Council of the
European Union

**Brussels, 8 May 2025
(OR. en)**

8453/25

LIMITE

**COSI 67
ENFOPOL 126
IXIM 86
CATS 19
COPEN 101
CYBER 111
DATAPROTECT 72
JAI 514**
***CEPOL
EUROJUST
EUROPOL
FRA***

NOTE

From:	Presidency
To:	Delegations
Subject:	Access to data for effective law enforcement

Introduction

The 42 recommendations of the High-Level Group on access to data for effective law enforcement (HLG) issued in May 2024[1] address current and anticipated challenges against the background of technological developments, enabling a comprehensive EU approach to ensure effective criminal investigations and prosecutions as an essential element of the rule of law. The recommendations are clustered in three blocks: (1) capacity building, (2) cooperation with industry and standardisation, and (3) legislative measures. They are not binding but may contribute significantly to informing policy choices at national and EU level in the coming years.

[1] 11281/24.

The Council exchanged views on the HLG recommendations and the HLG concluding report[2] in June and December 2024 respectively, and adopted conclusions on access to data for effective law enforcement[3], inviting the EU institutions, bodies and agencies and the Member States to consider the valuable contribution of the HLG when developing and implementing concrete actions. In addition, the Council invited the Commission to present a roadmap by Q2 2025 for the implementation of relevant measures. In ProtectEU: a European Internal Security Strategy (hereinafter 'the Strategy')[4] presented on 1 April 2025, the Commission announced that it would present a roadmap setting out the way forward on lawful and effective access to data for law enforcement in 2025. In the exchanges of views at the Council, ministers referred to the possibility and advisability of implementing some actions without delay, including:

- the mapping of existing relevant legislation and case-law;
- capacity building;
- standardisation;
- cooperation with industry.

Bearing this in mind, the Presidency has conducted informal consultations and has identified measures that could be launched in the short term, and is suggesting some recommendations that could already be implemented or prioritised in the upcoming roadmap to be prepared by the Commission.

[2] 15941/2/24 REV 2.
[3] 16448/24.
[4] 7750/25.

Recommendations and suggested measures that should start being implemented[5]

The Presidency suggests starting the implementation of HLG recommendations 2, 7, 15, 16 and 26 as follows:

1. Member States should consider sharing available digital forensics tools, e.g. software licences, with the law enforcement authorities of other Member States through the Europol Innovation Lab's Europol Tool Repository (ETR), which is an established, regulated, and well-known source of cutting-edge investigation tools addressing a broad spectrum of operational requirements, including relating to digital forensics. The ETR has significant reach and can both facilitate the pooling of resources and help disseminate tools across Member States to enhance their overall capacity for improving access to data. Member States can make use of the services offered by the European Anti-Cybercrime Technology Development Association (EACTDA) to bring tools to a fully operational level prior to their distribution through the ETR.

2. Europol and Eurojust should set up a joint project to facilitate the sharing of knowledge and expertise in digital forensics similar to SIRIUS, subject to the allocation of sufficient financial and human resources.

3. The European Cybercrime Training and Education Group (ECTEG), supported by the European Union Agency for Law Enforcement Training (CEPOL), should put in place an EU certification scheme and additional training opportunities for digital forensics experts, based on the activities they already perform. Adequate and flexible mechanisms should be established to ensure that certification processes do not become a bottleneck.

4. Member States should support the activities under the EU Innovation Hub for Internal Security's thematic cluster on encryption, led by the Commission's Joint Research Centre (JRC), including on exploring a European approach for the management of vulnerabilities in internal security, while taking due account of the EU cybersecurity framework.

[5] Recommendations 2, 7, 15, 16 and 26.

5. The Commission and Member States should consider raising awareness about possible solutions facilitating lawful access to data and devising cross-cutting initiatives under EMPACT. Access to data should also be considered in the preparation of the General Multi-Annual Strategic Plan (G-MASP).

6. The European Working Group on Standardisation on Internal Security coordinated by Europol should propose ways to foster and better coordinate Member States' participation in standardisation fora, building upon the existing standards developed by the European Telecommunications Standards Institute (ETSI). This working group requires more resources in terms of both funds and technical staff to meet expectations. Europol has applied for ETSI membership, which would enable the agency to promote Member States' interests in relevant standardisation groups.

7. Member States should make best use of cooperation with industry, standard-setting, and building or acquiring relevant tools when preparing for the implementation of the e-evidence regime. It is important to adequately involve law enforcement authorities in the ongoing process.

8. Member States should consider concluding memoranda of understanding with private parties, laying down the principles of cooperation with industry, as well as leveraging the experience gained through SIRIUS, with a view to enhancing transparency and getting access to categories of available data. Coordination among Member States will be important. This does not exclude the possibility of setting obligations in line with recommendation 17 (see below).

9. Experts from Member States and relevant EU agencies are encouraged to apply to join the research group that will be established by the Commission to help assess the technical feasibility of lawful access obligations in compliance with fundamental rights and without undermining cybersecurity, in accordance with recommendation 26.

Recommendations that the Commission is invited to prioritise in the upcoming roadmap to ensure lawful and effective access to data

The Presidency welcomes the announcement made by the Commission in the Strategy that, following up on the HLG recommendations, the Commission will prioritise an assessment of the impact of data retention rules at EU level and the preparation of a technology roadmap on encryption to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights.

