Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 17 June 2026

WK 8875/2026 INIT

LIMITE

ENFOPOL	**FREMP**
JAI	**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.

NOTE

From: To:	General Secretariat of the Council Delegations
N° prev. doc.:	9659/26
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations

Delegations will find attached the compilation of comments received from Members States on the abovementioned proposal following the JHA Counsellors (CSA Regulation) meeting on 10 June 2026.

Written comments submitted by Member States

Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

(9659/26)

Contents

BULGARIA

Bulgaria would like to thank the Presidency for the efforts made.

Regarding the circulated document, we would like to express the following comments:

Regarding point A **"Scope"** and in particular detection/searches Bulgaria remains of the opinion that the scope of the search should be as broad as possible, as in cases of newly created content and solicitation, because it is usually the victim who is being abused in real time.

Regarding point B **"Definitions"**, lBulgaria is of the opinion that with regard to "content that is publicly accessible", such content could be considered everything that is publicly accessible on the Internet that does not require special access. Content in public forums that are publicly accessible and only require registration by a user should also be considered publicly accessible.

Regarding point C **"Own-initiative searches on content that is not publicly accessible – Article Z"** we are of the opinion that voluntary detection should include the widest possible scope, due to the arguments mentioned above, also reflected in our previous positions. We can support the implementation of proactive searches by hosting service providers as well.

Regarding point D **"Detection orders for content that is publicly accessible – Article X"** there are no obstacles for such orders to be regulated. It should be noted that organizations associated with INHOPE carry out daily searches for such content and provide reports to the competent services of the Member States. The problem with this content is its reappearance, sometimes within minutes, after removal, on the services of another hosting providers.

Regarding point E **"Detection orders for content that is not publicly accessible – Article Y"** and in particular the term "specific user", such an order would have practical value in cases where there is insufficient evidence for a specific person and it is necessary to control the user in order to confirm the illegal activity. The specification of a user account and possible duplication could be problematic in cases of voluntary detection at the initiative of a provider. Usually, after identifying a user, as a result of voluntary detection, the account is deleted, as it violates the rules for using the relevant service. In the case of regulating such orders, the scope should also be as broad as possible.

Regarding point F **"Searches by the EU Centre – Article 49"** Bulgaria is of the opinion that the added value of EC searches could be the acquisition of data on the customers of hosting service providers and their analysis with a view to taking measures by the relevant competent services. The scope of the searches should be as broad as possible.

Regarding point G **"Common provisions"** and in particular technology auditing, we believe that it should be independent, as this will ensure greater public trust in technology.

CROATIA

Article 66: Technology Committee - Lines 840-848b

HR considers it important that each MS be represented on the Technology Committee and regards this issue as a red line. *Earlier versions of the text concerning the Technology Committee envisaged the nomination of two members per Member State, whereas the current drafting refers to a maximum of 15 members.* ***Further clarification is therefore requested regarding the exact scope and interpretation of Article 66(1).***

A. Scope of the detection/searches

Child grooming represents a significant risk to children and its complete exclusion from the scope of the Regulation would substantially diminish the Regulation's effectiveness in ensuring a high level of child protection.

In our view, the exclusion of child grooming from the scope of the Regulation could only be accepted as a measure of last resort in the context of an overall compromise.

At the same time, the issue should be reviewed at a later stage, with a view to reconsidering the inclusion of child grooming within the scope of the Regulation.

B. Definitions

HR could show flexibility with regard to limiting the approach to defining only "publicly accessible content", as well as regarding the proposed wording of its definition.

C. Own-initiative searches on content that is not publicly accessible – Article Z

HR could support a permanent derogation as proposed. HR could also support the application, by analogy, of the same rules and safeguards as those applicable to providers of number-independent interpersonal communications services.

In our view, limiting the scope of content subject to own-initiative searches to known CSAM only would not be sufficiently effective from a child protection perspective. Own-initiative searches should enable service providers to ensure child safety effectively on their services and should therefore cover all forms of CSAM, rather than only known CSAM.

HR can also show flexibility with regard to the wording of Article Z.

D. Detection orders for content that is publicly accessible – Article X

HR could support the conditions for issuing the order under Article X. HR could show flexibility with regard to the issuing authority, including allowing independent administrative authorities, in addition to judicial authorities, to issue such orders.

HR would however appreciate clarification on how it is envisaged that an assessment would be carried out as to whether a publicly accessible service is being misused, i.e. whether it contains CSAM. The text indicates that "the order can be issued if there is content online, something that can be verified by national authorities".

In this context, it is unclear whether national authorities would be expected to proactively verify such content, or whether action would be triggered on the basis of notifications from citizens, institutions or other sources.

HR would also appreciate clarification on which authority would carry out such assessments. We would like to emphasize that, under Croatian national law, access to such content for the purpose of conducting investigations may only be undertaken by competent investigative authorities.

E. Detection orders for content that is not publicly accessible – Article Y

HR would underline that each Member State should be able to decide which authority is the competent issuing authority.

On the approach for non-public content, allowing own-initiative searches but mainly targeting known offenders, this could in practice discourage providers from using own-initiative searches and lead them to rely mainly on detection orders.

The conditions for issuing orders, including linking a user to CSAM or grooming and prior misuse within the last 12 months, largely follow an investigative logic used in national criminal law for targeted cases.

It is not clear how Member States would be expected to demonstrate such misuse within a 12-month period. Overall, this could limit the preventive role of providers and reduce the effectiveness of the framework for protecting children online.

F. Searches by the EU Centre – Article 49

HR could support giving the EU Centre the power to conduct own-initiative searches on publicly accessible content, to complement providers' detection and searches.

If the EU Centre is granted such powers, they should not be limited to "known" cases only. However, we could show flexibility in the context of reaching an overall compromise.

HR could also show flexibility on other issues related to the use of technologies that meet the requirements of Article 10 when conducting such searches.

G. Common provisions

HR strongly support that the **EU Centre** plays a significant role in assessing whether available technologies are suitable for CSAM detection, and we strongly support cooperation between service providers and the EU Centre in the development of future technologies.

ESTONIA

Section A

In regards to flexibility concerning the appropriate scope of application for each of the components our red lines are E2EE and the general obligation to monitor. We should especially be careful with grooming detection because grooming detection tools remain seriously unreliable. As known, the process of detecting grooming is generally the most intrusive for users as it requires automated review of text transmitted in interpersonal communications. However we remain flexible with the scope matter if technological solutions ever emerge that do not undermine end-to-end encryption and do not create a general obligation to monitor.

Section B

On page 3, it is mentioned that there is no definition for „non-public content“ as PRES proposes that all content that is not covered by the definition of ‘content that is publicly accessible’ and that is not encrypted would fall into this category. We note that for legal clarity, there should be a definition for „non-public content“.A separate definition would help establish clearer boundaries between the two concepts and reduce the risk of divergent interpretations across Member States.

Section C

In regards to section C and own-initiative searches. Based on the information provided in this document, we do not see any added value in this proposed approach, and as usual we certainly cannot agree to any approach that undermines E2EE.

On page 4, it is mentioned that (a) that providers would have to inform the EU Centre in advance of conducting own-initiative searches, and (b) national authorities would be able to suspend any own—initiative search activities by providers if they consider that the conditions of the Regulation are not met. On page 13, Article Z (c) establishes that this must be done [5 days] in advance. What is the added value of said administrative burden (requirement for the provider to inform EU Centre)? Especially if coordinating authority or data protection authority [subject to discussions – as we understand] is the one who does supervision on the „own initiative searches“, not EU Centre (see Article Z+1). Also regulation 2021/1232, which is now repealed, did not include such a requirement. Detection is an automated part of the service workflow, but based on the general wording, it could also be interpreted to mean that virtually every action performed by the systems must be reported in advance, which is not realistic. In general, if the coordinating authority oversees voluntary measures (Article Z+1), why is it necessary to notify the EU headquarters?

Article Z+2 – Article 7 of the DSA does not distinguish between public and non-public content in the context of voluntary scanning by intermediaries, nor does it impose any restrictions on the voluntary scanning of non-public content. It is unclear whether other legal acts impose restrictions on such activities. Establishing clear safeguards here seems reasonable.

Given that many of these providers of number-independent services are registered in the U.S. and that many will continue to operate even after April 2026 following voluntary self-identification, why should they notify the ECA of their voluntary self-identification, and to the CAs as well (e.g., should VLOPs such as META applications notify Ireland that they are conducting searches on their own initiative)? Is this notification intended as information or an indicator to ensure compliance with the provisions of Article 10, assuming that service providers operating in the EU have the relevant technology (reference to Article 50, including regarding small and micro-enterprises)?

On page 4 there are questions: Delegations are invited to consider whether they could show flexibility on the scope of the derogation. Specifically, delegations are requested to indicate whether they would be ready to accept a reduced scope regarding the content that is subject to own-initiative searches, for example only for known CSAM, and whether they could agree to allow hosting service providers to conduct such searches on content hosted on their services that is not publicly accessible as part of a wider compromise package.

We presume that "content that is not publicly accessible" can also entail content that is encrypted. If it is so, then for Estonia, it is a red line if while doing the „own-initiative searches", the encryption is being broken or that there is essentially a requirement to have a backdoors to encrypted content. Hence, how does this aspect correspond to proposed Article 1 paragraph 4a?

Section D

We support an approach where the order is issued independent administrative authorities to reduce the administrative burden on the courts. As noted (page 5), the European Parliament may favour a model requiring judicial decision. However, given the potentially significant number of requests and the need for efficient handling, requiring all orders to be issued by courts could create a considerable administrative burden and lead to delays. Independent administrative authorities could provide an effective alternative, on condition that appropriate safeguards and judicial redress remain available.

This is regarding public content and its detection order if a hosting service (or part of the service) is being misused for online child sexual abuse to an appreciable extent. There is no reference to any residual risk, since the order can be issued if there is content online, something that can be verified by national authorities. The order would contain the period of application, the information necessary for the provider to be able to execute the order and information regarding appeals. There is also a clarification that these provisions should not lead to a general monitoring obligation. But if said order is done, how in practice can it be made sure that there this order would not lead to a general monitoring obligation? Is it done by a) the requirement to have a period of application and b) the specific national authority that issues said order? Also, should other articles about detection orders also have the same requirement as in Article X (3) (content: The application of this article shall not lead to any general *monitoring obligation*.) ? Additional question: why are Article x (3) and Article Y (4) a bit different? Should they be aligned?

Articles X, X+1, Y, Y+1 – as with other arrangements, there is no need for a coordinating authority to intervene in the process. It would make sense for the competent authority to be the issuing authority or, at the very least, the requesting authority.

Article X – 2. A public content detection order shall only be issued if the service or part of the service is being misused for [online child sexual abuse] to an appreciable extent – this is too general; there should be more specific criteria to define what constitutes an "appreciable extent." Orders should be as targeted as possible and directed at services or parts of services where the violations are of a significant scale, recent, and verifiable.

