation grants competent consumer protection authorities the minimum powers to request all relevant information, data, or documents from any public authority, structure, agency, or any natural or legal person to determine whether a violation has occurred. These powers include tracking data flows [traffic data], identifying involved persons, and determining website owners. Recital 10 of the Regulation explicitly states that such information and evidence must be provided even when requested from telecom operators, domain registries, and hosting providers.

---

6. Access Rules and Conditions

Q: To what extent should EU legislation regulate access conditions to data subject to EU data retention requirements?

- A unified minimum retention period across all EU Member States is necessary to ensure legal certainty and predictability in the application of the e-Evidence Regulation.

a. Should access conditions be limited to what is strictly necessary under case law (e.g., access and further use only for sufficiently serious crimes, prior court or independent authority approval for significant intrusions)?

- Amendments to the Electronic Communications Law are currently being drafted to address access to retained data. The draft law stipulates that electronic communications providers must provide retained data upon request from operational entities or criminal procedure authorities, in accordance with the Operational Activities Law or Criminal Procedure Law. However, if connection (traffic) or location data is needed, authorities must apply to the court. According to ECJ case law, such data may only be used for national security, combating serious crime, and preventing serious threats to public safety. Latvia supports the current position that court control is required only when connection or location data is requested, and such data may only be requested for serious or especially serious crimes.

  However, at the EU level, a solution must be found to ensure minimal data availability for investigating less serious crimes, criminal offenses, and administrative violations.

  In cases of significant intrusion, access should only be allowed with court or independent authority approval. For less sensitive data, prosecutor approval should suffice.

Criteria should be developed for the process initiator to assess before requesting such data from the court. A broader regulation should be considered in a directive or regulation, allowing control by either a court or an independent authority (e.g., under certain conditions, the prosecutor could perform this role).

b. Should access conditions also apply to national access to data held by nationally established service providers, similar to the e-Evidence Regulation (e.g., standardized request formats, deadlines, secure communication channels)?

- Latvia supports unified procedural standards at the EU level (as in the e-Evidence Regulation): standardized requests, deadlines, secure channels, and audit mechanisms.

Regarding the supervision of the compliance of operational activities and the activities of state security institutions with the law, it can be indicated that the information that comes into the possession of the Prosecutor General's Office clearly shows that operational activity subjects, when performing the tasks specified in the law, often request information from electronic communications merchants. Unequivocally, the electronic communications data that are currently retained by merchants are important in the practical activities of operational activity subjects to effectively prevent threats to state security, as well as prevent and detect criminal offenses.

The most frequent problems in the practical activities of operational activity subjects are related to the temporary availability and deletion of data, and the inaccessibility of data from OTT (over-the-top service) platforms. For example, **the insufficiency of retention periods** is often an obstacle to investigating murders, when the information obtained is the basis for putting forward a new version, but the lack of retained data, because they have been deleted, creates difficulties in verifying it.

Criminals use communication applications (**OTT platforms**), which currently do not oblige themselves to retain even minimal metadata. This hinders investigations and creates a risk that serious crimes remain unsolved.

It is necessary to support a data retention regime based on objective criteria (person, geography, data category, type of service provider). This ensures a balance between the needs of the investigation and the protection of fundamental rights.

It is also necessary as an obligation for OTT service providers to retain a minimum set of metadata (IP address, user ID, connection time), which is essential for the investigation of serious crimes.

We draw your attention to the fact that **the accelerated retention mechanism (quick freeze)** is an effective tool to prevent significant data loss, ensuring that data is retained until court approval is received.

We agree that different time limits should be set for different categories of data: longer for IP addresses and identity data, and shorter for detailed location and traffic data, with stricter control.

We support a targeted, proportionate and legally harmonised data retention framework to include:

1. **A differentiated retention regime** – to establish obligations by data type and service provider type (e.g. IP addresses longer, location data shorter).

It should be noted that amendments to the Electronic Communications Law are currently being made. The main thing is that the amendments **do not provide for a new obligation for operators to retain all data for a certain period**, as this would contradict the findings of the Court of Justice of the European Union. The project envisages organizing the procedure for how subjects of operational activities can request data that are already available to operators for their own needs, for example, for billing or network maintenance. Access to this data will henceforth be closely linked to **targeting and control**: a request is possible only in the event of crimes or threats to national security and only with the court's approval. Therefore, these amendments do not expand the amount of data to be stored but rather **clarify the access procedure** so that it complies with both human rights and practical investigative needs.

2. **OTT metadata retention** – establish an obligation to retain a minimum set of metadata (IP, account ID, login details), with a clear exclusion for content retention.

3. **Accelerated retention mechanism (quick freeze)** – use as a mandatory EU tool to prevent data loss.

4. **Access rules with judicial control** – in cases of particularly serious interference, access only with the permission of a court or an independent authority, for less important data, the acceptance of a prosecutor is sufficient.

5. **Uniform procedural standards at EU level** (as in the e-Evidence Regulation): standardized requests, deadlines, secure channels, audit mechanisms.

6. **National security as an area of exception –** provide for general undifferentiated retention only as an exception, leaving it to the discretion of the Member States, with the obligation to ensure independent control and temporary nature.

7. **Transparency and public trust** – wherever possible, foresee that a person may subsequently learn about the use of data; strengthen monitoring mechanisms.

The initiative to create a single, harmonized European Union data retention framework, which would be in line with the case law of the Court of Justice of the European Union, is supported; restrictions on the fundamental rights of individuals should be carried out in accordance with the principle of proportionality.

Experience so far shows that the development of national frameworks has not been sufficiently successful, placing law enforcement authorities of the European Union Member States in unequal situations with regard to the available tools for performing their tasks, and similarly placing data subjects of the European Union in unequal situations with regard to the extent of the restriction of their right to the protection of personal data.

HUNGARY

1) **Scope of service providers: Do you consider that OTTs (over-the-top services) should be required to retain traffic data?**

We think, that OTT's should retain traffic data. In our opinion platform neutrality should be a top priority.

Overall, stored data is irreplacable in relation to criminal proceedings. With relevant data, investigators can get a clear picture about criminal offences. It is important to emphasize, that evidence is not always incriminating, in many cases it can lead to an acquittal. Because of this, it is appropriate to provide for new rules which include general data retention and which are accepted by the European Court of Justice.

We consider it appropriate to enforce fundamental rights aspects not by excluding general retention, but by limiting it to data which is strictly necessary, by limiting the duration to what is strictly necessary, and by limiting access. We are aware of that the court excludes general data retention, but from the legislative side it has to be assumed that it is necessary on a professional basis.

a. Which service providers and which services or data held by these service providers would you consider to be particularly relevant for criminal investigations?

All service providers should be covered, which provides a communication service, be it a telecommunications or other commercial service provider. The new rules should cover traffic and location data.

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?

We think, that the scope of the new data retention rules in relation to service providers should be the same as the scope of the e-Evidence Regulation.

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?

In our opinion, the possibility to impose a general and indiscriminate data retention obligation on telecommunication providers is the base of the criminal proceedings in relation to missing persons.

In these cases, the protection of human life is the most fundamental aspect, life is the source and condition of all other fundamental rights, thus preservation can be justified. Both the disappearance of persons and the commission of crimes are known to the authorities afterwards, in which case the most important thing is where and under what circumstances the missing person's phone last communicated. Lives can be saved if there is data retention in these cases.

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?**

In our opinion, a targeted/limited retention regime isn't sufficient to investigate serious crimes. A targeted/limited retention regime can affect the effectiveness of criminal investigations.

In the case of targeted data retention, it should be circumscribed to whom it is applied. If it is used against suspects, it does not provide a solution for first time criminal offenders, only for repeat offenders. All other aspects raise the issue of discrimination. For example, in the case of convicts who are deemed to have no criminal record. Equality of rights can only be ensured by general data retention.

a. **What are its benefits and shortcomings?**

We think, that the benefit of a targeted/limited retention regime is, that it will be possible to investigate all types of criminal offences. However, as we mentioned above, general data retention should be introduced.
We think, that a targeted/limited retention regime can lead to discrimination, and most of the affected perpetrators won't be covered (for example first time offenders, foreign perpetrators with a migration background, terrorists with no history in the country).

b. **Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?**

We think, that in relation to general data retention, a time limit can be introduced. The other possibility is the introduction of a limit of scope. A system that is not disproportionate can be established by the time limit and the limitation of the amount of data that can be retained.

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?**

We think, that quick freeze can have an added value, but only in case of general data retention. It is capable of compensating for a shorter overall retention period and therefore relevant data won't be deleted. Quick freeze can be very effective. As a similar measure, the acquisition of surveillance camera footage before it is deleted, can be mentioned.

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?**

In Hungary, general data retention is allowed for law enforcement purposes. By our experience, data stored for marketing and billing services isn't enough to conduct successful criminal investigations. In case of unlimited phone calls and prepaid services the system could be circumvented. Perpetrators will find regulatory gaps and the system will then be unable to detect well-prepared organised criminals.

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?**

In case of general data retention, one year should be the maximum period for retention. The length of investigations should be examined, and the retention periods should be defined according to this.

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?**

It is appropriate to create rules which do not exclude the possibility for Member States to provide general data retention. However, general data retention rules should be introduced within a reasonable framework.

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?

We think, that he overall duration of investigations should be examined. Any unnecessary narrowing of data retention periods will result in data loss. However, from a fundamental rights point of view, it is not possible to set an unlimited data retention period. In our opinion, it is not possible to define specific boundaries, but only to draw attention to a general context.

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?

We can support a range within which Member States can set shorter or longer retention periods in a flexible way.

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?

In our opinion availability of communication data is particularly relevant in relation to serious crimes, and in case of criminal offences, where a European Arrest Warrant can be issued.

a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?

We think, that this can't be determined exactly. In relation to crimes committed in the digital space, but also in the physical space, investigations can be affected by the lack of traffic and location data. The Dwyer case is an axample of this.

b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

We think, that the scope should cover not just cyber enabled and dependent crimes, but all other types of serious crimes as well.

