

Translation of [German original document](#)

Classification: RESTRICTED – For Official Use Only

Date: 15 September 2025

From: Permanent Representation of the Federal Republic of Germany to the EU

To: Federal Foreign Office

CC: Federal Chancellery (BKAm), Federal Ministry of the Interior (BMI), Federal Ministry of Justice (BMJV), Federal Ministry of Finance (BMF), Federal Ministry for Economic Affairs and Energy (BMWE), Federal Ministry for Family Affairs, Senior Citizens, Women and Youth (BMBFSFJ), BMDS*

Subject: Meeting of the Working Party on Law Enforcement on 12 September 2025

Purpose: For information

Reference No.: 350.80

Meeting of the Working Party on Law Enforcement on 12 September 2025

I. Summary and Assessment

Agenda Item 3: The basis for the discussion was the revised compromise text transmitted by the Danish (DNK) Presidency on 24 July. Given that the European Parliament (EP) has only indicated it will grant an extension of the interim Regulation on the condition that an agreement is reached in the Council, the Chair announced the intention to continue to seek a partial General Approach at the JHA Council on 14 October 2025.

Numerous Member States that took the floor essentially reiterated their previously known positions and announced that they would provide written comments subsequently.

The Chair requested the submission of written comments and remarks by 19 September 2025 and announced further meeting dates for the Working Party on Law Enforcement (Police) for 09 October, 10 November, and 03 December, without providing specific details on their agenda.

[...]

TOP 3: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (11596/25)

The Chair opened the meeting with a brief summary of the substantive and technical changes made to the compromise text. In addition, the Chair referred to the explanations on this in the Presidency Flash.

Numerous Member States taking the floor (Spain, Germany, Poland, Austria, Hungary, Romania, Sweden, Ireland, Cyprus) emphasized the urgent need to reach an agreement in light of the expiring interim Regulation and announced the submission of written comments (Austria, Poland, Estonia, Italy, Finland, Croatia, Portugal).

Belgium stated that it could, in principle, support the current compromise proposal. The text in its current form was useful and efficient. An adjustment was suggested concerning the accessibility of hits from detection: hits could be held by the respective service provider and only transmitted upon approval by the competent authority or a court, e.g., in cases of pending investigations or complaints. This would also allow detection to take place in an encrypted environment. Belgium will submit text proposals on this matter.

Italy expressed doubts regarding the inclusion of new Child Sexual Abuse Material (CSAM) in the scope of application; additionally, audio communication should be defined more comprehensively.

For **Lithuania**, the protection of fundamental rights was the focus, but at the same time, the compromise proposal should be as ambitious as possible. Lithuania continued to support the proposal.

Estonia noted that the text should be aligned with the Digital Services Act (DSA) regarding age verification (Art. 28 DSA). The Digital Services Act and the General Data Protection Regulation (GDPR) should be explicitly mentioned and referenced in the text. Furthermore, Estonia could not support the changes in Art. 10. Access to encryption must be dealt with at a single, unified point.

Latvia assessed the text positively, but it was still unclear whether it would find political support, as the proposal had received increased political attention over the summer break.

Spain clearly underlined that it continued to fully support the proposal and made it clear that the signals from the European Parliament regarding a possible extension of the interim Regulation were not good.

The **Chair** confirmed that they were very aware of the time pressure and were in close contact with the European Commission and the European Parliament on

this matter. To begin trialogue negotiations, significant progress in the Council was needed.

Slovakia stated that it was still examining the proposal. The focus here was on cybersecurity and fundamental rights. Non-selective scanning of communication was problematic, therefore, positive feedback could not be given at this time.

Czechia expressed doubts about the proportionality of the proposal and announced that it would reject it in the event of a vote.

Poland stated that it still could not approve the proposal and placed a scrutiny reservation. It supported the goal of the CSA Regulation, but not in the way it was formulated in the current compromise proposal. Prevention must be strengthened. In general, they were against anything that questioned data protection and the protection of privacy.

Finland saw the proposal ambivalently; it contained regulations that offered stronger protection, but also problematic provisions.

Bulgaria explicitly supported the proposal, including with regard to age verification.