It is also necessary to assess the impact of complying with such an order on the overall risk level of the service or part thereof—we see a risk that, otherwise, new detection orders could continue to be issued for a single service as soon as the deadline for the previous one expires. This would essentially turn a temporary measure into a permanent obligation, which would lead to an increase in the administrative burden and is also inconsistent with the principle of legal certainty.

Further more a question related to article X. To whom should the detection order be addressed if the HSP data centers are located in the relevant EU Member State, but the service provider itself is located

in a third country? Or if the HSP is established in the relevant EU Member State or operates there only on paper, while its actual operations and personnel are located elsewhere, at an unknown address?

Section E

We believe that the scope should be narrowed in light of technological developments. As said before in section A that we should especially be careful with grooming detection because grooming detection tools remain seriously unreliable We support that the detection order for non-public content could be issued by all Member States. However If only the MS in where the provider is established, has said power, then how can other MSs "use" the same measure? The suspected individual might not have connections to the MS where the provider is established. Is it to make sure that the order can be enforced by said authority that is in the same MS as the provider?

Article Y, paragraph 2 – At first glance, targeting the regulation at specific users seems reasonable, since there must be grounds for suspicion in the case of non-public content, as one cannot stumble upon CSAM by accident. As for the explanatory note accompanying the article (p. 6) the reasoning related to criminal proceedings does not sound particularly convincing. If there must be grounds to link a specific user to child abuse in order to issue an order, then why shouldn't the initiation of proceedings be a prerequisite for the order? The timeframes for the orders (24 months for CSAM/12 months for grooming) also raise questions. Long before these deadlines, it should be clear whether CSAM distribution or grooming is taking place or not—I don't see how it could be legally acceptable to monitor someone's private communications or content for up to two consecutive years if the initiation of proceedings is not a prerequisite. The same issue arises here with repeated orders.

This article likely refers to certain types of users whose behavior exhibits recognizable patterns—for example, in practice, platforms have done a great deal of work on their own, including in collaboration with law enforcement agencies, to address actions that endanger children and prevent serious harm. Although criminal proceedings are generally initiated based on such information, pieces of the puzzle must be put together to initiate proceedings (since offenders use measures to conceal their actual location and identity, hierarchical communication, etc.). There are also examples where anomalies have been detected in which there is no "offender" to be found. In criminal proceedings, evidence is collected based on the provisions of the Code of Criminal Procedure and the general principles of the Civil Code, not through an identification order. Or, as stated in the text/addition to Article 1, and it is worth noting: The Regulation does not limit the application of Union law in the field of cooperation in civil and criminal matters, nor does it limit the application of national law in civil and criminal matters.

We understand that this aspect is about detection orders for content that is not publicly available and that this is the "non-public content" mentioned at the start of the document. Said possible definition (see page 3) mentions that this content also entails non-encrypted data. And that this detection order is a about specific users. What is meant by "specific users"? Are they specific individuals? Or can they be classified on a more general level, e.g. by in a way that they have a specific characteristic or activity that is common for them all?

The text also mentions that the order could also have information on appeals and it is in Article Y+1 (4) (c). Who can appeal here? The provider? Not the relevant user? Is said aspect covered by Article) (on pages 18-19)?

Section F

Since the exact organizational structure of the EU center is currently unclear, it is difficult at this point to envision who would oversee its operations. What is clear is that the center's work should facilitate the work of member states, not burden them. From Estonia's perspective, the activities of the EU Centre should provide clear added value and support the work of Member States rather than duplicate

existing national efforts. It is important to avoid overlaps between the tasks carried out by the EU Centre and those already performed by competent authorities at national level, as such duplication could create unnecessary administrative burdens without corresponding benefits. In addition, it is important that the requirements regarding the use of technology be the same as those for service providers, including requirements relating to necessity, proportionality, reliability and the protection of fundamental rights.

Scanning of public content by the EU Center (amendments to Article 49) – in principle, there is no objection; for example, market surveillance authorities already routinely use web scrapers to identify dangerous products.

"The notification shall also clearly state that it is for the provider's voluntary consideration" – the wording in the document is unclear, but the key point is that the service provider can decide whether to act if the EU Center's notification includes a request for removal. It cannot be voluntary for the service provider to decide whether to review a notification regarding potentially illegal content at all.

What happens if the service provider does not remove the content, restrict access, or notify the EU Center—does this trigger a request for a discovery order (and who makes the request)?

While the general rule appears to be that the EU Centre informs the provider of its findings, it is unclear how the exception would operate in practice. In particular, it is not clear how the competent law enforcement authority would become aware of the findings in time to request that the provider is not notified. Further clarification of the coordination mechanism between the EU Centre and law enforcement authorities would be welcome.

Section G

Article 10- The issue of consent. In this version, it simply states that users must be informed, but is that acceptable even if the content isn't end-to-end encrypted (E2EE)? As we recall, obtaining consent was a very heated topic in the Council's discussions, as was the question of whether it could be addressed through the terms of service. If I don't agree to content scanning, do I have to give up the service?

Article 11- Guidelines, EU-wide risk assessments/trends are also available to the public.

On Article 50(1), there is the question: (a) Whether the technologies should be independently audited (as the EP mandate indicated)? Who would pay for these audits? On page 20 about Article 10, the paragraph 4 mentions: If said technology falls under the cyber resilience act (Regulation (EU) 2024/2847; the CRA), then could said framework provide an answer to said question? Especially when taking into account that CRA applies to products with digital elements, that also includes software. This should be further looked into, especially when taking into account the proposed Article 50 on page 23.

Page 11, Article 49 It mentions that European Data Protection Board [EDPB] shall issue guidelines regarding the compliance with GDPR […] that are used by the EU Centre to conduct the searches referred to in paragraph [1]. But EU Centre is an EU Body/authority – the GDPR does not apply to it. For said authority, the EUDPR applies. Hence – why are EDPB and GDPR mentioned here?

Page 12, article 49 It mentions that The notification shall also clearly state that it is for the provider's voluntary consideration. But at page 8 it is mentioned: The reports resulting from own-initiative searches by the EU Centre should be treated by the provider in the same way as reports from the public, meaning that the provider would be obliged report it back to the EU *Centre in accordance with Article 12 and 13 of this Regulation and, potentially, remove the reported content or disable access to it where it finds it to be incompatible with its own terms and conditions. The Article and its explanation do not match – what is the envisaged outcome for that situation?*

Page 12, Article 49 Paragraph 3 mentions that if a competent law enforcement authority of a MS requests it, then EU Centre shall suspend the notification to the provider in question. How can/does the EU Centre know that it has to suspend the notification?

Page 13, Article Z regarding the (a) The processing is:

i. strictly necessary for the use of specific technologies for the sole purpose of searching for [online] child sexual abuse/[material] and reporting it in accordance with Article 12; …

iii. limited to content data and related traffic data that are strictly necessary for the purpose set out in point (i);

How are said provisions (especially iii) in compliance with the fundamental right to privacy?

Pages 18-19, Article 9 paragraph 1 also mentions that "users concerned by the measures taken to execute [order], shall have a right to information and effective redress". But how can the concerned users even know that their activities are monitored due to detection order? Also, if a concerned user finds out about the detection order, then could this also hinder criminal investigation?

Page 23, Article 50 Is the EU Centre's task to provide a list of the technologies and their manufacturers? Or is EU Centre also a manufacturer?

FINLAND

Definitions

Content that is not publicly accessible

FI: This definition is broad, covering a variety of functions that are protected to varying degrees. It appears to cover restricted but partially accessible social media pages, as well as various restricted discussion groups and confidential bilateral communications. Although the protection afforded to the confidential communications is broad and may also extend to traffic data, the content of communications intended to be confidential is protected differently from, for example, communications within a group that may include tens of users or partially accessible social media pages. Currently, these distinctions are not reflected in the text of the regulation, although considerations relating to fundamental rights may also vary significantly depending on the type of non-publicly accessible material being detected.

X Article

Detection orders for content that is publicly accessible

Generally, the detection of CSA material in publicly accessible content raises significantly fewer fundamental rights concerns, provided that it is limited in scope and it complies with Article 8 of the DSA.

In light of the case law of the Court of Justice, such detection orders if imposed to hosting service provides should be limited to the detection of content—particularly known CSAM—that does not require an independent assessment by the providers and may be carried out by automatic means (C-18/18, *Glawischnig-Piesczek*, paras 34–35, 37, 45–47).

In order to ensure that it satisfies the criteria for specific monitoring obligations and does not constitute a prohibited general monitoring obligation, the text of the regulation should be further specified and clarified.

For the obligation to be sufficiently precise, it is not sufficient merely to state that "the application of this article shall not lead to any general monitoring obligation".

Moreover, it should be clarified what its legal effect is and how it relates to the removal order. In particular, it remains unclear what occurs once the content has been identified, and what added value this provides in comparison with the obligation relating to the removal order, under which equivalent and identical content would likewise be subjected to removal.

Z article

Own-initiative searches by providers in content that is not publicly accessible

Finland recognises the importance of voluntary measures for the protection of children online. Voluntary detection has played an important role in identifying and reporting CSAM. However, FI also notes that voluntary detection does not remove all relevant fundamental rights concerns related to detecting particularly content protected under the confidentiality of communications.

In this regard, from the perspective of the necessity and proportionality assessment of voluntary detection, it is particularly important to determine whether such detection would also interfere with the content of communications and what safeguards are provided in the regulatory framework to prevent it from becoming overly broad and insufficiently specific with regards the detection of communication content.

Article 3 (1) (b) of the interim regulation (EU) 2021/1232 states that *to the extent that they are used to scan text in communications, **they are not able to deduce** the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse*. This wording is clearer than that of Article 10(5)(b) of the CSA proposal: *not allow for the acquisition of knowledge of the content of the communications or any information from the relevant communications other than that which is strictly necessary for the purpose referred to in paragraph 1, including patterns pointing to [online] child sexual abuse/[material], as applicable*. The wording should be formulated that inferring the content of these confidential messages is prohibited, both in voluntary and possible obligatory detection.

Article Y

Detection orders for content that is not publicly accessible

The detection order to not publicly accessible content is targeted to specific users. However, the scope of this group of users remains unclear. In particular, it is uncertain whether the users must be individually specified, or whether such measures may be directed at a defined closed group comprising a potentially large number of users, or at a specific part of a service, without applying to all users. This could still potentially result in a very broad and proactive detection of a large, if not entirely unlimited, number of users.

The phrase 'clear indications, based on information lawfully acquired' requires specification. Moreover, according to Article 52 (1) of the EU Charter, any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law. This thus limits the extent to

which the scope of a restriction on a fundamental right may be determined primarily by the recitals, particularly if this regulation possible also concerns the essence of certain fundamental rights.