6) Access rules and conditions: To what extent should EU law regulate access conditions for data subject to EU retention obligations?

In our view, it is necessary that access to the data concerned to be subject to authorisation by a judicial authority. This is essential to avoid the possibility of profiling.

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)?**

We can support the necessary level of access. In our opinion, fundamental rights considerations can be enforced here.

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?**

We can support the introduction of other requirements, which are similar to the requirements in the e-Evidence Regulation.

AUSTRIA

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?

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?

Do you miss the possibility to impose a general and indiscriminate data retention obligation on telecommunications providers in order to locate missing persons, whose location is unknown to the authorities?

Ad 1:

AT would like to thank the Danish Presidency for their balanced presentation of the CJEU case law. Naturally, this case law has not yet been extended to OTT services due to a lack of legal basis.

Nevertheless, AT does not consider the range of providers to be problematic, and believes that a discussion on the transferability of the CJEU's data retention approaches to OTT services is potentially feasible. As with traditional telecommunications providers, an exception to the confidentiality of communications at EU level could be considered for OTT services.

However, from AT's perspective, the decisive issue is the practical availability of traffic and location data. These data are generated in any case by traditional telecommunications providers for connection establishment, network operation and billing, and established data inventories and processes already exist. The situation is different with OTT services: Many services store little or no data by default because it is not required for the service (privacy by design). A blanket storage obligation would therefore often necessitate the introduction of new data collection and storage processes. From AT's point of view, this raises questions of necessity and proportionality.

The rationale behind data retention has been to access traffic and location data that actually exists and are required for service operation. The idea has been to use 'ordinary' data that providers need for their operations. However, if there is no operational need for storage in the case of OTT services, further questions arise: Who would bear the costs of infrastructure and processes to build, store and make available standardised data inventories similar to those of traditional providers?

From AT's perspective, a robust technical impact assessment by the Commission is required in any case, including with regard to OTT architectures, as well as international coordination.The effectiveness of the e-Evidence Regulation, which already covers OTT services, must also be considered. AT does not currently have a final political position on data retention in general.

Ad 1a:

Particularly important for criminal investigations are:

- Communication services such as messenger services (WhatsApp, Signal, Telegram, Threema, Wickr, Viber, WeChat), VoIP providers (Skype, Zoom), social networks with messaging functions (Facebook, Instagram, X/Twitter, Snapchat, YouTube, TikTok)
- Cloud services (e.g. Dropbox, Google Drive, iCloud)
- E-commerce and payment services such as PayPal, Amazon, online banking
- Domain and hosting services: domain registrars, DNS providers, web hosting companies
- Online platforms such as marketplaces, forums, or darknet-like structures
- Taxi and food delivery services (e.g. About, Lieferando)
- Gaming platforms (e.g. Steam, PlayStation, Discord)

Ad 1b:

From AT's perspective, the question is too narrow as it does not address an essential aspect: AT believes that the first priority should be to clarify how to deal with service providers that are not covered by the e-Evidence Regulation. It is precisely in this area that delays currently arise, as investigative authorities can only obtain data via the lengthy process of mutual legal assistance by which time the data has often already been deleted. This directly affects traditional telecommunications providers established in only one Member State.

Only in a second step should it be considered whether additional retention obligations would also be appropriate for providers already covered by the e-Evidence package, and to what extent.

Ad 1c:

From AT's perspective, this question cannot be answered in general terms. In practice, it usually becomes clear relatively quickly whether a person is genuinely missing or has absconded. In such cases, it is possible to access data held by telecommunications providers (in Austria, for example, this is possible because the data are stored for billing purposes). However, if the relevant circumstances only become known much later and the data is no longer retained by that point, naturally a gap arises. The same would apply under a general data retention regime once the prescribed retention period has expired.

It should be noted in general that AT has involved practitioners in the Commission's impact assessment. In the Commission's questionnaire, practitioners highlighted that existing investigative tools are insufficient. At the same time, however, this assessment was only partially shared, insofar as the absence of digital evidence was said to prevent investigations altogether.

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 competitors?

b. Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?

In principle, a targeted data retention regime (based on geographical criteria, for example) can be an effective tool for investigating and combating serious crime. This approach aligns with that of the CJEU, who have ruled that retention and access are permissible only under strict and differentiated conditions. However, such criteria are demanding: their technical feasibility must be ensured in practice, and geographical risk areas are dynamic and require regular review. Therefore, whether and how such a limited data retention regime can be designed in a legally robust and operationally useful way remains an open question.

From AT's perspective, the question is also slightly misleading because targeted data retention does not necessarily have to be limited to 'serious crime'. Under CJEU case law, the decisive factor is the seriousness of the interference, particularly whether the data can be used to draw insights into an individual's private life. The CJEU has emphasised that differentiation by data category can be meaningful since not all data are equally intrusive. It has repeatedly referred to the 'quality' of data: identity data are considered less sensitive, whereas IP addresses are more sensitive as they allow inferences about user behaviour. However, if IP addresses are technically separated in a 'watertight' way from other traffic data, the level of intrusiveness may decrease. The CJEU suggests a step-by-step process for this: by using technical measures, a serious interference can be reduced – without having to meet the "serious crime" criterion. It is vital that this logic and balancing process is examined for other data categories too. For this purpose, a legal and technical impact assessment by the Commission is required.

For AT, the concept of 'serious crime' is particularly important in this balancing exercise. The current linkage – serious interference only permissible for the prosecution of serious crime – originates in the now annulled Directive 2006/24/EC. The CJEU has upheld this principle in subsequent case law. CJEU Judge *von Danwitz* expressly emphasised this during a hearing.

Therefore, this equation and balancing did not originate with the CJEU, but with the EU legislator. AT therefore recognises the risk that a future legal act could define the term 'serious crime' independently (and potentially more narrowly or broadly), even though the CJEU has not yet developed an autonomous definition in the absence of a valid legal act. The discussion on 'seriousness', both of the interference and of the criminal offences, must therefore be conducted carefully. National competences must not be undermined.

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 telecommunications providers are, in any case, storing for marketing and billing services? Is this data enough for them to successfully conduct their investigations?

The quick-freeze model has been legally established in Austria. In practice, it is considered a useful and viable tool because it enables specific data to be preserved before it is deleted by telecommunications providers. Statistically, however, the model plays little role in practice because, in most cases, data are accessed directly without the intermediate step of quick-freeze, namely the data that providers store for three months on their own initiative (see answer below).

With regard to extending this model to OTT services, the answer to question 1 should generally be referenced.

Ad 3a:

Law enforcement authorities can only access data that telecommunications providers are already storing for billing purposes. These data can generally be retained for up to three months. As part of their duty to cooperate, providers are authorised and obliged to provide these data. The retention period is therefore limited and the available data may be incomplete. Investigative authorities regularly make use of these data, when legally permissible, to help identify and investigate crimes. IP address allocations and cell site data are particularly crucial for investigating cybercrime, terrorism and serious crimes. In many cases, existing billing and traffic data can successfully support investigations (e.g. identification of perpetrators via IP addresses and reconstruction of communication links).

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?

It It should be emphasised again that AT does not have a final political position on data retention. Therefore, we do not make any positive or negative determination. The decisive factor is that retention periods must be strictly necessary, proportionate and purpose-bound, in line with CJEU case law. As reported to the Commission during the impact assessment, practitioners in AT consider a retention period of 6–12 months to be necessary for combatting crimes such as smuggling, human trafficking and organised and cyber crime.

Austria wishes to stress that the national competences of Member States must not be undermined. This applies to the definition of 'serious crime' and to national security.

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?

Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

From AT's perspective, the Commission should consolidate the feedback it has received from practitioners and other Member States in the course of the impact assessment, and present the results of this assessment. AT believes that discussing specific offences is premature, given that it is not yet clear which group of providers (e.g. OTT services) would be subject to retention obligations.

Nevertheless, AT wishes to emphasise the following, which it considers essential: traffic and location data are particularly relevant when an offence leaves few traces other than such data and when there is otherwise a risk of systemic impunity due to a lack of alternative leads (e.g. offences committed exclusively in the virtual space), an approach recognised by the CJEU (e.g. in cases of child pornography). Against this background, AT rejects offence catalogues, as they would imply an EU-wide definition of 'serious crime' in practice and thus interfere with national competences.

Instead, what should be decisive are the specific purpose of the investigation, the degree of interference depending on the data category, and strict, differentiated safeguards. A list of all possible offences is not enough because of the way criminal behaviour changes over time and the fact that there may be other evidence available. This other evidence will determine whether data are needed and, if so, how much.

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 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?

From AT's perspective, it must be emphasised that access rules for data retained in advance must necessarily comply with the requirements already established by the CJEU. These requirements are based on fundamental rights considerations. First and foremost, this means prior judicial authorisation.

Exceptions are only justifiable where the interference is typically minor, such as identity data or, as recognised by the CJEU, IP addresses. From AT's perspective, the quick-freeze model has also proven effective, involving freezing on the order of the prosecution authority and granting access to data only in a second step with judicial approval. This ensures efficient law enforcement. Comparable exceptions may be justified, and discussions on this possibility can also take place.

Questions of the admissibility of evidence should remain within the national competence of the Member States, in line with the CJEU's existing case law. Any change in this area would be clearly unacceptable.

Ad 6b:

The intention of the question is not entirely clear to AT and would require further clarification. From AT's perspective, the e-Evidence Regulation only standardises to a limited extent. The technical design of formats, for example, should in any case remain within the competence of the Member States. Processes in AT were already harmonised with the first implementation of data retention, so changes to the syntax/semantics of data transmission would incur significant costs and strain the budget.

POLAND

General comments

The absence of a common legal framework at EU level, combined with the existing case-law of the CJEU, poses significant challenges both for the Member States and for the Union as a whole. On the one hand, it is essential to respect the CJEU's jurisprudence, in particular regarding the interpretation of the Charter of Fundamental Rights with respect to data retention and access to data; on the other hand, it remains necessary to ensure that law enforcement authorities are equipped with effective and adequate tools to carry out their tasks.