Beyond that, the Presidency suggests inviting the Commission to also prioritise the following recommendations in the upcoming roadmap to ensure lawful and effective access to data, in compliance with fundamental rights and without undermining cybersecurity:

1. Developing a mechanism at EU level for jointly purchasing the licences of digital forensic tools, to share them among Member States.[6]

2. Fostering transparency rules for providers of electronic communications services with regard to the data they process, generate or store by concluding cooperation agreements with them or, if necessary, by setting mandatory obligations.[7]

3. Drawing inspiration for future legislative, practical, and technical initiatives from a common definition of requirements, such as that set out in the Law Enforcement Operational Needs for Lawful Access to Communication (LEON). Setting up an ad-hoc group of experts, possibly coordinated by Europol, would ensure that LEON is updated where needed, possibly under the coordination of the working group on standardisation for security hosted by Europol, whose mandate should be extended.[8]

[6] Recommendation 3.
[7] Recommendation 17.
[8] Recommendation 21.

4. Assessing the technical feasibility of lawful access obligations (including for accessing encrypted data) for digital devices while meeting the objectives of lawful access, fundamental rights and cybersecurity and building on the work of the expert group that the Commission will set up and the technology roadmap on encryption.[9]

5. Assessing and developing rules on accountability and enforceability for service providers in order to enforce obligations on them to retain and provide data, e.g. through the implementation of administrative sanctions or limits on operating in the EU market.[10]

6. Exploring the feasibility of or the possibilities around setting obligations on service providers to turn on or off certain functions in their services to obtain certain information after receiving a warrant (for example storing geolocation of a specific user after s/he is targeted by a lawful request).[11]

7. Developing a mechanism to ensure that Member States can enforce sanctions under administrative and criminal law against non-cooperative electronic communications services, and that such measures act as a deterrent against those entities.[12]

[9] Recommendation 26.
[10] Recommendation 30.
[11] Recommendation 32.
[12] Recommendation 33.

Communicating on access to data for effective law enforcement

Several Member States and the EU Counter-Terrorism Coordinator (EU CTC) have expressed their intention to actively contribute to communication efforts about access to data for effective law enforcement, following a common narrative that underscores the importance of law enforcement authorities operating within legal frameworks to safeguard society, while fully respecting fundamental rights as laid down in the European Union Charter of Fundamental Rights and the European Convention on Human Rights and without undermining cybersecurity. These communication efforts should also encourage cooperation between service providers and public authorities and foster a constructive public discourse.

To demonstrate that the risk of ‘going dark’ is a challenge to the rule of law and the security of citizens today and in the future and to underpin the need for law enforcement authorities to lawfully access data, the relevant authorities of the Member States should provide concrete examples including evidence and statistics on the difficulties regarding lawful access to data (e.g. criminal investigations that were impeded because data was not stored/retained, was encrypted and could not be decrypted or was not released by the service provider).[13]

It is of utmost importance that law enforcement and judicial authorities raise awareness about their perspectives and the consequences for internal security if they do not have access to the data they need, and that they engage with stakeholders such as the European Parliament or national parliaments, data protection and cybersecurity authorities, civil society including victims’ rights organisations and national human rights institutions, industry, academia, and the general public.

Below, the Presidency provides delegations with examples of communication activities, and, in the addendum to this note, with a repository of non-exhaustive key messages and case examples that could help national authorities, including law enforcement and judicial authorities, the Commission, the EU CTC and the JHA agencies, when communicating about access to data for effective law enforcement at national, EU or international level. This repository could be further developed with the support of Europol and Eurojust.

[13] The SIRIUS EU Electronic Evidence Situation Report identifies barriers to effective cooperation in accessing electronic data across borders for criminal investigations.

Examples of possible communication activities include:

- Study visits to a law enforcement authority to explain/demonstrate practical problems and difficulties ‘on the spot’.
- Hands-on experience workshops involving practitioners and case studies based on real-life situations that illustrate the difficulties faced by law enforcement and judicial authorities in investigations.
- Member States’ active contribution to the discussions in relevant international fora such as the International symposium on access to data in London in March 2025 or the G7.
- Organisation of an annual seminar by the Member States on access to data following the French initiative launched in 2023.
- Organisation of a conference by the Commission and the Member States to present and discuss the upcoming roadmap to ensure lawful and effective access to data.
- Incorporation of references to access to data for law enforcement in Commission strategies and legislative proposals in the areas of telecommunication, data protection and cybersecurity.
- Establishment of a network on access to data for effective law enforcement like the Camden Asset Recovery Inter-Agency Network (CARIN), emphasising the involvement of the justice, data protection and cybersecurity sectors.

Way forward

Building on the discussion at the Standing Committee on Operational Cooperation on Internal Security (COSI), the Presidency intends to prepare the following points to frame and facilitate an exchange of views at the meeting of the JHA Council on 13 June 2025.

Questions for delegations:

1. Do you agree with the selection of measures that should be implemented in the short term and with the selection of HLG recommendations that the Commission should be invited to prioritise in the upcoming roadmap to ensure lawful and effective access to data?

2. Do you support the proposed communication activities? Are you willing to contribute to or undertake such activities?

3. Do you support the development of key messages for communicating about access to data? Do you agree that, building upon and facilitating the further development of the key messages outlined in the addendum, Europol and Eurojust should be invited to collect relevant case examples and communication products?