Finland considers that, in its current wording, the term 'clear indications, based on information lawfully acquired' leaves the scope of its application rather open, as well as the criteria for what constitutes a sufficient basis for issuing a binding detection order. It also seems that it is mainly service providers, not public officials, who initiate this process, and thereby potentially define the persons at whom a binding detection order should be directed. In particular, it is unclear whether a binding detection order could be based, for example, on a report by an individual user concerning potentially unlawful content, in which case the threshold would appear to be relatively low.

First of all, any interference in the confidentiality of communications must, according to the necessity criterion, must be as targeted and limited as possible. In assessing the proportionality of the restriction, relevance should be given, inter alia, to the closeness and nature of the person's connection to the criminal activity forming the basis for the restriction (cf. Szabó and Vissy v. Hungary, 12 January 2016, paras 67 and 89; judgment in Tele2 Sverige, C-203/15 and C-698/15, paras 105 and 119; judgment in Prokuratuur, C-746/18, para 50). It is relevant how serious and extensive the restriction on fundamental rights is, and, conversely, how serious a threat the exercise of powers is intended to prevent. It is doubtful whether, for example, a report by a single user concerning potentially unlawful content, or other similar lawfully obtained information, would suffice to meet the threshold and the required connection to serious crime as laid down in the aforementioned case law, such as the requirement of an objective evidence how the target a possible detection order (see Tele2 Sverige, para 111 and 119).

Therefore, further clarification is required in order to analyse, whether a binding detection order issued to not publicly accessible material entailing potentially also the content of private messages is line with the criteria set out in the case law of both CJEU and ECtHR.

Given that the content of electronic communications may form part of the very essence of Article 7 of the Charter (see judgment in Digital Rights Ireland, C-293/12 and C-594/12, para 39, Tele2 Sverige, para 101), it is particularly unclear, considering the technology available, whether the detection of grooming is feasible without deducing the substance of the content of communications. This would require further elaboration.

The proposed targeting of detection orders seems to move close to the logic of criminal investigations, especially where the measure would be based on clear indications relating to specific users or groups of users. This raises a question about the relationship with existing powers of law enforcement and judicial authorities, and whether the new mechanism could create a parallel or overlapping framework with different safeguards and thresholds.

In line with the Council's Legal Service's comments, we would also like to receive further clarification on how the issuance of detection orders operates territorially, and to what extent a single authority may issue such an order in a way that could potentially target users across different countries.

Article 10

Article 10(5)(b) of the proposal should be drafted in more stringent terms to ensure that the technologies used are not able to deduce the content of communications but are solely capable of detecting patterns indicative of potential CSAM or grooming, if it is added to this regulation. The wording of Article 3(1)(b) of the interim Regulation (EU) 2021/1232 appears to be clearer in this respect.

Moreover, the phrases “in accordance with the state of the art” in Article 10(5)(c) and “sufficiently reliable” in Article 10(5)(d) require further clarification.

More generally, the criteria applicable to the technology are formulated in broad and general terms, which raises the question of how a court is able to assess the functioning and proportionality of such technologies, and thus ultimately the scope and application of the limitation of fundamental rights, taking into account that, under the proposed Article Y(2)(c), a detection order must be necessary and proportionate and must outweigh any potential negative effects on the various fundamental rights that may result, for example, from the use of certain technologies.

FRANCE

General comments

The French authorities are concerned about the great complexity of the proposed arrangements and mechanisms/procedures, which, taken as a whole, seem difficult to implement and are not well adapted to the temporalities of the operational services.

On detection orders:

- With regard to the comment procedure:

In particular, they find it difficult to understand the usefulness of the commentary procedures provided for in Articles X+1 (paragraphs 1(a) and (b)) and Y+1 (paragraphs 1(a) and (b)) and highlight the excessively cumbersome nature of those procedures, but also recall that the legitimacy of the detection order is already fully ensured by the fact that a judicial authority or an independent administrative authority issues that measure.

Furthermore, that procedure questions the procedure to be followed in the event that the Centre and/or the supplier considers that the infringement found does not justify the introduction of a detection measure. Should the national authority abandon/relinquish the request for an injunction even though it is aware of the commission of one or more offences on a platform? This does not seem to be consistent with risk assessment measures and difficult to conceive for operational services engaged in the fight against child crime online.

In line with the above, we are surprised that the risk assessment and categorisation procedures provided for in Article 3, which normally constitute the starting point for the implementation of preventive measures, are not included in the proposed compromise. At first sight, it seems simpler and more consistent to make the issuing of draft injunctions conditional on the assessment of a risk associated with a given service. If this cannot apply to Article Y, this approach would significantly simplify the procedures proposed in Articles Z and X.

The French authorities also alert the Presidency to the fact that the proposed arrangements appear to be very demanding in terms of human resources, both on the Centre's side and on the side of suppliers and national competent authorities.

- *With regard to the duration of injunctions:*

Also with regard to detection orders, the French authorities question the relevance of including dates for the start and, above all, the end of the order (Article X(3)(a) and Article Y(4)(a)). It does not seem to be within the competence of the Coordinating Authority or the Issuing Authority to pre-determine how long a service is likely to present a risk. Moreover, limiting these injunctions in time is not adapted to the criminal phenomenon, whose movements and developments are unpredictable. The French authorities therefore consider that, once a risk has been identified on a service (as part of the risk assessment procedure in Article 3), the lifting of the detection order (which is a measure to mitigate and prevent those risks) should be conditional on the provider demonstrating that the risk no longer exists on its service.

- *With regard to future amendments to the forms:*

Finally, we support the principle of adapting the forms to the technologies available by means of delegated acts (Articles X+1(4) and Y+1(5), which refer to Article 86). However, they hope that the Member States may also be able to ask the Commission to initiate this revision procedure, if necessary.

The concept of reference indicators:

As regards the relationship between this compromise and the rest of the text, we would like to return to the reference to the ‘reference indicators’ for issuing detection orders, provided for in Article 44. This article provides for "indicators to detect the dissemination of child sexual abuse material not previously detected and identified as constituting child sexual abuse material in accordance with Article 36(1); and indicators to detect the solicitation of children (see Article 44(1)(b) and (c)). However, the French operational services question the concept of indicators applied to those purposes. In practice, there are simply no pre-established indicators to detect unknown content or grooming phenomena. Furthermore, it is not possible to use rigid lists of indicators, as online child crime is evolving very rapidly.

Currently, according to its own methods, in particular through artificial intelligence-based tools allowing for example to identify certain weak signals (such as the percentage of skin visible in an image), then to exclude content clearly involving adults, etc. There are currently no standardised indicators. Thus, it is a set of elements (beam of clues) that makes it possible to detect content representing sexual abuse of minors. This leads to the generation of an alert, which is then subject to human verification in the competent service of the receiving Member State. The same logic

applies for textual content, which is systematically analysed in relation to the context associated with the alert.

In the light of these elements, we would ask the Presidency to explain what these indicators would consist of in practice and how they could be operationally defined and used.

We would also point out that the Centre's indicator base cannot be the sole reference base. As the French authorities have pointed out on several occasions, Interpol's ICSE database (which is funded by the European Commission) remains the world reference in the field and the only international database identifying the hash of paedo-docriminal content to date. Due to the cross-border nature of online paedocrime, it is necessary to rely on Interpol's ICSE in order, in particular, not to miss out on content already known outside the EU.

On voluntary detection:

- **Voluntary detection - as a risk prevention measure that has proven to be effective - must be preserved and cover a wide range of content, as allowed by the derogation regime. We therefore reiterate our commitment to a voluntary detection system based on a broad scope of application that is consistent with the operational challenges of identifying perpetrators and the need to preserve the physical integrity of minors. They also point out that the establishment of a system of detection orders for service providers seems to them compatible with the use of voluntary detection as a risk mitigation measure. These two approaches are not mutually exclusive and can usefully be combined. Since the spirit of the proposed text is to improve the fight against and prevention of online sexual abuse, it would be inconceivable that the text of the perennial regulation could be less effective than that of the derogating regulation.**

A. Scope of the detection/searches d'application de la détection / recherche :

The French authorities may first of all reiterate the need **to keep (new) unknown content within the scope of detection and indicate that they do not have any margin of flexibility on this point.** Indeed, an overwhelming majority of perpetrators of child sexual abuse detected online are identified from new or unknown content. Moreover, in the majority of cases, this content is the only vehicle for investigative services to identify content producers – that is, abusers in contact with minors, who film and broadcast their crimes. Their detection is, in that respect, a priority, since it determines the possibility of identifying victims and interrupting ongoing offences.

On the other hand, 'known' content corresponds to material that has already been reported and, for the most part, has already been brought before the courts. Where the initial investigations did not identify the perpetrator or victim, the repetition of reports on the same content does not usually provide new evidence. Therefore, limiting the detection device to only known content would, in practice, deprive law enforcement authorities of an essential lever to identify

perpetrators and protect victims, some of whom are sometimes in very serious danger, even though encrypted digital environments already offer authors particularly extensive and almost impenetrable spaces for exchange.

The French authorities will also be able to reiterate **the importance of keeping grooming and pedo-trapping within the scope of detection.** Indeed, many offences – such as bribery of minors (e.g. minors in custody or victims of sextortion) or attempts to organise physical encounters with a view to sexual assault – are mainly based on text exchanges, without there necessarily being any prior dissemination or sending of paedophile content. The detection of grooming and pedo-trapping is therefore necessary to continue to prevent these risks. [By way of illustration, the number of cases of sextortion recorded in recent years has been steadily increasing: OFMIN identified 27 000 cases of sextortion in France in 2024, compared to 10 000 in 2023 and 1000 in 2022.]

Finally, the French authorities may recall the need **to retain the possibility of accessing traffic data and metadata as part of the [in particular voluntary] detection mechanisms,** since the exclusion of such data would prevent the services from identifying and locating the respondents, thus depriving the detection of its effectiveness and rendering the device operational.

B. Definitions

|*As regards the definition of public content in Article 2 and content excluded from that definition]*

- The proposed definition, based on that of the TCO, seems to us to be relevant and helps to strengthen coherence within European legislation.
- As regards the content excluded from this definition, we propose that a dedicated recital accompany it, thus excluding any risk of re-reading or reinterpretation. It could thus be ingrained that any content that does not meet the definition of public content is considered non-public. This would also make it possible to secure the detection actions of service providers in those spaces, where the latter can take place. This recital could take the following form: Given that the digital environment is evolving and new platforms and services are emerging, digital environments should be defined in a non-restrictive manner. Therefore, to supplement the definition of publicly accessible environments, 'non-public content' should refer to all content that is not covered by the definition of 'content that is publicly accessible' and that is not encrypted.'