Difficulties in cooperation between national authorities are already evident due to the differences between national legal frameworks. Poland expresses the hope that, through joint efforts, it will be possible to develop an effective solution capable of addressing current challenges and operational needs.

Poland favours an approach that provides for the broadest possible data retention regime, differentiated according to the type of data retained and combined with a justified and sufficiently long retention period. Such a system should be complemented by an access mechanism for law enforcement authorities fully compliant with the case-law of the CJEU, ensuring oversight by independent bodies or judicial authorities.

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?

Poland considers that Over-the-Top (OTT) services should be brought within the scope of future EU rules on data retention, in order to ensure the availability of selected categories of traffic and user identification data to the extent necessary for the effective investigation and prosecution of serious crime, in particular terrorism, cybercrime, child sexual exploitation and trafficking in human beings.

In recent years, electronic communication has increasingly shifted from traditional telephony to internet-based messaging services and encrypted communication applications. The absence of retention obligations for OTT service providers has created significant evidentiary gaps, which in practice hinder law enforcement authorities in identifying perpetrators, tracing criminal networks and preventing serious offences.

From the perspective of criminal investigations, the following categories of OTT service providers should be regarded as particularly relevant:

– encrypted internet messengers (such as WhatsApp, Signal, Telegram, Viber);

– social media platforms (Facebook, Instagram, TikTok, X – formerly Twitter);

– VoIP and videoconferencing applications (Skype, Zoom, Teams);

– and electronic mail services (Gmail, Outlook, ProtonMail and others).

In addition to the services already covered under the e-Evidence Regulation, other types of service providers may also prove essential for the effective prosecution of crime. These include domain name registries and hosting service providers; e-commerce and financial platforms (Amazon, Allegro, OLX, PayPal, Revolut and others); as well as cloud storage services (Dropbox, Google Drive, iCloud and others).

It is recognised that the introduction of such data retention obligations reflects primarily the operational needs of law enforcement and judicial authorities and may not be easily achievable within future legislative frameworks. Nevertheless, this issue deserves thorough consideration in the context of ongoing discussions.

For these categories of providers, retention obligations should be strictly limited to basic identification data and IP addresses, accompanied by the relevant date, time (including time zone) and source port number.

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?

Poland considers that a data retention system based solely on personal or geographical criteria does not constitute an effective tool for law enforcement authorities in combating serious crime. While such an approach safeguards the right to privacy and remains consistent with the case-law of the CJEU in this regard, it simultaneously weakens the operational capabilities and overall effectiveness of law enforcement.

It should be recognised that there are exceptional circumstances and certain categories of serious crime that may require a broader data retention regime, provided that such a regime is duly justified. In such cases, attention should be focused on introducing additional safeguards and requirements governing access to retained data by law enforcement authorities in order to protect fundamental rights, rather than on restricting the data retention framework itself.

Alternatively, consideration could be given to the introduction of a targeted retention regime based on the type or category of data that is most intrusive to fundamental rights, while allowing for certain exemptions, for instance depending on the type of crime involved, such as terrorism or trafficking in human beings.

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?

Poland considers that the possibility to issue expedited data preservation ("quick freeze") orders in specific circumstances may constitute a significant added value. Such a mechanism should remain exceptional in nature and serve as a complementary measure to the general data retention regime. It could provide a key operational tool for law enforcement authorities in urgent situations, such as kidnappings, offences against children, acts of terrorism, and serious threats to national security.

Polish law enforcement authorities make limited use of marketing and billing data. These data have only limited evidential value and may prove useful solely in certain categories of offences, such as online or credit fraud. However, they are insufficient to enable the effective investigation and prosecution of all types of serious crime.

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?

Poland remains sceptical about the inclusion, in future EU legislation, of a data retention mechanism for the purpose of safeguarding national security, as such matters should remain within the competence of the Member States. However, should such a proposal be introduced, it should allow for the possibility of extending the retention period up to 24 months, leaving this decision to the discretion of national authorities. In order to ensure compliance with the case-law of the CJEU, such decisions should be duly justified and subject to judicial oversight with regard to access to the retained data.

For all other situations, Poland supports the introduction of a uniform and fixed data retention period for criminal justice purposes across the European Union, set at a minimum of 12 months. A harmonised retention period would undoubtedly facilitate cross-border cooperation, establish common standards throughout the internal market without affecting the competitiveness of service providers from different Member States, and enhance the overall effectiveness of law enforcement responses.

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?

Poland supports the development of the broadest possible catalogue of offences for which the collection of data is indispensable. The list annexed to Article 12(1)(d) of the e-Evidence Regulation could serve as a basis for its establishment.

The categories of offences where the unavailability of traffic and location data may lead to systemic impunity include: terrorism and threats to national security, organised crime, kidnappings and disappearances, offences against life and health, cybercrime, online sexual offences, and serious economic and financial crimes.

With regard to cybercrime, this should encompass: strict cyber-dependent offences (such as ransomware or DDoS attacks), hybrid crimes (including human trafficking, terrorism, and organised crime), as well as exceptional life-saving situations (such as child abductions, missing persons, or rescue operations).

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?

Poland considers that the forthcoming EU legal framework should be based on the access standards established by the CJEU, while at the same time allowing for certain exceptional circumstances to be duly taken into account. The case-law of the CJEU cannot be disregarded; however, it should be recalled that the Court's judgments were rendered in specific factual contexts. The interpretation of the Charter of Fundamental Rights presented therein is, in principle, of a universal nature, yet it should be possible to reconcile it with the operational needs related to combating serious crime.

The main objective of the CJEU is to protect citizens' privacy against uncontrolled interference by law enforcement authorities. Therefore, a rigid and literal application of those requirements would not be an optimal solution. Instead, the principle of proportionality should remain the guiding criterion when assessing measures related to data access. At the same time, there must be appropriate mechanisms ensuring oversight of such measures by independent bodies or judicial authorities in order to guarantee the full protection of fundamental rights.

The forthcoming legislative proposal could draw upon the standards and mechanisms established under the e-Evidence Regulation, while ensuring their proper adaptation to the specific context of data retention and access for law enforcement purposes.

PORTUGAL

I – General remarks

The relevance and complexity of the issues associated with data retention in the context of criminal investigations are well known to Portugal, which has consistently advocated for a balanced approach that ensures both the effectiveness of law enforcement and the protection of fundamental rights. Access to communications data is now essential for the prevention and investigation of serious and organized crimes – such as terrorism, human trafficking, child sexual abuse, or kidnapping – as well as less serious offences committed through digital means.

However, such access must always take place in full compliance with the principles of necessity, proportionality, and legality, under effective judicial supervision.

Portugal has therefore reiterated its support for the establishment of a common legal framework in the field of data retention and access, based on harmonised rules that ensure legal certainty and prevent the current legislative fragmentation among Member States.

In this regard, we support the adoption, at European Union level of a legislative solution that balances the imperative of public security with the safeguards inherent in the protection of privacy and personal data, in accordance with the Charter of Fundamental Rights of the European Union and the case-law of the Court of Justice of the European Union (CJEU). Any such initiative must reflect the lessons learned from past experience, particularly those that led to the annulment of Directive 2006/24/EC, ensuring that measures in this area are accompanied by robust safeguards against unlawful access and misuse.

Finally, we deem it essential to recall that any legislative development in this field must be based on a thorough impact assessment and a sound legal basis, framed within judicial cooperation in criminal matters and discussed in COPEN, which we consider to be the appropriate forum.

II. Questions posed by the Presidency

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?***

Over-the-top (OTT) service providers should be encompassed within future data retention rules, as they currently account for the majority of electronic communications. It is worth noting that, for commercial, quality assurance, and security purposes, they are already subject to obligations to retain metadata related to their business operations. In this regard, we consider that metadata associated with communications should also explicitly include the so-called "source port" of the communication IP addresses.

It is likewise deemed essential to ensure expeditious responses in cases of missing persons, by enabling prompt access to relevant data. Even in cases where a disappearance shows no indication of criminal relevance, it is essential to establish a legal framework allowing access to metadata, which necessarily presupposes its prior retention. Without this, the practical effectiveness of the measure would be undermined. However, once it has been determined that the disappearance does not involve a criminal element, the justification for access ceases, and the subsequent exercise of the "right to be forgotten" must be duly safeguarded.

In any case, such procedures must comply with the limitations established under European Union law, as interpreted by the case-law of the Court of Justice, which requires that any data retention regime be based on objective criteria, be limited in duration, and be subject to rigorous oversight and supervisory mechanisms.

For example, in Portugal, it has been observed that certain electronic communications operators have, by analogy, enabled access to data on the basis of precautionary measures provided for in the Code of Criminal Procedure, under the associated safeguards, notably the simultaneous notification of the competent judicial authority.

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?***

We understand that any solution involving non-indiscriminate data retention inevitably raises the issue of the technical difficulties in implementing the intended measures.

Non-indiscriminate data retention based on a distinction between categories of data appears to be the most feasible approach, provided that the most intrusive data (such as location data) are always retained, even if for shorter periods than those applied to less intrusive data, such as IP addresses (including dynamic IPs), and that access criteria are likewise defined according to the degree of intrusiveness.

A data retention solution based on geographic criteria versus crime rates could be feasible, if the technical implementation challenges are overcome and provided that minimum retention periods are, in any case, guaranteed in all regions, including those with the lowest crime rates.

The establishment of *a priori* retention criteria based on personal characteristics appears highly questionable from a constitutional standpoint when applied to generic categories of persons. We must also mention that even where data retention is envisaged on the basis of individuals' biographical records, such a measure is not technically feasible, and any approach of this kind would, in practice, amount to *data interception* rather than *data retention per se*.

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?***

Portugal has an expedited data preservation regime resulting from the transposition of the European Directive and the Budapest Convention. This regime allows for renewable expedited preservation for periods of three months up to one year, always under the supervision of the competent judicial authority.

