Council of the European Union
General Secretariat

Brussels, 11 June 2026

WK 7985/2026 INIT

LIMITE

COSI	**TELECOM**
ENFOPOL	**COPEN**
JAI	**CYBER**
IXIM	**CT**
FREMP	**DATAPROTECT**
CATS	**ENFOCUSTOM**

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

MEETING DOCUMENT

From:	Swedish Delegation
To:	Delegations
Subject:	Non-paper on Lawful Access to Data for Law Enforcement

Delegations are provided in the Annex with a non-paper on lawful access to data for law enforcement for the COSI Support Group meeting on 25 June 2026.

Non-paper on Lawful Access to Data for Law Enforcement

Summary – A call for Action

Across Europe, law enforcement is losing ground as criminals use encryption and anonymisation tools that prevent investigators from accessing essential evidence, leaving victims without justice.

Sweden therefore calls for coordinated EU-wide solutions to ensure lawful access to data while safeguarding fundamental rights, cybersecurity and the security of communications for the users and service providers. Key priorities include:

- **Lawful access by design** – Designing services in such a way that they allow law enforcement to access data in readable format when judicially authorised.
- **Technical and legal alignment** – Secure technical solutions must accommodate privacy, key business interests, national defence and law enforcement needs. Ensuring a high level of cybersecurity in the EU remains a strategic priority.

Crime evolves faster than legislation. The EU must act now to close the gap, without introducing security vulnerabilities or weaknesses in encryption of communications

Lawful Access to Data is necessary

Our societies are facing serious and increasing threats from terrorism and organized crime. The appalling development with gun violence and detonations in public areas and online recruitment of children can never be accepted and must be stopped.

Lawful and controlled access to data is imperative for combating serious crime and is needed in nearly all investigations. However, as organised crime increasingly exploits digital tools for criminal purposes, law enforcement faces growing difficulties. In this new environment, law enforcement needs support by policy and legislation fit for the digital age to be able to do their crucial job.

Without access to digital information in readable format, law enforcement agencies face significant challenges in effectively preventing, detecting, investigating and prosecuting crime. To be specific, in the context of an ongoing investigation or law enforcement intelligence, the absence of accessible and readable data seriously hampers several critical investigative objectives, in particular:

1. To **identify a user** of communication, anonymisation and hosting services.

2. To establish **who** has communicated with whom, **when** the communication occurred, **where** the communication occurred and **how** the communication was conducted.

3. To obtain the **content** of a communication in transit (i.e. live interception) and at rest. This includes, but is not limited to, the text of a message or email, spoken words in a voice call, images, video, or any files exchanged through electronic communication services.

Encryption on the March: Law Enforcement is going Dark

Criminals exploit anonymity, and modern technologies provide unprecedented means for them to conceal their identities and activities. More and more service providers are providing end-to-end encrypted communication services, especially over-the-top (OTT) providers[1] and services providing anonymisation are widely available which is challenging for law enforcement. For the time being, it is mainly content data that is being end-to-end encrypted. However, it is regularly being reported that also metadata is encrypted. Taking into account the fact that OTT services today transmit 97 % of electronic messages, it is evident that law enforcement, lacking access to encrypted data in intelligible format, is becoming increasingly blind.

Accommodating Privacy, Cybersecurity and Law Enforcement needs

All actors in society today rely on cybersecurity, in particular end-to-end encrypted communication services. This includes both governments, private companies, including providers of critical infrastructure, as well as

[1] Definition in Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code - *companies that offer internet-based services over a telecommunication infrastructure that they do not own or manage, including number-independent interpersonal communications services (NI-ICS)*.

individuals. The threat from malicious cyber threat actors is on the rise. Therefore, ensuring a high level of cybersecurity in the EU remains a strategic priority. Strong end-to-end encryption is a cornerstone of cybersecurity and a necessity for a modern digital economy. The actions suggested in this non-paper shall not imply that security vulnerabilities or weaknesses are introduced in encryption of communications. Indeed, it is paramount that our modern society can uphold and maintain secure and reliable communications across the Union and beyond.

All legal, policy, and regulatory measures must safeguard and be in full respect of fundamental rights, avoiding unjustified interference with inter alia the rights to freedom of expression, information, and privacy, and be done without prejudice to fundamental constitutional principles as applied in the national context. The right to privacy is a fundamental right, but not an absolute one. Proportional limitations in this right can therefore be justified by objectives of general interest such as upholding public security and safety as well as justified by the need to protect the rights and freedoms of others, such as victims of crime. Ultimately, accommodating and deciding on the balance between privacy, cybersecurity and law enforcement needs should be determined by democratically elected lawmakers, who are accountable to the public, and in turn the judiciary.