C. Own-initiative searches on content that is not publicly accessible – Article Z

[Regarding the scope]:

- The removal of new content from the scope of detection, regardless of the legal or technical configuration chosen, is not possible for the French authorities.
- As stated in the past, voluntary detection loses much of its interest and effectiveness if it does not detect new content. This requirement is all the more central in the environments referred to in Article Z, in which storage spaces (drives, clouds, etc.) mainly host self-produced visual content, precisely corresponding to new content and which makes it possible to identify new victims and, where appropriate, perpetrators. It should be recalled that the primary objective of this system is the detection of situations of ongoing abuse in order to allow the immediate protection of the minors concerned and the interruption of offences. From that point of view, limiting the scope of detection only to already known content and grooming would not make it possible to achieve that objective.

[As regards the possibility for content hosts to carry out such a detection]:

- That type of arrangement is a continuation of what was done under the derogation regime. In this regard, the operational services point out that this model is already the one to which the platforms have committed themselves and that they will continue to apply in the United States, regardless of the environments targeted. They have developed technologies specifically designed to secure their online environments by detecting illegal content.
- These include the establishment of internal hashing databases and the use of ICSE (Interpol) databases to benchmark against content verified by competent authorities. The expertise of large service hosts is also recognised at international level, as evidenced by the fact that ICSE regularly requests the transmission of their hash bases, in a manner similar to what is requested from the competent national authorities.

[As regards the wording of Article Z]:

- Article Z(a)(iii): If a reference to 'content data' and 'traffic data' is maintained, which is necessary from an operational point of view, those two concepts should, however, be defined in Article 2.
- The French authorities question the PRCY on the *nature* of the information that service providers may analyse in the context of voluntary detection, as listed in Article Z(a)(iii); These do not necessarily correspond to the nature of the information to be contained in alerts (see the information provided for in Article 13(1)(f), discussed at the meeting of JHA Counsellors on 5 May 2026). Indeed, if the detection procedure is to lead to an alert when an infringement of this Regulation is found, it is imperative that the information processed during the detection procedure is sufficiently complete and usable to enable the competent authorities to identify the perpetrator and the victim(s). In the interests of legal certainty and consistency of the operative part, the French authorities are in favour of aligning the categories of information referred to in Article Z(a)(iii) with those provided for in Article 13(1).
- Article Z(c): The procedure for 'declaring' detection activities carried out by suppliers as proposed in Article Z is not appropriate. In practice, online service providers use

detection devices based on algorithms integrated into the very operation of their systems. They are therefore not one-off 'scanning' actions, but continuous and structural processes. In addition, some suppliers mobilize teams dedicated to these activities, which are thus fully integrated into the day-to-day operation of their services. In those circumstances, the detection activity is inseparable from the architecture and operation of the service. If the objective of the article is to ensure some form of transparency through a supplier statement, it should not have a temporal dimension, since it is a continuous activity, intrinsically linked to the functioning of the platform.

As regards Article Z+1, the French authorities consider that the suspension of voluntary detection activities is not intended to be addressed by that regulation, since, in the event of misuse of such tools, rules and remedies already exist at national level. More broadly, the French authorities consider that as long as the exact role of the coordinating authorities is not better defined, it is not possible to confer such competence on them

D. Detection orders for content that is publicly accessible – Article X

[As regards the conditions for issuing such orders]

- Cf. General comment (point (a) of the note)
- Article X(1)(a) and (b): As announced in the general comments above, we would like to ask the Presidency about the usefulness of the comment procedures provided for in these points, even though the right of appeal exists and this mechanism will in any case be subject to validation by a judicial authority or an independent administrative authority. In this respect, the steps provided for in points (a) and (b) appear redundant or even counterproductive.

[Regarding the competent authority and the possibility of designating an IAA]

We are in favour of adopting the formulation of a competent authority in order to respect the national systems already in place, which can also operate under the supervision of an independent administrative authority. Without this constituting a definitive position, the French authorities also express strong reservations in the event that this authority is a judicial authority.

[As regards the wording of Articles X and X+1]

Article X(1): The French authorities, in addition to the questions and comments made earlier in relation to Article 44 (see general comment (point (a) of the note), request that a reference to Interpol's ICSE database be included in this paragraph so that the reference databases for this type of measure are as complete as possible.

E. Detection orders for content that is not publicly accessible – Article Y

[Regarding the competent authority and the possibility of designating an IAA]

We are in favour of adopting the formulation of a competent authority in order to respect the national systems already in place, which can also operate under the supervision of an independent administrative authority. Without this constituting a definitive position, the French authorities also express strong reservations in the event that this authority is a judicial authority.

[As regards the wording of Articles Y and Y+1]

- General remark: The arrangements proposed in this compromise do not have a clear advantage over the judicial measures that already exist in this area.
- In addition, we wonder what the Presidency means by the term 'user'. Is it just a pseudo/handle? If that is the case, the effectiveness of such devices is really questionable, because monitoring a nickname while a user can have an unlimited number, on various platforms, at the same time, seems very ineffective.
- Article Y(2)(b): We wonder about the practical consequences of this provision. It provides that users who have disseminated pedocriminal content via an inactive account for at least 12 months can no longer be subject to a detection order under Article Y. While the French authorities understand the objective of not imposing supervisory measures on permanently inactive accounts, the absence (seems?) of a mechanism to react when an account has been used by a potential author appears to be problematic. It limits the ability of authorities to deal with situations where particularly serious content has been disseminated through such accounts. More flexibility would be needed.

F. Searches by the EU Centre – Article 49

[As regards the possibility for the Centre to have such a prerogative, in addition to the detection put in place by the suppliers and the scope of that prerogative (known, unknown and grooming content)]

- The French authorities do not object in principle to the scope of the EU Centre's detection prerogatives being able to include known and unknown content, provided that the staff who will be responsible for carrying out this task are competent and accredited to deal with this type of content.

- They recall that deconfliction work will have to be carried out in order for this device to be functional and effective.

[As regards the technologies used and their compliance with the criteria set out in Article 10]

No comments

[Regarding the wording of Article 49(1)(ba)]

- *No comments*

G. Common provisions

[S'agissant de l'audit indépendant des technologies utilisées et de leur financement]

- *Pas de commentaires*

[S'agissant des autres dispositions relatives à ces articles]

- *Pas de commentaires*

GERMANY

All of the following remarks by Germany must be considered preliminary, subject to further scrutiny and political review. We reserve the right to make further comments.

A. Scope of the detection/searches

Delegations are invited to indicate their flexibility concerning the appropriate scope of application for each of the components.

From our point of view, the scope of own-initiative searches by providers should not be restricted and should refer to both known and unknown CSAM and grooming.

Especially unknown CSAM and grooming gives clues to current, ongoing abuse and opens up the possibilities to end it and to protect affected children and adolescents.

Germany asks for clarification whether own-initiative scanning for known content using hash value technologies is not allowed anyways under the current legal framework when there is no human access to user communication on the part of the providers and therefore no "*listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users*" in the sense of Article 5 para. 1 ePrivacy Directive.

In any case, it should be kept in mind that member states are free make restrictions to Article 5 under the stipulations of Article 15 para. 1 ePrivacy Directive. Any CSA Regulation prohibiting scanning for unknown material and grooming would therefore only restrict the member states' possibilities to strengthen the fight against CSAM and child abuse in comparison to the status quo (even without the Interim Regulation).

B. Definitions

Delegations are invited to provide their comments on the approach to only define publicly accessible content and the proposed text of the definition.

Germany agrees with and supports the definitions and the proposed texts.

C. Own-initiative searches on content that is not publicly accessible – Article Z

Delegations are invited to consider whether they could show flexibility on the scope of the derogation. Specifically, delegations are requested to indicate whether they would be ready to accept a reduced scope regarding the content that is subject to own-initiative searches, for example only for known CSAM, and whether they could agree to allow hosting service providers to conduct such searches on content hosted on their services that is not publicly accessible as part of a wider compromise package.

Delegations are also invited to provide feedback on the suggested wording of Article Z.

For Germany, it is of the utmost importance that a CSA Regulation strengthens and not complicates the fight against CSAM and child abuse. New rules must therefore not fall short of the legal situation during the period of application of the Interim Regulation. As mentioned above, even the current status quo without the Interim Regulation allows the Member State to restict Article 5 ePrivacy Directive. Germany therefore strongly warns against all regulations that effectively lead to a restriction of voluntary searches. Any regulation that contains rules that impose additional restrictions compared to the Interim Regulation, even if only new bureaucratic hurdles exist, is likely to restrict providers in their valuable activities to combat child abuse, reduce the number of child abuse cases reported to European law enforcement authorities and thus reduce the number of cases where child abuse is detected and ended. It has to be borne in mind that out of the measures discussed in the draft CSA Regulation, voluntary scanning is the only system that is known to be a functioning and valuable contribution to the fight against CSAM and child abuse. It does, however, since it is voluntary, entirely depend on the willingness of the providers to continue their efforts. Any restriction can jeapordise this willingness and cut European law enforcement agencies off from one of the most valuable sources of hints to CSAM and child abuse, which are the reports the receive from voluntary scanning. This even includes voluntary scanning outside the scope of Article 5 ePrivacy Directive, which is currently possible in compliance with the GDPR, regardless of the Interim Regulation. Again, any CSA regulation containing such restrictions risks resulting in a situation that restricts efforts to fight CSAM and child abuse even more than the current situation without the Interim Regulation.

Germany therefore does not agree with:

- Requirements for providers to provide any information in advance of voluntary searches
- Specific provisions within the CSA Regulation giving any authority the power to suspend voluntary searches
- Limiting the voluntary searches to certain types of material, technologies or in any other way.

D. Detection orders for content that is publicly accessible – Article X

Delegations are invited to provide feedback on the following:

a) The conditions for issuing the order under Article X;

b) The appropriate authority to issue the order, and whether there could be flexibility on this point, including on whether there might be scope to reach a compromise by having independent administrative authorities (in addition to judicial authorities) issuing these orders;

c) any additional feedback on the suggested wording of Articles X and X+1.

a) Germany considers the proposed conditions for issuing detection orders for publicly accessible content to be vague ("if the service or part of the service is being misused for [online child sexual abuse] to an appreciable extent") and more precise criteria should be elaborated. It is currently unclear how this would work in practice and there is concern that this measure would provide no practical benefit for identifying CSAM and child abuse. If detection orders can only be issued once a suspicion has already been established, any additional benefit over existing measures of criminal procedure could be to minor to make up for the bureaucratic procedure envisaged for this measure, even if the legal threshold should be lower than for criminal law suspects.

b) Germany is flexible with regard to the question of appropriate authority to issue these orders. Before being able to discuss details of procedure it has to be understood how this measure would work.

c) -

E. Detection orders for content that is not publicly accessible – Article Y

Delegations are invited to provide feedback on the following:

a) the types of authorities involved in the issuing of the detection order for non-public content and whether such orders could be issued by all Member States or only by the Member State in which the provider is established;

b) the text proposed for the detection order;

c) the scope of material (known, new CSAM and/or grooming), of the users concerned and how this scope might interact with own-initiative detection, for example: would it be appropriate/necessary to allow own-initiative detection by providers, while in parallel having a detection order regime that has more restrictive conditions?

d) any additional feedback on the suggested wording.