The preservation regime presupposes the prior retention of data, which in the Portuguese context, for commercial purposes, amounts to six months.

Portugal acknowledges the need for legislation on the retention of, and access to, communication metadata for the purposes of criminal investigations. This is because the practical application of the expedited data preservation mechanism, when limited to a six-month period, has in many cases proven to be insufficient.

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?***

In our opinion, matters of national security should not be covered by EU-wide rules on data retention.

Outside the scope of national security, retention periods should be differentiated according to the degree of intrusiveness of the data in question. So, in ascending order of intrusiveness, this includes civil identification data, communication IP addresses, traffic data, and location data. IP data should be available for any criminal investigation relying on digital evidence for a period of one year. Other categories of data should be retained for the investigation of serious crimes for a minimum period, which may be adjusted downward, for instance to six months, taking into account their relevance and the degree of intrusiveness.

More serious criminal phenomena, such as criminal organizations that, by virtue of their structure, scale, and *modus operandi*, threaten the sovereignty and security of Member States, require a differentiated approach, particularly in States more directly confronted with such realities.

The definition of minimum and maximum retention periods would better accommodate the different national circumstances, provided that a common minimum is established. Setting a fixed period applicable to all jurisdictions has the advantage of facilitating assessment against the case-law of the Court of Justice of the EU.

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?***

Crimes that involve the use of information systems, or whose execution depends on such systems and which could not be effectively investigated without access to traffic and location data, should definitely be considered. Similarly, crimes for which investigation or proof relies on communication data, even when assessed according to a severity criterion, must also be included.

In defining the types of crimes to be included, it is necessary to take into account that the perception of impunity depends not only on the seriousness of crimes whose prosecution may be affected by the lack of access to communication metadata, but also on the sense of inevitable failure in prosecuting crimes that rely on such data, thereby contributing to the "dark figure" of unreported crimes and the development of alternative compensatory mechanisms.

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?***

In our view, the protection of fundamental rights in matters relating to communications necessarily entails the effective and enforceable respect of fundamental safeguards at the initial stage of interference represented by the data retention, As such, it should focus primarily on the regime governing access to metadata for the purposes of criminal investigation.

In fact, all criminal investigations, and particularly the use of more intrusive investigative tools, must, in light of the existing European legislative and case-law framework, be subject to oversight and guidance by a competent authority to assess the necessity, adequacy, and proportionality of such intrusive measures, namely judicial authorities or independent bodies. Such oversight should apply

especially to the most intrusive metadata, as categorized above. From this standpoint, in our opinion, civil identification data and communication-specific IP addresses should be considered less intrusive, as is already the case in Portugal (IP addresses of a specific communication may be requested by the Public Prosecutor; IP addresses covering a communication period must be requested by a judge).

Looking forward, and taking into account the existing legislative, jurisprudential, and operational context, as well as the fact that legal certainty underpins European judicial cooperation in criminal matters, we consider that any new proposal should aim at establishing a coherent and harmonized framework, while eventually allowing more operational issues to be addressed through separate, more targeted legislative instruments.

SPAIN

Following indications of the Chair in the COPEN meeting last 25 September, hereby we provide inputs for questions 3 to 6 and only for these questions, since the position to question 1 and 2 was expressed during the meeting.

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?

Quick freeze is currently available. Once a crime is reported, quick freeze can be requested only if the provider has that information stored in that moment in time. If there are no generic data retention obligations, crimes such as murder won't be investigated since it took place at a specific moment in time and data might not be available anymore.

Even though service providers may have that information stored because of their profit interests for some days, there are a great number of delays that prevent investigators to contact the provider in time. First of all, there is a delay in reporting crimes. Secondly, investigators must gather evidence that could lead to requesting data to providers. This second step is necessary not only to get the valid identifiers that may be of interest, but also to analyze the proportionality of this measure in order not to make broad quick freeze requests that may not be necessary. This meaning that quick freeze indeed is useful but cannot be considered as a viable alternative to the establishment of a data retention regime for which we strongly strive.

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?

Since we have data retention obligations in place, we do not access that information. We know they might store that information for those purposes only for a month. That only comprises 11,83% of the requests made by our investigators. You may find the average time slot between date of request and first data requested for traffic & location data in the following table:

Days	*Requests*	*Accumulated requests' %*
0	308	0,49%
0-30	7088	11,83%
30-60	7598	23,97%
60-90	7508	35,98%
90-120	6251	45,97%
120-150	4639	53,39%
150-180	4461	60,53%
180-210	3414	65,98%
210-240	2491	69,97%
240-270	2288	73,63%
270-300	2394	77,45%
300-330	2402	81,29%
330-360	2051	84,57%
360-390	2964	89,31%
+390	6684	100,00%

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?

It should be noted that various studies indicate that the majority of requests for telecommunications-related data in the context of criminal investigations refer to data generated within the past year. It seems evident that the shorter the periods for storing traffic data, the lower the risk of being able to illegally establish a complete profile of the individuals affected, and therefore, the lower the abstract intensity of the interference with fundamental rights. However, retention periods cannot be so short that they render data retention practically ineffective.

One year is the period we consider adequate, striking a balanced assessment between the conflicting interests. Taking into consideration the data provided in the aforementioned table that reflects current reality in a country with a data retention regime, there is a need for a 1-year retention period for non-content retained data associated to communications. There are always cases that reach the year of time lapse. Not retaining data for a year would mean leaving some cases without the possibility of investigation.

Dataset requested are narrow in time range for traffic data and location data. Comparing that information with the time slot between when the request was made, and when the communication of interest was made, it is easy to see that investigators, prosecutors and judges do not request more information that the one they need.

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?

It must cover general and indiscriminate data retention in terms of national security in order to enable it. However, there must be room for national legal developments on every matter with regards to national security.

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?

The judgment of the CJEU of October 2020 expressly acknowledges the possibility of legislative measures mandating the general retention of two categories of data deemed to entail a lower degree of interference with fundamental rights: source IP addresses and civil identity data. This interpretation has subsequently been reaffirmed in later rulings.

The principal concern, therefore, lies with traffic and location data, which are the focus of the CJEU's restrictive jurisprudence.

We consider that the debate surrounding differentiated retention periods based on the nature of the data is both appropriate and necessary. To that end, it is essential to assess the degree of interference with fundamental rights: data relating to communication processes cannot be equated with data generated from accessing online content such as digital newspapers.

Directive 2006/24/EC established a retention period of no less than six months and no more than two years. A reasonable—and arguably optimistic—standard would be a one-year retention period. However, in accordance with the principle of proportionality, it would be legitimate to consider differentiated retention periods depending on the category of data and its corresponding level of intrusiveness.

We do not endorse the criterion of "relevance for criminal investigations" as a basis for determining retention periods, given that all categories of data under consideration may be relevant depending on the specific circumstances of each case. Consequently, we reject this criterion as insufficiently precise and with implementing difficulties.

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?

Ideally, the more homogeneous the system is across the EU, the better for an efficient judicial cooperation. However, those rules must take into consideration differences between countries or providers.

It should be borne in mind that not all providers are in the same condition to comply with retention obligations due to their dimension and financial resources. Small entities may not have the budget or the technical capability to establish maybe the higher data retention period, so consideration could be given to these differences.

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?

All of them. As stated by EUROPOL, more than 85% of crimes require digital evidence.

a. Which are the crimes where the lack of traffic and location data bears the risk of systemic impunity?

Mainly crimes that only take place in a single act. For crimes that take place over the course of an extended period of time, investigators are more likely to resort to other type of evidence. For instance, for crimes such as murder –but not restricted to –if there is no traffic data of the moment in time when it took place, there will not be any thread that investigators can pull in order to gather any evidence.

This question is linked to the relevance of electronic evidence in the context of the specific case. There are crimes that rely almost exclusively on traffic and location data as evidence. Therefore, the risk of impunity is connected to this element. When the main instrument has been the use of electronic tools, the lack of information about that instrument creates greater difficulties in the investigation. When the investigators has other tools at its disposal, the issue is different. The distinction lies between crimes committed through electronic means and crimes facilitated by electronic means. We cannot not provide a list in this regard.

b. Would this include all cyber enabled and dependent crimes or only some or other crimes as well?

For all of them. For cyber enabled crimes what need to be defined is a technologically neutral regulation. This way, current information needed for investigations on the Internet such as port numbers would be included, but the future new information that may be necessary can be included as well. However, IP addresses assignments by themselves are not enough for investigating cyber enabled crimes.

6) Access rules and conditions: To what extent should EU law regulate access conditions for data subject to EU retention obligations?

To the maximum extent possible. Generic data retention must be in place since data need to exist if it is ever going to be accessed. There must be a great focus on the way investigators lawfully access it so that we can ensure that no authority access information without the needed preconditions being met.

We believe that the element of access is absolutely fundamental. This is perhaps the reason why our law has been able to endure: due to the large number of safeguards it includes.

Safeguards:

- ✓ The application of guiding principles for access to this type of data, which seriously interferes with fundamental rights: necessity, proportionality, adequacy, ultima ratio, suitability, and specificity, which our Criminal Procedural Law foresees for any technological investigation measure.
- ✓ Limitation to a specific set of criminal offenses.
- ✓ Judicial authorization: with absolute precision regarding the individuals who may access the data—this is one of the aspects the Court of Justice has focused on.
- ✓ Strict guarantees in data sharing.
- ✓ Criteria for data sharing: limited to serious crimes, included in a predefined list, including cybercrime, and other offenses referenced by a penalty threshold—this also passes the Court's scrutiny.
- ✓ Level of data protection and security: data must not be processed for purposes other than those for which it was collected.

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)?

Yes. These requests should only be made for serious offences. Moreover, if we want data retention regime to be more restricted, sets of information that could be requested depending on specific offences could be established.

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?

Yes. ETSI standards should be implemented as much as possible in order to improve the efficiency of the disclosure of the information. Moreover, they serve as a layer of protection for providers, since they would know exactly what they need to do, and they would have been the ones creating those standards in order to fit their technical needs.