Technologies like end-to-end encryption are vital for secure communication including, but not limited to, protecting sensitive data in e.g. research, innovation and business. They are also imperative from a national defence (both military and civil defence) standpoint. However, while upholding cybersecurity, electronic communications should include mechanisms for exceptional lawful access to uphold public safety and security. In a digitalized world, law enforcement require access to data, including communication metadata and content data, if serious crime is to be pushed back.

Controlled Access to Data

Lawful access must be carefully regulated. Governments should never have unrestricted access to private communications. Law enforcement powers must be used only when necessary, proportionate and legally justified, with strong safeguards, transparency, independent oversight and accountability if powers are abused.

Providers of communication services should be obliged to cooperate with law enforcement when lawful access criteria are met. Non-compliance should result in clear, enforceable sanctions when the service provider can justifiably be held responsible. In relation to hosting services and datacentres, similar obligations to cooperate should be considered in combination with requirements on "Know Your Customer".

Lawful Access by Design

Encryption is a necessary means of protecting the digital security of governments, industry and society as well as a prerequisite for Member States' national defence. At the same time, the European Union and its Member States need to ensure that the ability of competent authorities in the area of security and criminal justice to access data is maintained and developed to be fit for fighting crime in the digital age. Technical solutions and standards that make it possible to maintaining strong encryption and cybersecurity while enabling lawful access to readable data are therefore required. Lawful access should also remain targeted and limited to specific communications.

The Swedish Government supports working towards establishing, in practice and in law, a principle of *"lawful access by design"*. This involves:

- Designing services in such a way that they allow law enforcement to access data in readable format when judicially authorised.
- Integrating legal and cybersecurity requirements into technology systems from the outset, without jeopardising a high common level of privacy and cybersecurity across the Union.

Time for action: Now

We can never accept that law enforcement falls behind in combating serious crime. It is crucial that the legislation and the standards on access to data are up to date in the light of the rapid technological development, changing communication habits and evolving cybercrime. Organized crime is also advancing at an alarmingly fast pace across borders. Firm action at the EU level is needed promptly to tackle the challenges we are facing. Harmonised and up-to-date standards and legal requirements enhance legal certainty and predictability, ensuring a good regulatory environment for business, and a level playing field in which both law enforcement authorities and service

providers clearly understand the conditions and procedures for lawful access to data across the EU.

The work at the EU level has provided a stepping stone…

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. Many Member States are of the view that the recommendations on lawful access to encrypted data in readable format are among the most important to take forward, ensuring at the same time strong information security, cybersecurity and that legal obligations on lawful access are met. The HLG recommended that new obligations, legal instruments, or standards must not require providers to weaken the security of communications by generally undermining or weakening end-to-end encryption. An evidence-based approach and thorough assessment of technical solutions that do not weaken the cybersecurity was recommended.

The standardisation bodies ETSI[2] and 3GPP[3] are at present actively working to assess possible technical solutions in order to allow for the implementation of the principle of lawful access by design. The technology roadmap envisaged by the Commission for 2026, will also provide a valuable contribution to this work that was recognised by a reference to effective access to data for law enforcement purposes in European Council conclusions in June 2025.

… but several steps forward must be taken

To enable lawful access by design for judicial and law enforcement purposes, and to ensure that service providers comply with access orders, we need to pursue as a priority the exploration of both technical and legal ways forward at EU level. Obviously, it will be necessary to pursue the discussion on the need for lawful access to data in various contexts with a view to shed light on the interests at stake, including the risks of widespread impunity and lack of rectification to crime victims unless the legislation is not up to date with the technological development.

[2] The European Telecommunications Standards Institute (ETSI) is an independent standardisation body for telecommunications in Europe.

[3] The 3rd Generation Partnership Project (3GPP) is an umbrella term for a number of standards organizations which develop protocols for mobile telecommunications

In this process, EU's cybersecurity and its position in global digital affairs need to be safeguarded. Further, new measures also need to be considered through the lens of EU's commercial and political relations with key partners.

The objective should be to develop EU-level legislation, building on the principle of lawful access by design, that obliges service providers, including OTT services, to provide law enforcement authorities with lawful access to communications metadata and content data in a readable format when judicially authorised, while at the same time not weakening cybersecurity and the security of communications for the users or service providers. It is essential that the approach remains balanced and does not jeopardise key business interests, European competitiveness and strategic autonomy or military and civil defence interests. In parallel with the legislative work, technical solutions that enable secure and lawful access while maintaining cybersecurity need to be further analysed.