We are flexible with regard to the types of authorities.

In our view, a restriction to authorities of the Member State in which the provider is established leads to a concentration on a few Member States. In our view, the power to issue detection orders should be equally vested or at least possible in all Member States.

Especially unknown CSAM and grooming gives clues to current, ongoing abuse and opens up the possibilities to end it and to protect affected children and adolescents. However, limitations of the scope would, on the other hand, reduce the level of interference with fundamental rights. Germany does not oppose detection orders as long as they are an additional measure to voluntary searches, and as long as they meet the requirements under German Basic Law for an individual suspicion to access communication content data, subject to further scrutiny. In this regard, we would appreciate further explanations by the Presidency on how it deems the requirements for a detection order to differ from the criminal law sense. Also, it seems unclear on which basis certain groups of users would be identified. To better understand the proposed rules, Germany asks for clarification how this process would work in detail.

F. Searches by the EU Centre – Article 49

The Presidency requests feedback from delegations on the following:

a) Whether they can accept to give the EU Centre such a power to complement detection/searches by providers.

b) The scope of the EU Centre's powers in this regard – should it be limited to searches for 'known' CSAM as per the EP mandate or should it also be able to scan for 'new' CSAM and/or solicitation of children?

c) Whether the EU Centre should be required to use technologies that meet the requirements of Article 10 when conducting those searches.

d) Any other comments on the suggested wording of Article 49 (1)(ba).

a) Yes, Germany can generally accept that the EU Centre conducts searches as already possible for everyone. To give the searches of the EU Centre any advantage over searches of the general public, there should be a legal obligation for providers to allow for the searches of the EU Centre including the use of technologies that are not allowed for general users in the terms and conditions (e.g. web scraping, registering and using profiles for the purpose of conducting searches etc.). Especially, as searches by providers happen on a voluntary basis and reporting obligations as set out in Article 12 of the regulation only apply if the provider "become aware of illegal content", it is helpful that there is an entity such as the EU centre which proactively searches the web for CSAM. However, the evaluation also with regard to fundamental rights implications is still ongoing. For the purpose of a thorough assessment, it would be helpful to learn about currently available technologies to conduct such measures. The safeguards of Article 10 should apply to technologies used by the EU Center, as applicable. If the technology relies on web scraping, it may also be useful to implement retention periods, in particular for material that does not lead to a hit.

In any case, even if the searches of the EU centre are supported by additional legal powers, this measure cannot replace voluntary detection by the providers.

b) In general, it is obvious that the impairment of fundamental rights is lower for publicly accessible content compared to confidential communications. Especially unknown CSAM and grooming gives clues to current, ongoing abuse and opens up the possibilities to end it and to protect affected children and adolescents. Limitations of the scope would, on the other hand, reduce the level of interference with fundamental rights.

c) In line with b) the EU Centre should not be restricted in its searches in any way that does not apply for the general public either.

d)

The CSA regulation should clarify which role the EU centre should have once having identified known or new CSAM in relation to law enforcement agencies. In cases of new CSAM and ongoing abuse and exploitation of children the fast involvement of law enforcement is crucial. In cases of known hashes the take-down of CSAM can be the priority. The current proposal foresees a complicated workflow as the EU centre identifies CSAM, then reports to the providers. Once the provider has reported back to the EU centre and classified the content as urgent, law enforcement is contacted. In cases of ongoing sexual abuse and exploitation this workflow seems too long. The EU centre should have the possibility to contact law enforcement agencies and Europol directly in case of acute abuse and exploitation and address providers in case of known hashes for take-down. It is recommended to engage with the International Watch Foundation and the Canadian Centre for Child Protection on their experience in relation to the cooperation of their organisations with law enforcement agencies, their procedures in forwarding reports and the internal rules of saving traces which law enforcement might use at a later stage by request.

G. Common provisions

Delegations are invited to provide feedback on the following:

a) Whether the technologies should be independently audited (as the EP mandate indicated)? Who would pay for these audits?

b) Any other aspects of the text on Articles 9, 10, 11 and 50(1)6.

As set out under C., Germany strongly warns against restricting the voluntary searches that have successfully led to combatting child abuse for years. Any new requirements would lead to a lower number of reports and deny European law enforcement authorities access to information.

As regards audits for technologies used on the basis of detection orders, Germany does not deem independent audits necessary, but is flexible. In case of a detection order, the audit should be payed for by the provider who is the addressee of the order.

HUNGARY

Hungary appreciates the Presidency's efforts to find a compromise on detection and asks the Presidency to firmly keep the Council mandate adopted in November 2025 as we generally cannot support a compromise proposal with a narrower scope on detection.

We are critical of the new presidency concept on decetion because we do not consider the separation of publicly available and privately shared content to be effective; known, new CSAM and grooming should remain within the scope of the Regulation, but the presidency concept excludes grooming in fact; and the effectiveness of the implementation according to the concept is highly questionable.

A. Scope of the detection/searches

We propose to keep all three categories, known and new CSAM content as well as content shared during grooming, within the scope of the CSA.

B. Definitions

Since CSAM content uploaded in a closed user group is just as illegal as CSAM content publicly accessible to a potentially unlimited number of users, we do not consider it justified to differentiate the obligation significantly at the level of the regulation.

From a technical point of view, the distinction is also not justified, since the digital fingerprints of CSAM content can be checked during the upload in both cases. The publicly accessible definition is another problem, since quasi-automated entry into a closed group can also be carried out, which can lead to the formation of extremely large "closed" groups (see e.g. Telegram).

C. Own-initiative searches on content that is not publicly accessible – Article Z

We consider the broader compromises solution to be supportable in the event that the hosting service provider is obliged to notify the coordinating authority of the place of establishment of the planned filtering of content that is not publicly accessible stored on its service in advance, and the hosting service provider is only entitled to carry out the filtering if the coordinating authority of the place of establishment has not objected to this.

The service provider's own-initiative search could apply to both already known and new CSAM content.

At the same time, as a guarantee – with regard to privacy rights – it should be considered that the hosting service provider can conduct a search on its own initiative on content that is not publicly accessible stored on its own service if the conditions set out in Article Y. (2) – relating to the issuance of a detection order for content that is not publicly accessible – are otherwise met in contrast to the planned search.

Regarding Article Z(b), it would be important for service providers to be able to carry out self-initiated searches (voluntary searches) as of the entry into force of the CSA Regulation in order to restore the level of protection that existed before the expiry of Regulation (EU) 2021/1232 on 3 April 2026 as soon as possible.

Under Article Z(b), service providers must use the relevant indicators provided by the EU Centre in accordance with Article 44 for self-initiated searches. It would also be useful to lay down the rules under which service providers are entitled to carry out searches until Article 44 enters into force or until the EU Centre publishes the indicators.

D. Detection orders for content that is publicly accessible – Article X

Where the EU Centre carries out a search under Article 49 in relation to the publicly accessible content of a service provider, the coordinating authority of the place of establishment should nevertheless be able to initiate the issuance of a detection order under Article X by a judicial or independent administrative authority of the Member State.

Before such an initiative, the coordinating authority of the place of establishment may consult the EU Centre in advance, or a list of searches carried out by the EU Centre may be made available to the coordinating authorities of the Member States.

E. Detection orders for content that is not publicly accessible – Article Y

We consider detection orders for non-public content to be acceptable. It would also be appropriate to allow service providers to carry out searches on their own initiative (voluntary detection), despite the fact that a detection order with stricter conditions would exist in parallel.

This would be particularly important so that, if the provisions on detection orders were to be introduced at a later date after the entry into force of the CSA Regulation, children would not be left without protection during the transitional period.

If only the coordinating authority of the place of establishment of the service provider would be entitled to initiate the issuance of a detection order before the judicial or independent administrative authority of its own Member State, the process of issuing detection orders could be significantly slowed down due to the caseload.

In relation to Article Y(3), in addition to known and new CSAM content, it would be appropriate to ensure the issuance of a detection order also in relation to "grooming", the acts related to which typically do not take place in the form of public content (but rather in the form of private messages in a social media application or chat service, etc.).

F. Searches by the EU Centre – Article 49

We support the EU Centre being able to carry out own-initiated searches of content made publicly available by service providers for both known and new CSAM content. However, in this case, provisions should also be made to ensure consistency with the proposed Article X (see comment on point D).

Article 10 applies safeguards (e.g. data security, data protection) to the technology and its application, and it would therefore be appropriate to expect the EU Centre to use technology that complies with Article 10.

Furthermore, pursuant to Article 50(1), the EU Centre shall make technology for identifying CSAM content available to service providers upon their request.

It is likely that the EU Centre would use the same technology for its own searches that it otherwise makes available to service providers, which also supports the fact that the requirements of Article 10 should apply to this technology as well.

G. Common provisions

With regard to Article 10, if the service provider is entitled to choose the technology, it may be justified to have an independent audit of the technologies used by the service providers, and that the service providers pay the costs of the audit. Each service provider (including SMEs) can choose, in accordance with its capacity to bear the burden, whether to use the technology made available by the EU Centre (in this case, there are no additional costs) or to choose another technology and bear the costs of the independent audit.

It would also be worthwhile to ensure that the IT market player developing the technology is also entitled to initiate an independent audit of the technology, while bearing the costs incurred, so that service providers licensing the technology would no longer be burdened by this audit, which would be particularly beneficial for SMEs.

In relation to Article 50(1), it would be appropriate to extend the scope of operation/identification of the technology to be provided free of charge by the EU Centre to service providers to also include grooming (currently, the term "solicitation of children" is in brackets, which should be omitted).

ITALY

A. Scope of the detection/searches

Upon certain conditions, Italy can support the scope of detection/searches activities under the proposed regulation to cover known and new CSAM. On the contrary, grooming should be excluded. Moreover, text-based communications and audio communications (especially real-time voice communications) are also to be excluded (see comments to document 9139/2026).

B. Definitions

Italy has already expressed its support for an approach that differentiates the treatment of content according to whether it is publicly accessible or not. However, further clarification in the text would be beneficial, so to make explicit that encrypted content cannot, under any circumstances, be considered publicly accessible. In this regard, the Presidency may wish to consider adding the following sentence to art. 2: "Content protected by encryption shall under no circumstances be considered publicly accessible."

C. Own-initiative searches on content that is not publicly accessible – Article Z

As consistently stated throughout the negotiations, Italy does not support the introduction of own-initiative searches by providers aimed at detecting new CSAM or grooming on non-publicly accessible materials, this representing a red line.

D. Detection orders for content that is publicly accessible – Article X

To the extent that publicly accessible content does not raise privacy concerns, the issuance of detection orders in relation to such content does not appear problematic, and Italy could support the Presidency's proposals in this regard.