SLOVENIA

For the purposes of further discussions on the "Future Rules on Data Retention in the European Union", the Republic of Slovenia hereby submits its response, which reflects the positions provided by the competent national authorities and is without prejudice to the official position of Slovenia with regard to possible future proposals

1. Scope of service providers

We consider that providers of OTT services, such as social media platforms, instant messaging applications, virtual private network (VPN) providers, and virtual private server (VPS) providers, should also be subject to mandatory traffic data retention obligations. Given that many of these providers offer electronic communications services, or are used by users of such services (e.g., the VPN service), and considering the widespread use of such platforms and services in the commission of criminal offences, their inclusion is essential to ensure effective law enforcement. These entities frequently store key traffic data (e.g. IP addresses, login timestamps), which are crucial for identifying the users and thus for the effective investigation and prosecution of criminal offences.

a) For the purposes of criminal investigations, we deem it necessary to also include services that enable the dissemination and exchange of video and audio content. Due to the nature of these services, they may be used for the commission of serious crimes. Access to traffic data related to users who publish, share, or access such content is indispensable for identifying perpetrators of the most serious offences, such as terrorism and child sexual abuse material.

b) In light of the e-evidence legislative package, it is logical and coherent that all service providers falling within the scope of the e-evidence Regulation should also be subject to harmonised data retention obligations. This is the only way to ensure the practical implementation of the Regulation and to avoid legal and operational inconsistencies.

c) We support the possibility of general and non-targeted data retention in strictly defined cases, such as search and rescue operations for missing persons or situations involving the protection of life and physical integrity. In such cases, the principle of proportionality is inherently fulfilled, given the urgency and gravity of the circumstances.

2. Regime for retaining traffic and location data

It is challenging to unequivocally assert that targeted data retention, on its own, constitutes a sufficient instrument for the investigation and prosecution of serious criminal offences. Traffic and subscriber data must be assessed in conjunction with other types of evidence throughout the criminal procedure.

The adequacy of targeted retention is therefore context-dependent and varies significantly depending on the nature and complexity of the offence. We assess that targeted retention alone is insufficient for the effective investigation and prosecution of serious crime, as it is impossible to predefine all criteria that would adequately reflect the evolving nature of criminal behaviour and the continuous emergence of new modi operandi, particularly in light of technological advancements, and circumvention attempts.

a) The main shortcomings lie in the rapid adaptability of modern criminal activity, the frequent switching of platforms and jurisdictions, and the inability to anticipate all relevant data categories due to technological developments. Another risk is the loss of critical data resulting from overly narrow retention scopes. On the other hand, a clear and specific regulatory framework can help limit the interference with the right to privacy.

b) We consider it reasonable to differentiate retention periods based on the category of data. Data that are essential for identification and prosecution (e.g. subscriber data) should be retained for longer periods, while data that entail a greater interference with the confidentiality of communications (relevant types of traffic data) could be subject to shorter retention periods. We do not support limiting retention obligations based on the type of service provider, as this would undermine the coherency of the framework and the objective of criminal investigations. The decisive factor should be the type of data available, not the type of the provider, since different providers may store or have access to similar types of data.

3. Expedited preservation orders

The instrument of expedited preservation represents a significant added value, as it enables the preservation of data held by electronic communications service providers that would otherwise be deleted in accordance with standard retention periods, before a judicial production order could be issued.

a) In Slovenia, law enforcement authorities may only access data that providers retain for commercial and operational purposes. When traffic data are obtained, authorities acquire only those data that are strictly necessary for the detection and prosecution of criminal offences. However, the limited scope of retained data poses a challenge: a broader dataset would undoubtedly facilitate prosecution and, more importantly, enable the detection of criminal activity.

The retention period is particularly problematic. As a general rule, providers retain data for business purposes for approximately three months, while other types of data are retained for varying durations or not at all. Traffic data retained by service providers for commercial purposes often do not include all types of data that would allow successful criminal investigations, and the scope and duration for which the data are retained vary significantly between providers. As criminal activity, especially serious and organised crime, increasingly shifts to digital environments, traffic data are becoming ever more crucial. Without a broader and consistent set of retained data, which can be preserved and subsequently obtained, effective pre-trial procedures are likely to be significantly hindered or rendered almost impossible in the future.

4. Retention periods

We are of the view that data retention periods should be directly proportional to the gravity of the criminal offence, and in fact exponentially so, precisely due to the complexity of investigations, which often require extended timeframes before competent authorities can access key electronic evidence.

Retention periods should be harmonised across EU Member States to ensure the effectiveness of cross-border criminal investigations and judicial cooperation in criminal matters as well as to provide a level playing field for service providers. For instance, as presented during one of the European Judicial Network (EJN) meetings, Italy allows access to retained data up to 72 months in cases involving terrorism, organised crime, and other serious offences. In contrast, retention periods in other Member States, including Slovenia, are significantly more restrictive.

This disparity may result in situations where the involvement of a single Member State, through which perpetrators operate in the digital environment, can obstruct further investigation, potentially creating safe havens for the commission of certain offences.

In this regard, we support the establishment of a uniform EU framework, at least to define minimum retention requirements, as a necessary measure to ensure the effective investigation and prosecution of the most serious criminal offences. Based on practical experience in prosecuting offences that pose a threat to national security, we consider that a minimum general and non-discriminatory retention period of 24 months for the most relevant types of data in prosecuting such crimes is appropriate and proportionate. This is our early assessment, our final position on the retention period will largely depend on the findings of the impact assessment.

a) We believe that the retained data should, in principle, also be accessible for the purposes related to national security.

b) We support the establishment of minimum retention periods for all categories of data, with differentiated retention periods based on the relevance of the data for criminal investigations. As previously noted, it is both reasonable and proportionate to retain data essential for identifying suspects (e.g. subscriber data and traffic data for identification purposes, as defined in the e-evidence Regulation) for longer periods.

c) A harmonised retention framework across the EU would enhance predictability, namely, the expected scope of data that can be obtained from another Member State, which is crucial for procedural consistency and equal protection of fundamental rights. While allowing Member States to retain data for longer periods may be beneficial, permitting shorter retention periods would undermine the effectiveness of the framework. We therefore advocate for a binding EU framework that sets minimum retention periods applicable to all Member States, in particular with regard to serious offences.

5. Range of offences for which access to data is crucial

In light of the evolving nature of criminal conduct, frequently involving the use of information and communication technologies (ICTs), and the increasing migration of (serious) crime to digital environments, we assess that traffic and location data are essential for the investigation of all categories of criminal offences, particularly those committed using the ICTs.

a) This includes, in our view, all offences committed through electronic devices, offences classified as cybercrime, as well as terrorism, organised crime, economic crime, and corruption-related offences.

b) Traffic and location data play a crucial role in the investigation of the most serious criminal offences, particularly those related to national security, organised crime, and cybercrime. However, such data are also frequently indispensable for investigating offences that are either dependent on the use of ICTs or facilitated by them. These include, for example, online child sexual abuse, cyberstalking, misuse of personal data, fraudulent financial schemes, and abuse of official position. Therefore, we consider that mandatory data retention for these categories should encompass all cyber dependant and cyber enabled offences.

6. Rules and conditions for access to such data

EU legislation should establish minimum conditions for access to data subject to EU-level retention obligations, as this would contribute to the harmonisation of data-retention practices and enhance the effectiveness of cross-border cooperation between law enforcement authorities and public prosecutors.

a) In our view, access conditions should be strictly limited to what is necessary, in line with the principle of proportionality and relevant CJEU and ECHR case-law. The e-evidence legislative package reflects this approach by assigning the issuance of preservation and production orders to judicial authorities, thereby ensuring appropriate safeguards.

b) In addition to retention obligations, future EU rules should also regulate procedural and technical requirements related to the handling of retained data, namely, rules on data storage, acquisition, transmission, and the establishment of secure and uniform communication channels.

We support the introduction of basic EU-level access conditions, such as:

- applicability to serious criminal offences,
- requirement of a judicial authorisation, and
- compliance with the principle of proportionality.

Furthermore, we strongly support standardisation efforts, including forms/templates, deadlines, and secure transmission channels, in line with the model established by the e-evidence Regulation.

SLOVAKIA

1. **Scope of service providers:** *Do you consider that OTTs (over-the-top services) should be required to retain traffic data?*

- Yes, we agree with this approach. OTTs should also be required to retain traffic data, as they are required to provide such data under the e-evidence package.
- The obligation to retain data is a prerequisite for its effective and expedited preservation and production under the e-evidence package.

a. *Which service providers and which services or data held by these service providers would you consider to be particularly relevant for criminal investigations?*

- In general, we suggest basing it on the EU e-evidence package.
- For the purposes of criminal investigations, it seems that it is most important to have quick access to identification (i.e. subscriber) data, including IP addresses.
- The scope of data retained by virtual currency service providers but not regulated by MiCA should also be discussed in the future.

b. *Are there other service providers covered by the e-Evidence Regulation (which includes, in addition to electronic communication services, also information society services and domain name registers) for which requiring data retention would be particularly necessary for combating serious crime?*

- We consider both of the above categories to be important.

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?*

- Yes.
- However, the decisive criterion should not be the status of the person whose data is requested, but the purpose for which the data is requested.
- It is therefore important that this data is necessary for the justice or for the protection of persons and their safety. Not all cases need to involve a criminal offence.
- The current legal framework allows for some flexibility in accessing data, but a general and indiscriminate data retention obligation would provide a more effective and systematic framework, particularly in cases of missing persons.
- For this reason, the Slovak Republic supports legislative solutions at EU level that will allow for a combination of general retention of IP addresses of internet

connection source ports with harmonisation of a quick freeze mechanism in all Member States.

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?*

- No. We do not consider this approach right as a basic starting principle.

a. What are its benefits and shortcomings?