Austria referred to its already known and unchanged position and announced written comments with further technical remarks. In response to Austria's question about the timeline and further procedure, the Chair referred to the Presidency Flash and reaffirmed the plan to reach a General Approach on October 14.

Germany presented as instructed, maintained its scrutiny reservation, and referred to the still ongoing opinion-forming process within the federal government and the need for a coordinated government position.

Portugal saw the text as going in the right direction. It needed to be re-examined whether all the changes announced in the Flash had already been incorporated into the text. Portugal also noted that the success of the EU Centre would largely depend on how well the regulations fit with the national structures of the Member States.

Hungary maintained its scrutiny reservation but stated it was positive and necessary only for technical reasons. It was further noted that the 3-month deadline mentioned in Art. 24(6) was too long; Hungary proposed "immediately" up to a maximum of 8 days (as did France). The Chair replied that the 3-month

period was based on and adopted from the Network and Information Systems (NIS) Directive.

Ireland supports the compromise proposal, stating it offers significant added value. The additional safeguards ensure a good balance between data protection and child protection.

France showed broad agreement with the current text. It was good that detection orders were included again. It was also welcome that the risk classification and client-side scanning were included. Proportionality was maintained. It was important to ensure human review of hits. France would therefore like to see the "Hit-System" back in the text to reduce the number of false positives. Furthermore, there must be a way to quickly upgrade services to "high-risk" status based on relevant findings. As sextortion is a major problem in France, France advocated for a shorter review period for grooming (18 months instead of 3 years). France also welcomed the certification of detection technologies and the planned extension of the interim Regulation by 72 months.

The **Chair** explained that the Hit-System had been viewed critically by numerous Member States and was therefore removed.

Romania supported the text but would prefer to limit the risk categorization to 2 instead of 3 categories.

The **Netherlands** and **Luxembourg** supported the goal of the draft Regulation but did not agree with the compromise text and referred to their known positions. The Netherlands was also critical of the design of user consent.

Sweden was overall positive and welcomed the re-inclusion of detection orders and encryption. However, they were still examining the compromise text and working on a position. Sweden wondered, however, whether the current wording on End-to-End Encryption (E2EE) could represent a limitation with regard to future technologies.

The **Chair**, regarding the wording of Art. 1(5), referred to the work done under previous Council Presidencies, on which the formulation was based. It was seen as achieving the necessary balance between child protection and the protection of privacy and cybersecurity.

Croatia welcomed the latest changes in the text. However, they wished for a clearer definition of client-side scanning technology and visual content.

Cyprus agrees with the compromise proposal and stated that it would support anything that ensures citizens are safer. The text was going in the right direction. The draft Regulation was a top priority.

The **European Commission**, in response to a question from Belgium, reported that the evaluation report on the implementation of the interim Regulation was in progress and would be presented as soon as possible. Data collection had been difficult and numerous follow-up inquiries were necessary, which explained the delay.

The **European Commission** further stated that, according to the National Center for Missing & Exploited Children (NCMEC), the number of sextortion cases has increased 12-fold. The numbers for grooming and financial extortion have risen extremely. For example, organized crime groups in South Africa and the Philippines have specialized in this. According to NCMEC figures, it must be assumed that this phenomenon has already led to 3,000 child suicides.

Overall, the number of NCMEC reports has decreased by 7 million since the introduction of End-to-End Encryption in Facebook Messenger. However, reports from providers without End-to-End Encryption have increased overall. This clearly shows that encrypted communication must remain within the scope of the CSA Regulation.

On the subject of false positives, it must be clear that realistically, no technology is flawless. However, companies would never use a technology that produces too many false positives. And the EU Centre would not accept or certify one, to prevent being flooded with false reports.

Regarding the procedure proposed by Belgium, the **European Commission** stated that it would be practically unmanageable to store the hits exclusively with the provider at first. How would law enforcement become aware of them? It could not be accepted that children are being abused and providers have corresponding evidence, but this only comes to light if an investigation is already underway. This was absolutely unacceptable.

The **Chair** concluded by requesting the submission of written comments and remarks by September 19, 2025, in preparation for the (partial) General Approach at the Justice and Home Affairs (JHA) Council on October 14, 2025.