That said, the conditions for issuing such orders appear insufficiently clear. In particular, it is unclear how it would be determined that a given service is "misused for online child sexual abuse to an appreciable extent".

As for the appropriate authority to issue orders, Italy has consistently taken the view that detection activities should, at a minimum, be subject to supervision by a judicial authority (or by the corresponding independent administrative authority in those Member States whose constitutional frameworks require such an approach). However, we cannot support the conferral of such powers on purely governmental bodies or on centralised administrative entities such as the EU Centre, which does not provide equivalent guarantees and safeguards.

From the Italian perspective, the principles of legality and the need to prevent forms of generalised monitoring require that detection orders be issued by a judicial authority. The practical application of this Regulation may ultimately give rise to criminal proceedings of significant consequence, including cases in which prosecutions are initiated years after the relevant conduct and by authorities other than those of the suspect's Member State of residence. In the Italian legal system, as reflected also in recent Union legislative instruments, access to digital evidence is safeguarded through procedural guarantees linked to the intervention of judicial authorities. These safeguards are essential to ensure the proper assessment of the relevant content, verification of its evidential value, and attribution of criminal liability only where conduct can effectively be linked to the user concerned.

Moreover, the competence for the issuance of orders should not be attributed only to the authorities of the Member State of establishment. On the contrary, it should be extended to the authorities of the Member State that has jurisdiction over the potential abuse, namely the Member State where the offence is suspected to have been committed, is being committed, or is likely to be committed; the Member State where the alleged offender resides or is located; or the Member State where the victim resides or is located. As a second best, the regulation should explicitly provide that the results of detection activities are immediately shared with the competent authorities of the Member State concerned by the abuse. Such provisions constitute, in the Italian view, important safeguard against forum shopping and would help ensure the effectiveness of national criminal investigations.

E. Detection orders for content that is not publicly accessible – Article Y

As just said, Italy considers it essential that any detection order be issued by a judicial authority, which alone is capable of ensuring compliance with the constitutional principles of necessity and proportionality. Such judicial oversight should be exercised not only by the authority of the Member State of establishment, but also by the authority having jurisdiction over the alleged abuse. By contrast, it would appear excessive to confer such powers indiscriminately on the authorities of all Member States.

As regards the material scope of detection orders for content that is not publicly accessible, and provided that the other key elements of the Presidency's proposal remain unchanged – in particular the limitation of such orders to specific users linked to the dissemination of CSAM – Italy could envisage extending their scope to cover both known and new CSAM. At the same time, Italy cannot support the inclusion of grooming or conversational communications, whether in written, audio or any other form.

Any potential inconsistency with the approach taken in relation to own-initiative detection could be avoided by limiting the scope of voluntary detection to known CSAM only, as proposed by Italy.

F. Searches by the EU Centre – Article 49

Italy has consistently expressed its opposition to conferring proactive detection powers on the EU Centre, as this would fundamentally alter the nature of its role.

The European Centre could instead perform a coordination function with regard to reports, aimed in particular at identifying the competent jurisdiction and ensuring the appropriate allocation of cases to the relevant national authorities.

Moreover, Italy considers that any transmission of information to Europol should take place only with the prior consent of the Member State responsible for the processing of the data or competent for the investigation, in full respect of the principles of investigative sovereignty and national competences.

G. Common provisions

Technological safeguards are certainly to be welcomed. It is essential to ensure that the software used by providers fully complies with the agreed technological safeguards, in particular so as not to undermine encryption or enable large-scale and indiscriminate monitoring.

Detection technologies used by providers should be disclosed in advance to the EU Centre in order to ensure adequate levels of transparency and oversight. In this context, the EU Centre could be empowered to commission independent audits by qualified third parties, aimed at assessing the reliability, proportionality and compliance of the technologies used with the requirements of the Regulation and the protection of fundamental rights. At the same time, it should be recognised that such audits may entail significant costs and lengthy procedures.

As regards the allocation of costs, Italy considers that the financial burden should remain proportionate:
- if technologies are provided centrally by the EU Centre pursuant to Article 50, audit costs should be covered by the EU budget or by the EU Centre itself;
- for proprietary technologies developed by large service providers, audit costs should be borne by the providers, in line with the responsibility-based approach underpinning the Digital Services Act (DSA).

Any auditing mechanism should remain proportionate and avoid creating excessive costs or delays, particularly for smaller providers. In this regard, Italy could support a risk-based or sample-based auditing mechanism, taking into account, inter alia, assessments already carried out by the Technology Committee, the Victims' Advisory Forum and the European Data Protection Board.

LATVIA

General comment

Latvia considers that detection is one of the key aspects of the CSA Regulation, as it must ensure the effective protection of children online, while respecting fundamental rights, data protection requirements, the confidentiality of communications, cybersecurity and technological neutrality.

From a child protection perspective, it is important for Latvia that the adoption of the Regulation is taken forward as swiftly as possible, thereby strengthening the protection of children online and facilitating bringing perpetrators to justice. At the same time, it is important for Latvia that the final compromise is workable in practice and does not create legal uncertainty for Member States, providers and users.

Latvia generally welcomes the Presidency's attempt to distinguish between different detection and search regimes depending on whether the content is publicly accessible or not publicly accessible. Such an approach may help to differentiate more precisely the applicable conditions and safeguards, taking into account the different level of interference with fundamental rights.

Regarding A. Scope of the detection/searches

Latvia considers that the framework should provide effective tools for the identification of at least known and new CSAM, and preferably also the solicitation of children ("grooming"). This is essential in order to reduce the possibilities for child sexual abuse, to identify ongoing cases of child sexual abuse, and to prevent the re-victimisation of victims. Latvia takes the same position with regard to own-initiative detection/searches by providers.

Regarding B. Definitions

Latvia generally understands the Presidency's proposed approach to define "content that is publicly accessible" in the Regulation in order to distinguish between different detection and search regimes. At the same time, this distinction is of significant importance for the practical application of the Regulation. Latvia therefore invites the Presidency to provide further clarification and concrete examples of what, in its view, should be considered "content that is not publicly accessible".

Latvia also invites the Presidency to clarify the status of encrypted content in the proposed distinction of scope. In Latvia's view, the encryption safeguard clause included in Article 1, namely Article 1(5) in the Council general approach, primarily establishes that the Regulation must not prohibit, make impossible, weaken, circumvent or otherwise undermine encryption, including end-to-end encryption, and must not create any obligation for providers to decrypt data or create access to end-to-end encrypted data.

It is important for Latvia that the final text does not create legal uncertainty in this regard. If the intention of the co-legislators is to exclude encrypted content from the application of specific detection or own-initiative search measures, this should be clearly reflected in the text of the Regulation. Conversely, if the intention is only to ensure that the measures provided for in the Regulation must not require the weakening or circumvention of encryption or the decryption of data, this should be clearly distinguished from the question of the general material scope of the Regulation.

Regarding C. Own-initiative searches on content that is not publicly accessible — Article Z

Latvia supports providers' own-initiative activities to detect and report CSAM. In view of the expiry of the CSA Interim Regulation, it is essential to prevent a legal gap.

At the same time, such a framework must be clearly distinguished from an obligation to carry out detection. Own-initiative searches must not be interpreted as a general monitoring obligation or as an obligation for providers to systematically examine all users' communications.

Latvia can support the Presidency's proposed approach regarding own-initiative searches on content that is not publicly accessible, provided that adequate safeguards are ensured. The processing must be proportionate, limited to the specific purpose and based on technologies that meet the requirements laid down in the Regulation.

Latvia can show flexibility as regards extending this regime also to providers of hosting services, provided that equivalent conditions and safeguards are applied to them by analogy, to the extent necessary. This may be of practical importance, taking into account that content that is not publicly accessible may also be stored in clouds or other hosting services.

Latvia supports the proposal that providers should inform the EU Centre before conducting own-initiative searches. At the same time, this procedure must be workable in practice and must not create a disproportionate administrative burden.

Regarding D. Detection orders for content that is publicly accessible — Article X

Latvia can generally support the inclusion of public content detection orders in the Regulation. Given that, in the case of content that is publicly accessible, the interference with fundamental rights is usually less intensive than in the case of private or non-public communications, this regime may be subject to a simpler procedure.

At the same time, such orders must also be targeted, necessary, proportionate, limited in time and directed at a specific part of the service that is being misused for the dissemination of CSAM to an appreciable extent. Latvia supports the condition that such an order may be issued only where the service or part of the service is being misused for online child sexual abuse to an appreciable extent.

As regards the authorities issuing public content detection orders, Latvia can show flexibility. In Latvia's view, a model where such orders are issued by a competent authority or a Coordinating Authority could be acceptable, if this is provided for under national law and the necessary procedural safeguards are ensured. At the same time, Latvia can also consider a compromise solution providing for the involvement of a judicial or independent administrative authority, where this is necessary to reach political agreement and to ensure a sufficient level of protection of fundamental rights.

Regarding E. Detection orders for content that is not publicly accessible — Article Y

As regards content that is not publicly accessible, Latvia considers that the Presidency's proposed approach concerning detection orders for specific users requires further clarification and practical assessment. In Latvia's view, it would first be necessary to clarify what is understood by content that is not publicly accessible under this framework, and in which practical situations "specific users" could be identified for the purpose of issuing such an order.

Before taking a position in support of such an instrument, it would be useful to receive concrete examples of situations in which such orders would be used, including examples concerning the relevant types of services, categories of content and criteria for identifying the users concerned.

Regarding F. Searches by the EU Centre — Article 49

Latvia can support granting the EU Centre the power to conduct own-initiative searches on content that is publicly accessible, provided that such powers complement, but do not replace, the work of law enforcement authorities. The role of the EU Centre in this context should be to support the identification of CSAM, reporting and further action by the competent authorities.

Latvia considers that the technologies used by the EU Centre should comply with the requirements laid down in the Regulation.

Latvia can support the EU Centre's own-initiative search powers initially focusing on known and new CSAM in content that is publicly accessible. Latvia could also agree to a broader scope of the EU Centre's powers, including the solicitation of children, insofar as sufficiently clear safeguards, human review and a clear mechanism to prevent undue impact on lawful content and users' rights are ensured.

Latvia supports the possibility for law enforcement authorities to request the EU Centre to suspend the notification to the provider where this is necessary in order to avoid interfering with ongoing investigations. At the same time, such a suspension period should be clearly limited in time and justified by the needs of a specific case.

Regarding G. Common provisions — Articles 9, 10, 11 and 50

Latvia can generally support the Presidency compromise proposals.

LITHUANIA

A. Scope of Detection/Searches

Support with a substantive reservation.