- The principle of targeted data retention focused on a specific range of criminal offences, certain persons or geographical areas was a response to the requirement of case law that retention should not be blanket, but subject to a proportionality test.
- Despite this, like many other delegations, we pointed out the discriminatory nature of such an approach, its potential risks in terms of crime development and the burden it places on the private sector.

b. Could data retention obligations be limited in a meaningful manner based on other criteria, such as, for example, data categories or service providers?

- Yes, we would prefer solutions based on data categories. These categories should be defined broadly enough to take into account possible future technological developments on the one hand, while on the other ensuring compatibility with existing concepts in the EU acquis.
- In relation to proportionality, a certain solution offers EU e-evidence package, which distinguishes between subscriber (basic), traffic and content data in terms of their intrusiveness into fundamental rights and freedoms from the perspective of requirements for issuing an order. The solutions chosen are strictly in line with the criteria of the EU Court of Justice's case law on access to data. In this respect, even the latest case law has not brought about any fundamental changes.
- In our opinion, proportionality must therefore be ensured in terms of the degree of intrusion into fundamental rights. We consider the retention of and access to subscriber data (telephone directory) to be the least intrusive into fundamental rights and freedoms, and the retention of and access to content data to be the most significant (most fundamental) intrusion (the above also applies to real-time interception/monitoring of data).

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?*

- The e-evidence regulation already provides for the possibility of requesting the production of subscriber data and data for the sole purpose of identifying the user in urgent cases (Article 4(5)). Extending this possibility to traffic and content data also makes sense, but the conditions for access would need to be tightened.

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?*

- In the Slovak Republic, law enforcement authorities use only those traffic and location data that telecommunications providers store for billing and marketing purposes.
- Those data are important source of information. However, its extent and availability is limited and often insufficient to successful investigation, mainly in serious criminal offences investigation or missing person's investigation. In general, it can be said that retention periods alter from zero (not retained) to 2 months. The most standard retention period, depending on the service provider or service provided, is 7 days to 3 weeks.
- For this reason, it is necessary to supplement the legal framework with targeted and time-limited tools, such as general retention of IP addresses of internet connection source ports and a quick freeze mechanism.

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?*

- No. We want to limit this provision to criminal proceedings only. We also have doubts about the legal basis.

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?*

- The repealed Data Retention Directive of 2006 distinguished between two basic retention periods: six months for IP addresses and one year for other data.

- In principle, we are open to any solution that brings about an improvement on the current situation. However, the minimum retention period should not be less than 6 months.
- We have long faced problems, particularly in the investigation of child pornography. We often encounter the reality that by the time the law enforcement authorities learn of a crime and take the necessary steps, the data is no longer available and the crime cannot be solved. Information that is more detailed is provided in the annex. There is not possible exclude cases involving the investigation of older serious organised crime where such information may be also crucial.
- We do not rule out combined solutions for public and private sector.

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?

- We can agree with the approach of minimum harmonisation at EU level.
- The clear advantage of such an approach will be to streamline cross-border cooperation, increase legal certainty and enhance the security and safety of the population. It will also reinforce the non-discriminatory nature of the private sector, as it will be subject to the same minimum rules.

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?

- In an increasingly digitalised world, access to data is key to the successful investigation of crime.
- We therefore believe that the question above should be reworded.
- The emphasis should be on achieving justice for victims of crime and ensuring that perpetrators of serious crimes cannot escape responsibility for their illegal actions simply because digital traces have been deleted or were not available because they were not retained.
- At the same time, in the absence of traffic and location data, there would be a high risk of systemic impunity, particularly in cases of:
  - cases of sexual violence against children, where rapid access to data can be crucial for protecting victims and apprehending perpetrators,

- serious cybercrime (however should not , it be forgotten that it is often knowledge of that several 'minor' criminal offences leads to the detection of serious crime),
- organised crime and terrorism, where participants use anonymised or rapidly changing connections,
- cases of missing persons, where without location data it may be impossible to locate victims quickly.

- The most common crimes in the Slovak Republic that require the request of operational and location data for investigation include fraud (online economic crime) and child pornography. From a global perspective, drug and arms trafficking, terrorism, terrorist financing and money laundering should be added to this list.
- If it is not possible to obtain operational data, it is not possible successfully identify either the perpetrators of these crimes or the extent of the criminal activity. Similarly, it is not possible to confirm or refute investigative hypotheses in the absence of data.

b. Would this include all cyber-enabled and dependent crimes or only some or other crimes as well?

- The importance of operational and location data in the Slovak Republic is not limited to cyber-enabled or cyber-dependent crimes.
- Their use is particularly crucial in criminal offences where it is necessary to identify the participants in the communication, locate persons or establish links between events and places.
- The Slovak Republic therefore considers traffic and location data to be important not only for all cybercrimes, but also for other serious crimes that are not directly dependent on the internet, where the rapid and accurate retrieval of data can be crucial for the successful investigation and prosecution of perpetrators.
- We are aware of the requirements of the case law of the Court of Justice of the European Union, but it is not possible responsibly and realistically designate only a certain group of crimes for the purposes of retaining data on them in advance.

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)?

- Yes. We believe that the issue of general data retention should primarily be a matter of regulating access to data.
- The case law of the Court of Justice of the European Union must be respected in this regard, particularly with regard to court orders for content and traffic data, with the exception of data necessary solely for the identification of a person/perpetrator.
- If quick freeze is being considered, future regulation should not be limited to regulating access to data in terms of the seriousness of the crime, but in terms of the requirements for the authority issuing access authorisation with regard to the intrusiveness of the interference with privacy. We consider the approach adopted in the EU e-evidence package to be appropriate.
- In addition it is also possible consider additional/supplementary criteria for access to operational and location data , for example:

- proceedings in which digital evidence is the only or one of the key pieces of information for identifying the perpetrator of a criminal offence,
- the principle of proportionality, for example where there is serious harm to life, health, human dignity or extensive economic damage,
- the data has a short lifespan and there is a risk of its irretrievable loss,
- less invasive means have not led to the clarification of the criminal offence in question,
- the case has a cross-border dimension that makes it difficult to obtain evidence quickly by other means.

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?

- We are open to considering such a requirement.

Appendix

Information on unresolved investigations into the distribution of child pornography

The Slovak Republic, like other Member States of the European Union, regularly receives reports from **the National Centre for Missing and Exploited Children (NCMEC)** concerning suspicions of the distribution of child sexual abuse material.

In most cases, the identification of the user **of the** specific **IP address** from which the illegal activity originated is essential in order to identify the perpetrator. However, in the Slovak Republic, there are fundamental problems in obtaining this information from internet service providers (ISPs).

Some providers **do not store information about IP address allocation at all** (e.g. **Antik Telecom**), while others only store it **for a very short period of time, usually 14 days** (e.g. **Slovak Telekom**). This situation significantly hinders or prevents effective investigation of cases, as:

- reports from NCMEC often arrive **with a time lag**,
- they are then **forwarded to the relevant departments of the Police Force**,
- and these departments must then **obtain a court order** to obtain the data from providers.

This entire process usually takes longer than two weeks, during which time the data is still available from some providers. As a result, **in many cases it is not possible to continue criminal proceedings** because it becomes impossible to identify the perpetrator.

For these reasons, the Slovak Republic considers it **extremely beneficial and necessary** for the EU legislative framework to establish an obligation to retain information on IP address users **for at least six months**. Such a measure would significantly strengthen the ability of law enforcement authorities to respond effectively to cases of child sexual abuse and would ensure a higher level of protection for minors in the online environment.

The table below provides indicative statistics on the number of reports received and an overview of providers who:

- do not provide data on assigned IP addresses at all, or
- only store this data for a limited period of time, which prevents law enforcement authorities from taking effective action.

2021

Received:	3991	100.00 %
Antik Telecom (0 days)	33	0.82 %
Slovak Telekom (2 weeks)	1188	29.77 %
Total unrealised:	1221	30.59 %

2022

Received:	7918	100.00 %
Antik Telecom (0 days)	72	0.91 %
Slovak Telekom (2 weeks)	1876	23.69 %
Total unrealised:	1948	24.60 %

2023

Received:	24,618	100.00 %
Antik Telecom (0 days)	214	0.87 %
Slovak Telekom (2 weeks)	2335	9.48 %
Total unrealised:	2549	10.35 %

2024

Received:	62,326	100.00 %
Antik Telecom (0 days)	335	0.53 %
Slovak Telekom (2 weeks)	6510	10.45 %
Total unrealised:	6845	10.98 %

01-09/2025

Received:	49,991	100.00 %
Antik Telecom (0 days)	242	0.48 %
Slovak Telekom (2 weeks)	4244	8.49 %
Total unrealised :	4486	8.97 %

FINLAND

FI Written Comments 10.10.2025
Presidency Paper Future rules on data retention in the European Union WK 11640/2025

General remarks

Finland is currently in the process of forming our official position on the topic of updating data retention rules on EU level. At this stage, the answers presented below should be regarded as preliminary expert views. We mean to clarify our position as soon as possible to provide more detailed responses and participate in the important discussion on the future of data retention rules.

Finland welcomes the European Commission's initiative to conduct an impact assessment on potential EU-level solutions. Finland considers it essential that any potential legislation is proportionate and that interference with confidentiality of communications is limited to what is strictly necessary. Any legislative initiative must take into account the obligations arising from the EU Charter of Fundamental Rights, data protection legislation, and the case law of the EU Court of Justice, while also recognizing the need to develop legislation that meets the needs of the digital environment.

Answers to questions presented in the Presidency Paper

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 combat-ing 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?

In general, Finland is supportive of measures that improve the means of criminal investigations and crime prevention, without undermining citizens' fundamental rights. FI supports on focusing on such a group of communication service providers, for whom EU level obligations would particularly be needed. Especially regarding services operating in multiple Member States, it could be justified to seek a solution at the EU level. FI recognizes the challenges underlined by the High-Level Group on Data Access regarding the availability of data and compliance of data requests by the OTT service providers.

According to our national law enforcement authorities, in addition to communication services data, data from cryptoasset service providers and payment services as well as VPN services are often relevant for criminal investigations.

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?

