Council of the European Union

Brussels, 3 October 2025
(OR. en)

13029/25

COPEN 272
CYBER 252
ENFOPOL 330
JAI 1275
DATAPROTECT 222
COSI 163
IXIM 199
CATS 46
FREMP 241
TELECOM 310
CT 117

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Access to data for effective criminal investigations - State of play

Ensuring lawful access to data on electronic communications for the purpose of law enforcement and criminal investigations is a priority for the Council and is particularly necessary in the context of the fight against serious and organised crime and terrorism.

Following the work of the High-Level Group on access to data for effective law enforcement (hereafter the High-Level Group) that issued recommendations[1] in May 2024 and a concluding report[2] in November 2024, and the Council conclusions on access to data for effective law enforcement[3] from 12 December 2024, the Commission presented a Roadmap for lawful and effective access to data for law enforcement[4] on 24 June 2025 ('the Roadmap'). In its conclusions of 26 June 2025, the European Council invited the EU Institutions and the Member States to take further action to strengthen law enforcement and judicial cooperation, including on effective access to data for law enforcement purposes.[5]

In particular, the Presidency would like to draw the attention of Justice Ministers to the issues of data retention (1), lawful interception of communications (2) and the horizontal challenge of encryption (3).

1. Data retention

'Data retention' refers to the obligation placed on service providers to retain non-content data (subscribers' information, IP addresses, traffic and location metadata) for a certain period of time so that it can be made available to law enforcement authorities for the purpose of criminal investigations.

The High-Level Group dedicates one of the three chapters of its concluding report to data retention. Among key issues, the report insists on the current fragmentation of national legislation and the additional challenges presented by providers of 'over-the-top' services (OTTs), including widely used messaging apps for mobile phones. As possible solutions, the High-Level Group points at establishing harmonised minimum rules for retention and access. It also advocates for reinforcing the cooperation between service providers and practitioners.

1 11281/24.
2 15941/2/24 REV2.
3 16448/24.
4 10806/25.
5 EUCO 12/25.

In its Roadmap, the Commission indicates that it will prepare an impact assessment with a view to updating EU rules on data retention as appropriate. The impact assessment was launched in May 2025 and is expected to be finalised in the first quarter of 2026. The Commission also urges Europol and Eurojust to work further on streamlining cooperation with communications service providers and to develop, in cooperation with these providers, a catalogue of data which they process for their business purposes.

In the Council, the Working Party on Judicial Cooperation in Criminal Matters (COPEN) dedicated its meeting of 19 May 2025 to the issue of data retention, focusing on a possible future EU legislative proposal on the matter. A second meeting was held on 25 September 2025, where COPEN discussed the suitable content and criteria for that instrument, also in light of the requirements set out in the case law of the European Court of Justice (CJEU). The objective in both cases was to exchange views and provide input to the Commission's ongoing work.

Depending on the outcome of the Commission's impact assessment, the Presidency considers that a key development in 2026 could be the start of discussions on a legislative proposal for EU rules on data retention.

2. Lawful interception of communications

Lawful interception allows authorities to gain covert access to communications in real time.[6]

In its concluding report, the High-Level Group noted that 'while lawful interception of traditional telecommunications remains an essential tool in many investigations, the effectiveness of this measure has drastically decreased as telecoms services are now mostly provided by other actors: according to various sources, around 97 % of all mobile messages are now sent through messaging apps like WhatsApp, Facebook Messenger, and WeChat, while traditional SMS and MMS messaging accounts for only about 3 % of messages.'

[6] It also covers access to communication with little delay as further explained in the concluding report of the HLG.

The High-Level Group makes several recommendations, including with a view to making lawful interception requests enforceable for all types of providers of electronic communication services. They include clarifying the definition and scope of lawful interception, identifying necessary safeguards, clarifying the concept of territorial jurisdiction over data, exploring how the European Investigation Order could better support efficient cross-border lawful interception requests and fostering the development of bilateral agreements on real-time access to data with third States. In the longer term, based on further analysis and an impact assessment, the experts recommend devising an EU instrument on lawful interception (consisting of soft-law or binding legal instruments) for law enforcement purposes that would establish enforceable obligations for providers of electronic communications services in the EU.

In its Roadmap, the Commission indicates that it will propose measures to improve the efficiency of cross-border requests, strengthening existing instruments such as the European Investigation Order (by 2027), and to explore measures to create a level-playing field for all types of communication providers, determining the most efficient approach to tackle the non-cooperative ones.

During the Danish Presidency, Member States will be invited to share their practices and current limitations with implementing cross-border lawful interception measures, in particular in the context of the European Investigation Order and bilateral and multilateral agreements.

3. The horizontal issue of encryption

It is also important to insist on the challenge which encryption represents for access to data for effective criminal investigations, including for the issues of data retention and lawful interception mentioned above. Many services now use end-to-end encryption to protect the confidentiality of communications, privacy and cybersecurity, which can make it extremely difficult for law enforcement authorities to obtain lawful access to readable communication data.

The Commission announces in its Roadmap that it will present in 2026 a specific Technology Roadmap on encryption to identify and evaluate solutions that enable lawful access to encrypted data, while safeguarding cybersecurity and fundamental rights. To achieve this objective, the Commission is setting up a group of experts which plans to start work in autumn 2025.

The Commission will also support the research and development of new decryption capacities to equip Europol with next generation decryption capabilities (from 2030).

Next steps and coordination

The issue of access to data for effective criminal investigations is complex and requires a multidisciplinary approach. For the efficiency of the work ahead and to ensure that all aspects are taken into account, the Danish Presidency considers it essential to involve the various preparatory bodies of the Council, including those in charge of internal security and law enforcement cooperation, cooperation in criminal matters, and cybersecurity. In the Council conclusions from 12 December 2024, the Council tasked the Standing Committee on operational cooperation on internal security (COSI), in cooperation with the Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS), to coordinate, discuss and monitor the implementation of the Roadmap. The Danish Presidency has prepared a detailed overview of the envisaged activities on access to data for effective law enforcement, with a division of tasks and a timeline, which was considered by COSI on 18 September 2025.[7]

The Danish Presidency considers it very important to continue to ensure that both Ministers of Home Affairs and Ministers of Justice closely follow the developments on access to data for effective law enforcement, with the objective of providing law enforcement with the necessary tools to effectively prosecute crimes in full respect of fundamental rights. To this end, an information note to the Council will be prepared at the end of the Presidency's term encompassing the activities performed within the various Council structures.

---

[7] 12381/25.