Lithuania could support a flexible, risk-based approach to defining the scope of detection measures, allowing for differentiated measures depending on whether the risk concerns known CSAM, new CSAM, or grooming. However, it should be emphasized that the scope should not be narrowed and known CSAM, new CSAM as well as grooming should be included. It is essential to ensure that all major risk categories are covered and that the different detection mechanisms are aligned consistently in order to avoid regulatory gaps and maintain the practical effectiveness of the Regulation.

B. Definitions

Support with a reservation.

Lithuania could support defining only publicly accessible content, as this would facilitate a clearer distinction between detection regimes. However, the absence of a definition of non-publicly accessible content may create uncertainty regarding the scope of that category. The distinction between public and non-public content should therefore remain clear and consistently applied throughout the Regulation.

C. Own-Initiative Searches of Non-Publicly Accessible Content – Article Z

Support with a substantive reservation.

Lithuania could support providers' own-initiative searches of non-publicly accessible content as a complementary preventive measure. However, the scope, conditions and relationship with detection orders should be clearly defined. The mechanism should not be limited solely to known CSAM and should remain supplementary rather than replacing formal detection measures.

D. Detection Orders for Publicly Accessible Content – Article X

Lithuania could support detection orders for publicly accessible content as an important and comparatively less intrusive measure, provided that the conditions for issuing such orders are clear and sufficiently targeted.

(a) Conditions for issuing detection orders

Lithuania could support the principle that detection orders for publicly accessible content may be issued where a service has been used for the dissemination of CSAM, as this enables a prompt response to an existing and substantiated risk.

However, the criterion of **"appreciable extent"** should be further clarified to ensure legal certainty and consistent application across Member States. It should be clear that the criterion refers not to isolated or incidental cases, but to a more systematic or significant use of a service for the dissemination of CSAM. The assessment should be based on objective indicators, such as the number and recurrence of detected cases or the extent of misuse of particular service functionalities.

Consideration should also be given to the level of risk within specific parts of a service (e.g. comment sections, public groups or channels, or file- and photo-sharing functionalities). At the same time, the criterion should remain sufficiently specific and targeted to ensure that detection orders are not applied excessively broadly and do not create a risk of *de facto* general monitoring.

(b) Competent authority

Lithuania supports a model allowing detection orders to be issued by either judicial authorities or independent administrative authorities, provided that appropriate independence, oversight and operational efficiency are ensured. From Lithuania's perspective, maintaining an appropriate balance between effectiveness and legal safeguards is essential.

(c) Additional comments

Lithuania could support a simplified procedure for publicly accessible content, reflecting its lower impact on fundamental rights. However, it should remain aligned with other detection regimes and preserve a clear distinction between targeted measures and prohibited general monitoring.

E. Detection Orders for Non-Publicly Accessible Content – Article Y

Lithuania supports a targeted detection-order regime for non-publicly accessible content, while ensuring that the applicable conditions and procedures remain operational and effective, particularly in relation to new CSAM and grooming.

(a) Authorities and jurisdiction

Lithuania could support a model under which detection orders for non-publicly accessible content are issued by judicial authorities or independent administrative authorities, given the greater impact on fundamental rights. The chosen model should ensure adequate independence and oversight while remaining efficient and operational.

As regards jurisdiction, Lithuania could support assigning the primary role to the Member State of establishment of the provider in the interests of legal certainty and consistency. At the same time, other Member States should be able to effectively initiate procedures or provide information to ensure an appropriate response to cross-border violations.

(b) Proposed wording of the detection order

Lithuania could support the proposed text as a basis, particularly its targeted nature and the requirement to assess necessity and proportionality.

However, conditions such as "clear indications", the 12-month reference and certain procedural requirements should not be so restrictive as to undermine the practical effectiveness of the mechanism, especially in relation to new CSAM and grooming.

The framework should remain clear and flexible, enabling effective action across different situations, while keeping procedures proportionate, operational, and practically feasible for service providers.

(c) Scope and interaction with own-initiative detection

Supports that the detection orders should be capable of covering known CSAM, new CSAM and, where appropriate, grooming, while remaining focused on specific users.

The relationship between detection orders and own-initiative searches should remain coherent. Voluntary measures should not be allowed to operate under significantly broader conditions than the formal detection-order regime.

(d) Additional comments

Lithuania could support a clearer and more operational formulation, while maintaining that the wording should more focused on practical implementation:

A detection order for non-publicly accessible content may be issued only in respect of specific users where, on the basis of lawfully obtained information, there are sufficient factual grounds to reasonably believe that they are involved in the dissemination of child sexual abuse material or the solicitation of children.

The order must be necessary and proportionate, clearly define its scope, duration and indicators, and be based on objective criteria (e.g. reports, repeated activity or behavior patterns).

The procedure should be clear and operational, avoiding unnecessary or duplicative steps, while ensuring the provider's right to be heard and independent oversight.

The detection order framework should be aligned with the voluntary search mechanism to avoid inconsistent standards across different detection regimes.

F. Searches Conducted by the EU Centre – Article 49

(a) Whether the EU Centre should be empowered to conduct searches

Lithuania could support empowering the EU Centre to conduct searches of publicly accessible content as a complementary measure supporting the overall detection framework.

However, the EU Centre should remain a technical and coordinating body, rather than an autonomous operational actor, with clearly defined responsibilities that do not duplicate those of service providers or competent authorities.

(b) Scope of powers

Lithuania could support a scope covering known CSAM, new CSAM and, where appropriate, grooming.

At the same time, broader scope (especially for new CSAM and grooming) should be accompanied by stronger technical and legal safeguards, given the greater impact on fundamental rights and higher risk of errors. It is also important to ensure that the EU Centre's activities remain clearly defined and proportionate, and that the scope of searches does not expand into broad or insufficiently targeted monitoring.

(c) Compliance with Article 10

Lithuania could support requiring the EU Centre to use technologies that comply with Article 10 standards, provided that the requirements remain proportionate, technologically neutral and applicable consistently across the system. It is also important that they apply consistently to all actors, including service providers and the EU Centre, ensuring equal conditions.

(d) Additional comments

Any search powers granted to the EU Centre should remain clearly limited and complementary in nature and should not become the primary detection mechanism. The EU Centre's role must remain technical and supportive, rather than operational.

G. Common Provisions

(a) Independent audits

Lithuania could support independent audits of technologies as a means of strengthening confidence in their reliability, accuracy and compliance with fundamental-rights safeguards.

(b) Additional comments on Articles 9, 10, 11 and 50(1)

Lithuania could support the overall framework established by Articles 9, 10, 11 and 50(1). The relevant provisions should remain clear, proportionate and practically implementable. Commission guidance should remain within the limits of the Regulation, and technologies made available by the EU Centre should remain voluntary for service providers.

THE NETHERLANDS

B. Definitions

To clarify the scope of the two detection regimes, the Presidency proposes including a definition of "content that is publicly accessible" in Article 2 of the proposed Regulation, which draws inspiration from the concept of '*dissemination to the public'* as defined in recital 14 of the Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online.

As regards non-public content, the Presidency proposes that all content that is not covered by the definition of 'content that is publicly accessible' and that is not encrypted would fall into this category. Consequently, no definition is provided therefor.

Delegations are invited to provide their comments on the approach to only define publicly accessible content and the proposed text of the definition.

The Netherlands supports the proposed approach of defining only "content that is publicly accessible" and, in particular, supports the proposed definition as set out by the Presidency. With regard to the second category, namely non-public content, the Netherlands would appreciate further clarification on the types of services that would fall within its scope. Could the Presidency provide some concrete examples of services that would be covered? In addition, the Presidency refers to non-encrypted services. For the purpose of verification, the Netherlands would like to confirm that this refers to services that are 'just' encrypted (i.e. a broader scope), rather than only services that are end-to-end encrypted (i.e. a narrower scope).

C. Own-initiative searches on content that is <u>not</u> publicly accessible – Article Z

Delegations are invited to consider whether they could show flexibility on the scope of the derogation. Specifically, delegations are requested to indicate whether they would be ready to accept a reduced scope regarding the content that is subject to own-initiative searches, for example only for known CSAM, and whether they could agree to allow hosting service providers to conduct such searches on content hosted on their services that is not publicly accessible as part of a wider compromise package.

At this moment, the Netherlands supports voluntary detection measures only on a temporary basis. Regular reassessment is necessary to ensure an appropriate balance between the objective of detection and considerations relating to privacy and cybersecurity. The Netherlands takes a flexible position regarding the scope of detection measures (limited to known material) in order to accommodate the European Parliament's concerns and avoid the appearance of maintaining a legal gap.

Delegations are also invited to provide feedback on the suggested wording of Article Z.

The Netherlands would welcome further clarification on the suggested wording of Articles Z and Z+1.

Article Z(c)

- It is unclear how a provider carrying out voluntary detection is expected to inform the EU Centre. The Netherlands would appreciate further clarification on the procedure and requirements for such notification.

Article Z+1

The Netherlands has several questions regarding the practical implementation and enforcement of this provision:

- How would a Coordinating Authority (CA) become aware that a provider carrying out voluntary detection is no longer complying with the conditions set out in the Regulation?
- How would a CA subsequently notify such a provider that it is not complying with those conditions?
- How would compliance be enforced to ensure that the provider effectively ceases the detection activities concerned?

- What powers or measures would be available to a CA if, despite being instructed to stop, the provider continues carrying out detection activities?
- If a provider modifies its detection measures so that they (once again) comply with the applicable conditions, would it be required to notify the EU Centre again before resuming such detection activities?

D. Detection orders for content that is publicly accessible – Article X

Delegations are invited to provide feedback on the following:

(a) The conditions for issuing the order under Article X;

Artikel X (1)
*The Coordinating Authority [of establishment] [may]/[**shall** have the power to request a judicial **authority** [or independent administrative authority] of its Member State to] issue an order requiring a provider of hosting services under the jurisdiction of that Member State to detect [online] child sexual abuse [material] on a part of its service that contains only content that is publicly accessible ('public content detection order') using indicators from the databases operated by the EU Centre pursuant to Article 44 and technologies for detection that fulfil the requirements of Article 10.*

(b) The appropriate authority to issue the order, and whether there could be flexibility on this point, including on whether there might be scope to reach a compromise by having independent administrative authorities (in addition to judicial authorities) issuing these orders;

The Netherlands is able to support the option of allowing an independent administrative authority, in addition to or instead of a judicial authority, to issue public content detection orders.

E. Detection orders for content that is not publicly accessible – Article Y

Delegations are invited to provide feedback on the following:

(a) the types of authorities involved in the issuing of the detection order for non-public content and whether such orders could be issued by all Member States or only by the Member State in which the provider is established;

Study reservation.

(b) the text proposed for the detection order;

Intended scope:

Before commenting on the substance of Article Y(2)(a) and (b), we would appreciate further clarification from the Presidency regarding the intended scope of the notion of "content that is not publicly accessible and not encrypted". To our understanding, most data in non-public parts of the internet will be encrypted at some stage. Therefore, we would be interested to understand which services and use cases are envisaged to fall within this category, and how this concept is intended to operate in practice.