We have nationally assessed the possibility of clarifying the current data retention obligation in accordance with the restrictions set by the case law of the Court of Justice of the European Union (CJEU). The targeting criteria established by the CJEU were found somewhat problematic.

Technical implementation of a geographical targeting criteria would require further analysis. However, targeted retention based on the criteria based on CJEU case law could lead to weakening the possibility of investigating offences and the realization of criminal liability, if it means that less data is retained.

Defining the geographical locations relevant to the investigation of serious offences on a statistical or other risk-based basis is a very challenging task, and the residence and movement of persons between different areas may form a very complex technically manageable and feasible system. In homicides, for example, it is customary for the place of commission or concealment to be located in a remote area. The risk-based retention of data on the basis of a geographical or personal criterion could also citizens in an unequal position on the basis of their place of residence.

Targeting based on personal characteristics, on the other hand, was not considered not so useful for criminal investigations, as it is difficult to predict future behavior based on past criminal history. Moreover, such a measure does not appear unproblematic in terms of the presumption of innocence.

In addition, if targeted retention is applied in a way that it significantly reduces the amount of data available to LEA, it may also weaken the protection of fundamental rights. If the information is not available, the investigation of an offence could require the use of more intrusive coercive measures, repeated individual requests for information or the use of coercive measures mainly to secure the information. Data would also have to be collected and combined from different service providers and different data sources by means of criminal requests. In practice, this means that service providers would be given more information than at present on the perpetrators of offences.

However, in light of the principles of proportionality and necessity, any legislation should limit the categories of data and the service providers to which the obligation are applied to, regardless of other targeting criteria.

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?

According to the information received in our national assessment, the retention periods of data stored for their own purposes vary depending on the operators. Some data, such as IP addresses or information on unanswered calls, are retained only for a very short time. In such cases, the availability of data would be random and predictability of access to such data would be weak. In addition, it is also challenging that the authorities must know in concrete terms, to whom the order is directed.

Therefore, a quick freeze order as the sole retention measure does not appear to sufficiently meet the authorities' needs for access to information. However, it could be a more useful measure when combined with other retention measures and as a supporting tool, e.g. for those service providers or categories of data which might not be included in the scope of retention obligations. Increasing use of retention orders would result in additional work for service providers in the form of repeated individual requests for retention.

In Finland, data retention obligation is only applicable to the main traditional teleoperators. Data requested from other service providers is thus directed to data retained for marketing and billing purposes by the operator.

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?

As a preliminary expert view, retention of data for the purpose of national security should not be regulated on the EU level. Instead, this topic should be left for the Member States to regulate.

In Finland, the current data retention obligations include different retention periods for each category of service. Our current retention periods are 6, 9 and 12 months.

Common rules for retention periods across the EU would increase the predictability of criminal investigations and would improve the use of resources and data protection, as unnecessary requests for information would not have to be submitted for data that is no longer available. Retention periods set in any possible legislative measures should be limited to what is strictly necessary to ensure effective criminal investigations.

For example, retrospective traffic data is highly significant in large investigations of organized crime, where the investigation periods are also long. Retrospective telecommunications monitoring is the most reliable, difficult to deny as a fact and often the only available piece of evidence when more than one month has passed from the time when the offence was committed. In some instances,

such as investigations of crimes directed at information networks or committed using them, authorities often rely on information that is available internationally.

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?

Our preliminary expert view is that *serious crime* should not be defined on the EU level, and instead this should be left to the Member States to determine (as in C-178/22 Procura della Repubblica presso il Tribunale di Bolzano). However, the purpose for which data must be retained, must be in a precise manner. This should be pursued in a way which takes into account both the needs of criminal investigations and the protection of fundamental rights.

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 authorization 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?

At present, FI does not have a position on how access to retained data should be regulated. The fairly new E-Evidence Regulation specifically addresses cross-border access to data. For the national assessment, we would require further information on what the referred access rules and conditions could mean.

SWEDEN

I. General considerations

The present impact assessment (IA) by the Commission on the retention of communication metadata for law enforcement purposes and judicial proceedings is very important to Sweden. Consequently, Sweden wishes to put forward a set of key considerations in relation to data retention, considerations that in the opinion of Sweden must be taken fully into account in the IA and be included in the possible elaboration of a legal EU-framework on data retention.

In general, Sweden is of the view that a legal EU-framework on data retention for law enforcement purposes will, provided that full account is taken of the present and well-described needs of law enforcement, bring added value to crime fighting across the Union. A level playing-field would clarify what type of data may be available for how long and the application of the EU Regulation on eEvidence would be strengthened. Obviously, an EU framework would also be helpful for service providers and standardisation bodies such as ETSI.

Furthermore, joint action at EU-level compared to action by Members States alone would also be positive for the effectiveness of access to data for law enforcement purposes, for instance in relation to obligations of number-independent service providers (OTT-services) originating from outside the Union. Indeed, approximately 97% of mobile messages are currently sent via these OTT-services, with traditional SMS and MMS making up only about 3% of the messages.

However, a further assessment on the added benefits and value of data retention and any consequences relating to the EU budget as well as national budgets must be made. The changing ways of communication, including a shift into OTT-services being the main way of communicating and the increase in cross-border flows of communication metadata, also necessitates an assessment on the possible impact of an EU data retention framework on the security and robustness of electronic communications.

II. Needs, necessity and proportionality

Numerous cases from across the EU illustrate the need and necessity to access retained communication metadata to investigate crime[27]. Indeed, the needs and necessity have been demonstrated again and again by experts, in reports, in various documents and by years of discussions at EU-level.

The Europol SOCTA and IOCTA reports describe an evolving online dimension of crime and an increasingly, wide-spread misuse of not least OTT-services for criminal purposes; the annual reports of the SIRIUS network have for six years described the needs for access to electronic evidence and the challenges to obtain it; the COPEN Working Party has prepared a compilation of cases and discussed all thinkable options to respond to the needs; Europol has organised workshops on the basis of a data matrix derived from 487 data fields included in the ETSI standard and Eurojust has presented two studies on data retention. In particular, the High-Level Group on access to data for an effective law enforcement has recently highlighted the need for law enforcement to access retained communication metadata.

In addition, many Member States have participated in one or more cases before the Court of Justice, and thereby been able to develop their explanations on the need and necessity to access retained traffic, location and subscriber data for the purpose to fight crime and uphold the rule of law also when society and criminality get digitalised.

Above all, it is, according to Sweden, imperative to stress that the need and necessity to uphold and strengthen the crime fighting capacity by means of access to retained communication metadata and subscriber data has grown exponentially over the past years and continue to grow. For these reasons it is of immense importance that the objective is set at an assessment of a possible EU legal framework that:

1. Corresponds to the present needs of law enforcement.
2. Takes into account the rapid development of digital tools that are misused as instruments to aid, abet, incite, instigate and commit crime.
3. Allow law enforcement services and the judiciary to better protect victims of crime and to provide rectification.

[27] C.f. WK 5296/1/2017, Retention of communication data - compilation of cases

4. Ensures a robust framework of safeguards and security arrangements, both at the obligated service provider and the processing authority and including both procedural and technical measures.

In addition to the clearly demonstrated need and necessity, an up-to-date proportionality assessment based on real world developments also lead Sweden to the conclusion that an EU-framework that lays down the non-targeted retention of traffic and location data for an appropriate length of time to fight serious crime, in conjunction with a set of safeguards, does not exceed what is necessary, appropriate and proportionate in a democratic society. On the contrary, such a framework would achieve a fairer balance between the right to privacy and the need for security and public safety as well as a much-needed review of the interpretation of Directive 2002/58, in particular its Article 15.1.

A case in point from a Swedish perspective is the online recruitment of minors into crime and the use of end-to-end encrypted services for the execution of the crimes.

In recent years, the Swedish Police have seen a frightening development in which criminal networks and its instigators are posting "job ads" on social media calling on minors to commit for instance murder of rival gang members and their relatives for money. Social media platforms where minors are present are used at the initial stage, but when a minor responds to a post, further planning and instructions are moved to an end-to-end encrypted service.

The instigators are often located abroad, in a country with which it is usually difficult to cooperate. Minors, as young as 13 years old, who are committing these crimes are often caught by the Police. However, the instigators walk free since they can be anonymous on social media and in their end-to-end encrypted services. The OTT communication services do not cooperate with law enforcement to the extent needed.

Online recruitment constitutes a very serious development that must be addressed with priority. To ensure that law enforcement action is effective throughout the chain from recruitment to the execution of a serious crime, access to retained traffic, location and subscriber data is indispensable. The cross-border dimension is also very present and further action at EU level to reach instigators and recruiters in countries other than where crime is committed is necessary.

In conclusion, Sweden is preliminary in favour of an EU framework that provides for the retention of traffic, location and subscriber data for law enforcement purposes that at a minimum, corresponds to the so called restricted and differentiated retention, i.e. the careful assessment and selection[28] of a set of traffic, location and subscriber data to be retained for differentiated periods in time and that will enable law enforcement services to perform their responsibilities (see below under V).

III. A robust framework of safeguards

Any legally mandated retention of communication metadata and access to such data must be accompanied by a robust framework of safeguards throughout the entire process (end-to-end safeguards).

This includes not least:
- Security requirements and arrangements to avoid the risk of abuse, unlawful access and breach of data secrecy of retained data, both at the service provider and the processing authority.
- Authorisation, judicial or directly by a law enforcement agency, depending on the intrusiveness of the data to be accessed.
- Clear and precise conditions for access to the retained data, including purpose limitation to prevention, detection, investigation and prosecution of crime, necessity and proportionality requirements.
-Differentiated time periods for retention depending on the intrusiveness of the type of communication metadata.
- Notification obligation to those affected by access to retained traffic and location data once it will not jeopardise the investigation.
- Review mechanisms by the data processing law enforcement agencies themselves and ex-post oversight of service providers and law enforcement agencies by dedicated independent administrative authorities such as data protection authorities and specialised agencies in the field of telecom.
- Complaint and redress mechanisms.

