Poland's written comments on Future Rules on Data Retention in the European Union

after meetings on 25 September 2025.

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.