Targeted detection:

The Netherlands welcomes the efforts to make the conditions for issuing a detection order more targeted. However, we are concerned that Article Y(2)(a) and (b) may set the threshold too high by effectively requiring a standard reasonable suspicion. This raises questions about the Regulation's legal basis and risks altering the nature of the instrument. Could the Presidency elaborate on how it considers

this degree of targeting to be compatible with the legal basis of the Regulation under Article 114 TFEU?

(c) the scope of material (known, new CSAM and/or grooming), of the users concerned and how this scope might interact with own-initiative detection, for example: would it be appropriate/necessary to allow own-initiative detection by providers, while in parallel having a detection order regime that has more restrictive conditions?

Study reservation.

(d) any additional feedback on the suggested wording.

No support for the current wording of Article Y+1(3). The court should be able to carry out a broader assessment of the circumstances of the case and should therefore retain sufficient discretion when taking its decision.

F. Searches by the EU Centre – Article 49

The Presidency requests feedback from delegations on the following:

(a) Whether they can accept to give the EU Centre such a power to complement detection/searches by providers.

We seek further clarification on the purpose of the proposed scanning activities by the EU Centre. In this context, the Netherlands would welcome clarification on how the proposed scanning activities by the EU Centre would relate to the existing roles and responsibilities of competent authorities, hotlines, as well as law enforcement authorities. In particular, it is unclear how overlaps and potential duplication of efforts would be avoided.

(b) The scope of the EU Centre's powers in this regard – should it be limited to searches for 'known' CSAM as per the EP mandate or should it also be able to scan for 'new' CSAM and/or solicitation of children?

The Netherlands supports limiting the EU Centre's scanning powers to the detection of known CSAM.

(c) Whether the EU Centre should be required to use technologies that meet the requirements of Article 10 when conducting those searches.

Support.

(d) Any other comments on the suggested wording of Article 49 (1)(ba).

Overall impression is that, with the Presidency's new proposal, a fundamentally new system of governance and supervision is being created. The key question is whether this system will, in practice, function effectively and allow for meaningful and realistic oversight.

Against this background, the Netherlands would appreciate further clarification on how the various elements of this new framework will interact. In particular, it would be helpful to receive a clear overview of all relevant roles, responsibilities, and competences of the different actors involved, as well as how these are intended to contribute to effective enforcement in practice.

G. Common provisions

Delegations are invited to provide feedback on the following:

(a) Whether the technologies should be independently audited (as the EP mandate indicated)? Who would pay for these audits?

The Netherlands strongly supports independent audits of CSAM detection technologies. Audits are essential to verify effectiveness, identify bias and false positives, ensure compliance with legal requirements, and strengthen cybersecurity. Transparent audit reports are also crucial for rebuilding public trust in this Regulation. We believe Member States would be willing to contribute to a robust and credible audit framework.

(b) Any other aspects of the text on Articles 9, 10, 11 and 50(1).

Under Article 10(6)(d), human oversight is required to ensure that the technology functions with sufficient reliability and to intervene in case of potential errors, including potential grooming of children. However, no conditions are linked to the design and implementation of this human oversight. Safeguards such as a four-eyes principle, logging of access and review actions, confidentiality obligations, and statistical reporting requirements could be added.

Furthermore, under Article 10(7), users are not to be informed of a detection order where such disclosure would undermine its effectiveness. However, no maximum time limit is set for such non-disclosure. The Netherlands questions whether the absence of any temporal limitation in this regard is desirable.

POLAND

General comments

- **Poland can support the direction of the Presidency compromise proposal, in particular the distinction between regimes applicable to publicly accessible and non-publicly accessible content, the exclusion of obligations that would weaken or circumvent end-to-end encryption, and the move away from general scanning towards targeted instruments.** The adoption of the CSAR remains important for creating stable EU-wide rules, improving cooperation with providers, the EU Centre, Europol, national authorities and specialised hotlines, and strengthening the protection of children against repeated victimisation.
- **Poland can support the proposed definition of "publicly accessible content" based on the approach used in the TCO Regulation, as this promotes consistency of EU law**. However, the recitals or future guidelines should clarify how content that is not publicly accessible should be understood, in particular with regard to closed groups, cloud services and interpersonal communication services. The practical application of the definition should also take account of semi-open spaces, such as easily accessible groups, channels, forums, file directories or spaces accessible after simple registration or automatic admission.
- **Poland's key concern is that it cannot accept any solution that would lead to mass, generalised or indiscriminate scanning of information that is not publicly accessible.** Therefore, Articles Z/Z+2 on own-initiative searches by providers require particular caution. Without a clear limitation of their scope, they could be interpreted as opening the door to broad scanning of non-public content, including content stored in cloud or hosting services. **This point should be explicitly clarified in the negotiations.**
- With regard to own-initiative searches, the preferred option should be to limit such activities at least to known CSAM, subject to prior notification of the EU Centre, the use of technologies

compliant with Article 10, human oversight, effective redress mechanisms, and the possibility for the competent authority to suspend such activities.

- In the case of detection orders concerning content that is not publicly accessible, the decision should be subject to a high safeguard standard and should preferably be taken by a judicial authority. The concept of "clear indications" should be further clarified in order to avoid an overly broad interpretation and unequal treatment of users. Such indications may include, where lawfully obtained and properly verified, reports from users, providers, national authorities, the EU Centre and specialised hotlines.
- **Detection orders concerning non-public content should remain strictly targeted at specific users or clearly identified groups of users in respect of whom there are lawfully obtained and clearly defined indications of a link to CSAM or grooming. This targeting is essential to distinguish the proposed model from general monitoring of private communications and to preserve proportionality.**
- As regards the material scope of the instruments, known CSAM should constitute the minimum scope of all relevant mechanisms. New CSAM may be considered where stronger technological safeguards, data protection impact assessment, human oversight and mechanisms limiting false positives are ensured. However, given the current level of grooming-detection technologies and the potentially significant number of false positives, particular caution is required before including grooming in detection orders concerning content that is not publicly accessible.
- Poland also underlines the importance of safeguards concerning detection technologies. Technologies used for detection should be secure, proportionate, effective, as minimally intrusive as possible, and subject to appropriate human oversight and error-limitation mechanisms. Independent audits are desirable, especially for technologies used to detect new CSAM or grooming; for technologies made available by the EU Centre, a central EU-level audit could help ensure consistency and avoid duplicating costs for providers.

SPAIN

A. Scope of the detection/searches

We consider that the scope of application should not be altered, particularly given the exponential rise in grooming cases in recent years. Flexibility? Perhaps this would involve removing the ban on grooming, but in exchange for something of value, such as allowing the voluntary detection of providers in both public and restricted-access areas, for both known and new material.

B. Definitions

We agree with the definition of "content that is publicly accessible" and, based on that definition, we should consider what constitutes "non-public content" but the difference must be very clear.

C. Own-initiative searches on content that is <u>not</u> publicly accessible – Article Z

We perfer to include known material, new material and grooming.

D. Detection orders for content that is publicly accessible – Article X

(a) *The conditions for issuing the order under Article X; When there is content accessible to the public.*
(b) *The appropriate authority to issue the order, and whether there could be flexibility on this point, including on whether there might be scope to reach a compromise by having independent administrative authorities (in addition to judicial authorities) issuing these orders; We can be flexible regarding the authorities.*

E. Detection orders for content that is not publicly accessible – Article Y

(a) *the types of authorities involved in the issuing of the detection order for non-public content and whether such orders could be issued by all Member States or only by the Member State in which the provider is established; To avoid problems, it would be preferable for the search warrant to be issued by the country in which the provider is established (even if this is at the request of another country)*
(b) *the text proposed for the detection order;*
(c) *the scope of material (known, new CSAM and/or grooming), of the users concerned and how this scope might interact with own-initiative detection, for example: would it be appropriate/necessary to allow own-initiative detection by providers, while in parallel having a detection order regime that has more restrictive conditions? We consider this to be consistent, as these are different yet complementary areas.*

F. Searches by the EU Centre – Article 49

(a) *Whether they can accept to give the EU Centre such a power to complement detection/searches by providers. YES*
(b) *The scope of the EU Centre's powers in this regard – should it be limited to searches for 'known' CSAM as per the EP mandate or should it also be able to scan for 'new' CSAM and/or solicitation of children? The three types, known, new and grooming,*
(c) *Whether the EU Centre should be required to use technologies that meet the requirements of Article 10 when conducting those searches. YES*
(d) *Any other comments on the suggested wording of Article 49 (1)(ba).*

G. Common provisions

(a) *Whether the technologies should be independently audited (as the EP mandate indicated)? Ok, it adds transparency. Who would pay for these audits?*

SWEDEN

Sweden reserves the right to comment further on this subject matter, all comments below are subject to change.

General comment: the disposition of the text and the general content of the articles seem reasonable at this stage, however more time is needed for analysis.

On scope: since the text does not include scope at this point, making a holistic analysis of the text is challenging. Sweden reiterates that the voluntary detection of new CSAM (including grooming and traffic data) is required to stop ongoing abuse and detect new victims.

For law enforcement, new material is essential for identifying offenders and protecting victims. Equally, identifying grooming behaviour enables earlier intervention and helps prevent abuse before it occurs (rather than responding only after abuse has taken place).

In our view, both the EU-center and law enforcement will rely on the continuous identification of new material. Without this ongoing process, existing databases would rapidly lose their operational value and effectiveness. Limiting detection to known content reduces the ability to respond to emerging threats and undermines efforts to protect all victims. Effective tools are therefore critical both for removing harmful material and supporting timely law enforcement action. To summarise: without continuous identification of new material, both investigative capabilities and detection systems degrade over time.

The issuance of orders: (for blocking, deleting, delisting and detection orders for content in public spaces as suggested in article X) should be handled by the responsible authorities designated by MS. The EP's proposal that these should be handled solely by judicial authorities is not acceptable for SE. Such a decision would entail unreasonable processing times in terms of handling, which would be detrimental for efficiency.

Article 10(5)(b): SE suggests that the word "patterns" be replaced by "evidence" for better precision.

Article X: SE maintains that MS Coordinating Authorities should be allowed to decide on the issuance of detection orders for content in public spaces, in order for efficiency (see rationale above) and the absence of risking privacy infringements.

Article Y: "specific users" is an improvement from previous proposals for "suspects". However, this is still not optimal as it risks overlapping with existing coercive measures such as seizures and forensic analysis. On one hand, this tool could be useful and serve as a complement (identifying material that has not been found during seizure, identifying the material remotely, e.g. in cloud services), but there is a great risk that it will not be used in practice due to the complicated process. Although SE is not against the article in principle, MS needs to be aware that this can prove to be underused (or not used at all) operationally. In our view, this still needs some discussion and focus among MS.