



Brussels, 7 June 2024  
(OR. en)

10666/24

---

---

**Interinstitutional File:**  
**2022/0155(COD)**

---

---

JAI 939  
ENFOPOL 276  
CRIMORG 90  
IXIM 149  
DATAPROTECT 231  
CYBER 182  
COPEN 296  
FREMP 284  
TELECOM 202  
COMPET 616  
MI 572  
CONSOM 209  
DIGIT 151  
CODEC 1431

## NOTE

---

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Progress report

---

## I. INTRODUCTION

1. On 11 May 2022, the Commission adopted the above proposal<sup>1</sup> accompanied by an impact assessment and a communication. The proposal is based on Article 114 TFEU and has two main building blocks. First, online service providers, such as providers of hosting services and interpersonal communication services, would be obliged to prevent the dissemination, detect, report and remove child sexual abuse material ('CSAM'), and to prevent, detect and report the solicitation of children ('grooming'). Second, a new decentralised EU agency (the 'EU

---

<sup>1</sup> 9068/22.

Centre')<sup>2</sup> would be set up to support the implementation of the proposed Regulation, together with a network of national Coordinating Authorities and other competent authorities.

2. In the Council, the proposal has been examined in 31 meetings of the Law Enforcement Working Party - Police (LEWP-P) so far to prepare a mandate for negotiations with the European Parliament.
3. The Council Legal Service issued a written opinion on 26 April 2023<sup>3</sup>.
4. The Permanent Representatives Committee had policy debates on the above proposal on 31 May and 13 October 2023, focussing on the scope of the detection order and aspects related to encrypted communications and cyber security. The Council also discussed the issue in public session on 19 October and 5 December 2023.
5. In the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) is the lead committee for the negotiations on the proposal. It appointed MEP Javier Zarzalejos (EPP, ES) as rapporteur in October 2022. The LIBE Committee adopted its report on 14 November 2023, and the position of the European Parliament was deemed adopted on 22 November 2023.
6. Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 extends until 3 April 2026 the period of application of the temporary legal framework on child sexual abuse foreseen in Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

---

<sup>2</sup> The selection of the seat of the EU Centre will be subject to an inter-institutional procedure following the example of the selection of the seat of the Anti-Money Laundering Authority.

<sup>3</sup> 8787/23.

## II. PROGRESS OF THE WORK DURING THE BELGIAN PRESIDENCY

7. Under the Belgian Presidency, the LEWP-P has devoted considerable time and efforts to consider new approaches to the proposed Regulation and to draft compromise texts at the meetings on 1 March<sup>4</sup>, 19 March<sup>5</sup>, 3 April<sup>6</sup>, 15 April<sup>7</sup>, 8 May, 24 May and 4 June 2024<sup>8</sup>.
8. The Presidency concentrated its efforts on responding to concerns expressed by some delegations regarding the proportionality and targeting of detection orders and related to cyber security:
  - The Presidency suggested two interlinked building blocks: (1) enhanced risk assessment and risk categorisation of services to make detection orders more targeted and (2) protecting cyber security and encrypted data, while keeping services using end-to-end encryption within the scope of detection orders.
  - Subsequently, delegations worked on developing a methodology for determining the risk of specific services based on a set of objective criteria (related to the size, type and core architecture of the service, the provider's policies and safety by design functionalities and a mapping of users' tendencies).
  - Following the outcome of this risk categorisation process, systems or parts thereof would be classified as 'high risk', 'medium risk' or low risk'. Based on this categorisation, additional risk mitigation measures could be imposed on the providers classified in the medium and high-risk categories. In case significant risks still prevail after the implementation of the additional risk mitigation measures, the Coordinating Authority could consider requesting the issuance of a detection order as a measure of last resort to services that are classified as high risk. Providers could also flag voluntarily to the Coordinating Authority of establishment whether they have suspicions of their services being used for child sexual abuse that might require issuing detection orders.

---

<sup>4</sup> 6850/24.  
<sup>5</sup> 7462/24.  
<sup>6</sup> 8019/24.  
<sup>7</sup> 8579/24.  
<sup>8</sup> 9093/24.

- The Presidency proposed to keep services using end-to-end encryption in the scope of detection orders issued to high-risk services, under the condition that this would not oblige providers to create access to end-to-end encrypted data and that the technologies used for detection are vetted with regard to their effectiveness, their impact on fundamental rights and risks to cyber security.
  - Following discussions at technical level, the Presidency has adjusted its approach and suggested adding further safeguards to ensure proportionality and the respect to fundamental rights, namely the limitation of the scope of detection orders to visual content and URLs, the delayed reporting after two hits of new child sexual abuse material to reduce false positives, the pseudonymisation of detected new child sexual abuse material prior to human verification, and the protection of end-to-end encrypted data while enabling detection in interpersonal communication via upload moderation requiring users' consent.
  - The Presidency also endeavoured to clarify that detection should not apply to accounts used by the State for national security purposes, maintaining law and order or military purposes.
9. The Presidency noted at the LEWP-P meeting on 4 June 2024 that there was no need to continue the examination at technical level, as all technical questions had been addressed in a comprehensive way.
  10. The Presidency is committed to reach a compromise and intends, following the presentation of the progress at the Council on 13 June 2024, to issue a compromise text and subsequently to invite the Permanent Representatives Committee to agree with a partial<sup>9</sup> negotiation mandate.

### III. CONCLUSION

11. The Permanent Representatives Committee/Council is invited to take note of the progress of the work of the Presidency on the Regulation laying down rules to prevent and combat child sexual abuse.

---

<sup>9</sup> "Partial" because the selection of the seat of the EU Centre is excluded.