[28] Cf. EDOC#965006v3 Concept of Restricted Data Retention and Targeted Data Access, Outcome of Data Matrix Exercise (based on 487 data fields of the ETSI-standard and discussing the concept)

IV. The High-Level Group on access to data for an effective law enforcement

In November 2024, the work of the High-Level Group (HLG) on access to data for an effective law enforcement was concluded with a report[29]. The JHA Council has concluded that the recommendations on data retention are among the key issues of the report to take further. The recommendations of the HLG as well as the explanatory text on harmonising minimum rules for the retention of metadata etc. are highly relevant in the context of an IA and the possible elaboration of an EU legal framework. This includes inter alia:

- That distinctions should be made between categories of data which would allow the intrusiveness of each data category – and hence the safeguards required – to be properly assessed.

- That user data retained for commercial and business purposes is effectively accessible for law enforcement under relevant safeguards.

- That in order to take future technological developments into account, entities subject to data retention obligations should include telecommunication providers, OTT-services and other service providers collecting data with a specific individual or legal person who uses their services, such as car manufacturers or LLM based AI systems[30];

- That obligations are needed to increase transparency requirements on service providers regarding the data they store and for how long.

Sweden concurs in general with the recommendations of the HLG as well as the explanatory text and is of the opinion that they are highly relevant in the IA and if an EU legal framework is elaborated.

V. Main purposes for accessing retained communications metadata in criminal investigations

The HLG recommends in Cluster 6, point 1, that categories of metadata should be defined based on the purpose of its use. Sweden agrees with this recommendation and wish to recall

[29] 15941/24
[30] Cf. Article 3.3 of the Regulation on e-evidence

the main purposes for retaining and accessing metadata for law enforcement purposes and judicial proceedings. Obviously, the overall purposes are the prevention, detection, investigation, and prosecution of criminal offences. But, for what specific purposes will the communication metadata and subscriber data be used? Primarily, the data will be used for two specific purposes, namely:

To identify a user of communication and online services (i.e. subscriber information such as IP addresses, e-mail, IMSI[31], IMEI[32], MSISDN[33], username)

To establish the following:

- *WHO has communicated with whom* (i.e. subscriber data, the source and destination of a communication).

- *WHEN the communication took place* (e.g. timestamp).

- *WHERE the communication took place* (i.i. location information).

- *HOW the communication took place* (e.g. fixed or mobile telephony, e-mail, device).

While recognising that communication metadata can be used also for other specific purposes and analysis, Sweden considers the above to be the main two purposes. On this basis specific types of required data can be assessed and defined in a technology-neutral and future-proof manner. A distinction between data categories to assess their respective degree of intrusiveness can also be made and such an assessment would also be helpful in relation to the principle of data minimisation.

National security concerns

Sweden maintains its position on the importance to adequately address the issue of national security in relation to an EU legal framework on data retention. The framework should not

[31] IMSI = International Mobile Subscriber Identity
[32] IMEI = International Mobile Equipment Identity
[33] MSISDN = Mobile Station International Subscriber Directory Number.

impede the Member States from exercising their responsibility for national security, in accordance with Article 4.2 of the TEU.

VI. Brief replies to questions in document 11640/2025

Scope of service providers

Sweden is of the view that OTT-services must be included in a future EU-framework with obligations to retain communication data. 97% of messages are today sent via OTT-services and only 3% via traditional telecom.

In addition to interpersonal communication services as defined in Directive 2018/1972 and including OTT-services, Sweden thinks that it should be examined which other service providers processing communication metadata that needs to be included in a data retention framework. It seems to Sweden that it would be of particular interest to include service providers within scope of the Regulation on eEvidence, providers of VPN-services and car manufacturers in such an examination.

Targeted/limited/differentiated retention framework for traffic and location data

Sweden is of the view that targeted retention (based on personal or geographical criteria) is not a sufficient tool to investigate and combat serious crime. Retention based on geographical criteria will leave gaps in the availability of historic communication metadata and since it is impossible to foresee where a crime will be committed a retention limited to certain geographical areas will not be sufficient.
There are also important technical challenges and significant costs involved in the implementation of targeted retention based on geographical criteria. A retention based on geography may also lead to discrimination.

As regards retention based on personal criteria, it seems to be less useful in that it would be very easy to circumvent, for instance by using a frontman.

Furthermore, Sweden is of the view that it is possible to limit data retention obligations in a meaningful manner based on other criteria such as data categories, in particular if the data categories to be retained are analysed in relation to the purposes for its use.

Above it is concluded that a framework is needed that provides for the retention of traffic, location and subscriber data for law enforcement purposes that at a minimum, corresponds to the so called restricted and differentiated retention that has been discussed many times in COPEN.

In this context, it should also be pointed out that a certain data category which may today not be deemed necessary for law enforcement purposes could already tomorrow become essential, for instance if certain technical components in communication tools change. It is therefore important to ensure technology neutral and future proof definitions of the data to be retained rather than listing technically very specific descriptions of the data. A neutral text would also allow standardisation bodies such as ETSI and 3GPP to translate the definitions into technical standards.

Expedited retention orders (Quick freeze)

Sweden is of the view that expedited retention orders or quick freezes may be a complement. However, it cannot replace the access to retained communication metadata.

Retention periods

It seems that a retention period of 12 months for crime fighting purposes is preferred by most Member States. However, a differentiation of retention periods should be made depending on the intrusiveness of the category of data to be retained.

On national security, see above.

Scope of crimes for which availability of communication data is particularly relevant

In our more and more digitalized societies, access to communication metadata is relevant for the investigation of in principle all types of crime. In view of the digital developments, the relevance will only increase.

Access rules and conditions

It seems to Sweden that traffic and location data are the most intrusive, while subscriber data is less intrusive. Consequently, access to traffic and location data can be limited to fighting serious crime and be subject to prior review by a court or by an independent administrative body. However, it must be for the Member States to define serious crime or serious offences in the light of the societal conditions prevailing in the Member State concerned.
As regards the less intrusive subscriber data, access should be allowed to competent authorities upon request for the purposes of combating criminal offences in general.

In relation to access rules and conditions, Sweden also wishes to underline that access to communication metadata presupposes that a threshold is met constituting probable cause or reasonable grounds or a criminal context.
It appears to Sweden that this circumstance has been disregarded to a not negligible extent in the discourse albeit it sets an important condition for access that also points to a subject of interest or suspect.

Furthermore, the purpose principle, the necessity principle and the proportionality principle apply to all orders on coercive measures in Sweden. The purpose principle means that the use of a coercive measure must be tied to the purpose for which the coercive measure has been decided. According to the necessity principle, an authority may use a coercive measure only when there is a clear need for it and a less intrusive measure is not sufficient. The proportionality principle means that a coercive measure may only be used if the reasons for the measure outweigh the infringement or other harm that the measure entails for the suspect or any other opposing interest. In other words, these principles provide an additional layer of conditions for access that Sweden is accustomed to.

Finally, Sweden wishes again to refer to the recommendations of the HLG that are highly relevant for further considerations on access rules and conditions, for instance "…ensuring that Member States can enforce sanctions against electronic and other communications services providers which do not cooperate with regard to the retention and provision of data…".

CTC

From the point of view of the EU CTC, data retention is crucial to prevent, investigate and prosecute terrorist acts. The EU CTC has participated in the High-Level Group on access to data for effective law enforcement and fully supports its recommendations on data retention. The EU CTC also contributed to the call for evidence in the framework on the Commission's impact assessment on data retention by service providers for criminal proceedings.

The Presidency's discussion paper gives a very good overview of the evolving jurisdiction of the Court of Justice of the European Union and raises six relevant questions. The EU CTC would like to give some input to these questions from a counter-terrorism perspective.

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?

We have to be aware that today more than 90% of messaging passes through OTTs. In accordance with the recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, the EU CTC is in favour of establishing a harmonised EU regime on data retention that is technology-neutral and future-proof and that covers present and future "data handlers", i.e. OTTs and service providers of any kind that could provide access to electronic evidence.

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?

The EU CTC is fully aware of the case law of the Court of Justice of the European Union. However, terrorist offences demonstrate well why it is very difficult or even impossible to define targeted retention criteria based on personal or geographical criteria. Very often we see attacks of perpetrators that were not known to law enforcement authorities before, and very often we see attacks in places that were not known as "hot spots" for terrorist attacks. Therefore, if jurisdiction requests to limit data retention obligations, data categories might be a better criterion.

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?

Quick freeze, also known as data preservation, and data retention are two different criminal investigation tools. The quick freeze procedure might work in certain specific cases. However, it is not a real alternative to data retention. Freezing is only possible when there is suspicion of a crime. However, this point in time is in many cases too late for freezing any data, because the data is no longer available. This can be clearly demonstrated by the example of IP addresses: Very often providers store IP addresses only between four and seven days. Sometimes they even store them only for one day or a few hours. Therefore, in most cases the quick freeze procedure is no longer capable of securing any relevant data.

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?

The terrorism threat in the EU remains high. This must be reflected in EU legislation as well. The fact that we have a patchwork rug of data retention rules in the EU does not match the overall terrorism threat in the EU. From the point of view of the EU CTC, the EU must adopt legislation on minimum data retention rules for service providers, which would allow more far-reaching national legislation to be preserved.

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?

The availability of subscriber, traffic and location data is particularly relevant for the effective investigation and prosecution of terrorist offences. Otherwise, this bears a very high risk of impunity.

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?

The EU CTC sees value in defining standardised formats for data retention. In fact, while a standard developed under the auspices of the European Telecommunications Standards Institute (ETSI) exists for traditional telecommunications metadata, it is not universally applied across the Member States even with telecommunications providers, and there is no agreement on a standardised format for data transmissions from OTTs to law enforcement authorities. This adds complexity to the data analysis in cases where data can be provided at all. Standardisation should be pursued to ensure harmonised categorisation of data to be retained and accessed, but also for establishing secure channels for the exchange between competent authorities and service providers.