Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 01 July 2025

WK 9150/2025 INIT

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

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

INFORMATION

From:	Presidency
To:	Law Enforcement Working Party (Police)
Subject:	LEWP-P meeting on 11 July 2025: Presidency flash on the new compromise text on the CSA Regulation

Delegations will find attached the Presidency flash on the above-mentioned subject.

Presidency Flash

Friday, 11 07 2025

Annex 1: New compromise text on the CSA Regulation

On 11 May 2022, the Commission presented a proposal for a regulation laying down rules to prevent and combat child sexual abuse[1] (the CSA Regulation). Since then, considerable time and efforts have been devoted to reach a partial general approach in the Council. Six presidencies have worked on the file so far and been close to reaching the necessary support. Most recently, the Polish Presidency presented a compromise text and two subsequent revisions focussing on voluntary detection and strengthening the aspects of prevention. Despite these efforts, no agreement has been reached, while the European Parliament adopted its position in the LIBE Committee on 14 November 2023.

At the same time, Regulation (EU) 2021/1232 (the interim regulation), providing a temporary derogation from certain provisions of the e-Privacy Directive, is set to expire on 3 April 2026. While no proposal for a prolongation has been presented by the Commission yet, the European Parliament's approach to such proposal might be impacted by the progress made in the Council with regard to the CSA Regulation. Without a prolongation of the interim regulation, a legal gap will be created and **voluntary detection by providers will no longer be possible.** Such legal gap might further stimulate the production and dissemination of CSAM.

It is against this backdrop that the Danish Presidency presents a new compromise text on the CSA Regulation aiming to **take into account the views of the Member States, in particular on the provisions on detection orders and encrypted communication,** presented during the last two and half years, while at the same time considering recent political developments inside and outside the Union. It further aims at addressing the fact that the amount of CSAM online has increased significantly in recent years, while technological developments allow for new ways of hiding, creating an obstacle for law enforcement authorities.

The aim of the compromise text

[1] 9068/22.

In accordance with calls of several Member States, the Danish Presidency presents a compromise text that will have **an added value in fighting online child sexual abuse**, while at the same time ensuring the **protection of fundamental rights** and **cybersecurity**.

Based on informal contacts, the Presidency has gotten the impression that it would be very difficult to come up with new approaches that would find support among the Member States. As we are running out of viable options, the Danish Presidency has decided to build upon the largely supported **approach prepared by the Belgian Presidency** in June 2024[2].

Detection orders with strong safeguards

Firstly, the compromise text reintroduces an enhanced **risk assessment** and a **risk categorisation** of services with a methodology for determining the risk of specific services based on a set of objective criteria and leading to the categorisation of 'high risk', 'medium risk' or 'low risk' services. It further reintroduces the possibility of issuing detection orders to services or components of services that are classified as high risk.

To ensure the protection of fundamental rights, the compromise text prescribes that detection orders can be issued **only if a significant risk prevails** after the implementation of risk mitigation measures, as a measure **of last resort** and upon **authorisation by a judicial or independent administrative authority**, following an objective and diligent assessment on a case-by-case basis. With a view to avoiding the imposition of excessive burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned. The issuance of a detection order should further be limited to an identifiable part or component of the service, such as specific types of channels of a publicly available interpersonal communications service, or to specific users or specific groups or types of users, whenever possible. The decision of one Member State to issue detection orders should not affect the jurisdiction of other Member States with regard to investigating and prosecuting criminal offences in accordance with their national law.

The scope of the compromise text in general includes both known and new CSAM as well as the solicitation of children (grooming). However, in line with the approach taken and largely supported during the Belgian Presidency and to protect fundamental rights and ensure proportionality, **detection orders should be limited to detect the dissemination of CSAM and cover only visual content and**

[2] 11277/24.

URLs, while the detection of audio communication and text should be excluded. A **review clause** is introduced for the Commission to assess, within three years of entry into force of the regulation, the availability of technologies for considering the inclusion of grooming in the scope of detections orders in the future.

By deviation from the Belgian approach, the concept of two hits as a precondition for detecting new material (delayed reporting) has been removed for reasons of technical uncertainty, moreover as **strict safeguards already apply to the issuing of detection orders for new material**. Such safeguards include e.g. the **requirement to detect new CSAM in a pseudonymised way**, so that the personal data cannot be attributed to a specific data subject prior to human verification, or the requirement that a **detection order on known CSAM must already have been issued** to the provider prior to issuing one on new CSAM. For reasons of simplicity, technical unclarity and lack of added value, the provisions introducing a sign of reduced risk and simulations tests have also not been included.

Protection of encrypted communication

In order to maintain a high level of cybersecurity and to exclude any possibility of **breaking into encrypted communication**, detection in interpersonal communications services using end-to-end encryption will be possible **only prior to the transmission of content** and **requiring the users' consent** (one-directional client-side scanning). The technologies must in any case be vetted with regard to their effectiveness, their impact on fundamental rights and risks to cybersecurity, and they must be approved by implementing act involving both the Commission and the EU Centre, with specific safeguards applying to technologies for detection in services using end-to-end encryption. The phrasing of the provisions on the protection of cybersecurity has not been amended compared to the compromise texts proposed during the Belgian and Hungarian Presidencies.

Additional changes

In addition to the amendments above, the compromise text entails that **the interim regulation** be extended until 72 months after the entry into force of the CSA-Regulation to avoid any undesired gaps. This would allow for the continuation of the current regime of voluntary detection for the period of transition into the long-term framework and until the Commission has presented its first evaluation of the CSA Regulation.

Finally, the compromise text contains certain elements introduced during the Hungarian[3] and Polish[4] Presidencies based on general support among delegations and with the aim of strengthening prevention and simplifying the text. These amendments entail e.g., the possibility to require providers of high risk services together with the EU Centre to take the necessary measures to effectively contribute to the **development of relevant detection technologies,** the preparation of dedicated **national strategies by the Member States** and a comprehensive communication and outreach strategy by the EU Centre, and the **merger of the provisions on adjusted and additional risk assessment and risk mitigation measures with the provisions on enforcement powers** of the competent authorities.

[3] 13726/24.
[4] 8621/25.