Council of the European Union
General Secretariat

Brussels, 20 March 2025

Interinstitutional files:
2022/0155 (COD)

WK 3471/2025 INIT

LIMITE

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

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Feedback from Member States

Delegations will find in the Annex the feedback from Member States following the meetings of the Law Enforcement Working Party (Police) of 5 February and 11 March 2025.

ANNEX

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

20 March 2025

Table of contents

AUSTRIA

A. Comments of 03.2025

We would like to thank the Presidency for the efforts and the opportunity to submit written comments on the Presidency's compromise text. Please kindly note that the comments below are preliminary and therefore we reserve the right to submit further comments.

1. Obligations for provider

- We expressly support the Presidency's statement that **preventive measures must not result in a *de facto* obligation to detect**. It is necessary, that a legal basis on the measures foreseen in Art 4a on the voluntary detection is well defined.

  However, there appears to be sufficient room in comparison to the current legal framework for additional effective preventive measures, such as mandatory risk assessment, age verification, content moderation, simplified reporting options, cooperation, knowledge exchange and information distribution through the EU Centre, which is to be set up for this purpose.
- The authorities' powers to oblige providers to comply with the preventive measures should be strengthened. To issue recommendations seems not sufficient.
- We suggest that the regulation should not only refer to 'prevention' in general. Therefore, the term 'risk mitigation' as well as the previous text of Art 5a (1) and (2) should be reinstated.
- The user notification mechanism laid down in Art 12 (3) should apply to all providers in order to avoid that offenders use other platforms.

2. Scope and organisation of the exemptions from certain provisions of Directive 2002/58/EC

- *How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?*

- The insertion of the passage in **Art. 4a para. 4** is expressly **supported** and should also be retained in future revisions.
- However, it should again be noted in this context that the preventive measures must not result in a *de facto* obligation to disclose.
- If the exemption continues to be incorporated in Art. 4a, it is **not at all clear** how and why the CSAM Interim Regulation (with the same content) should continue to apply at the same time. The simultaneous application of almost identical regulations only leads to misunderstandings and legal uncertainty.
- In order to address the problem that the EU Center will need time to create a list of indicators, it would seem to be a better solution for the relevant provisions (Art. 4a para. 3 lit. b and lit. c sub. lit. vii) to enter into force at a later date. Art. 88 should therefore be deleted and an adapted entry into force provision should be included in Art. 89 instead.

- We support the intention to **strengthen the rights of data subjects** under Art. 4a in addition to the rights of data subjects under the GDPR. To this end, information and transparency regulations could be added, e.g. comparable to Art. 19 of Regulation 2024/900, which obliges providers to make information about the technologies used and preventive measures public.

  - *Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?*

- We should avoid the parallel application of congruent provisions. Therefore, we agree to include the currently temporary provision of the Interim Regulation in Art 4a of the CSA Regulation.
- It is necessary to avoid a legal loophole through the expiry of the Interim Regulation without an appropriate solution in the CSA Regulation.

  - *Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.*

- The material scope of the exemption should be kept in its current form.
- In line with the previous AT position, we emphasise, that risk mitigation measures as well as voluntary measures to detect CSAM must under no circumstances result in a de facto detection obligation in coherence with data protection legislation and fundamental rights.

3. Use of technologies by providers

  - *How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?*

- In view of rapid developments in the area of information security, technology-neutral provisions for the implementation of security standards by providers are required.
- In this context, the provisions of the DSA and the GDPR must be adhered to.
- As already stated in point 1, it should be clarified that the definition of preventive measures and the provision of technologies to detect CSAM must not result in a *de facto* obligation for providers to detect CSAM.
- In this context, **Art. 1 (5) and Art. 1 (6)** are essential provisions that should be retained unchanged.
- As already stated in point 2, the insertion of the passage in Art. 4a para. 4 is expressly supported and should also be retained in future revisions.
- We support the proposal that the EU Centre must (not only could) **consult with the EDPB and/or the EU Technology Committee** before making technologies available. The current wording in Art. 53a para. 1 does not appear sufficient in this regard. However, the way in which the EDPB's should best be involved in the process could still be determined later, be it through formal opinions on each individual technology or in a more flexible way.

- *Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?*

– An overview of the technologies would be very helpful. However, we recommend drawing attention to a sensitive handling concerning the publication of the updated overview of the technologies currently used by the providers to avoid a possible misuse by offenders.

BULGARIA

A. Comments of 02.2025

Bulgaria would like to thank the Presidency for the efforts to find a compromise on the texts of the proposal for a Regulation on preventing and combating sexual exploitation of children through the proposed innovative approach. We agree that prevention should be part of the proposal, but the text should also maintain its focus on the prosecution of cases of online sexual exploitation.

We welcome the preservation of the possibility of voluntary detection of materials containing online sexual exploitation of children by providers. At the same time, we continue to share the view that imposing the obligation to detect would have significant added value in achieving the objectives of the Regulation. It should be noted that in practice, a very small number of providers voluntarily initiate measures to remove such content and in most cases do so after an order from law enforcement authorities. We believe that it is of utmost importance to introduce strict requirements for providers, in order to ensure the counteraction and prevention of this type of crime.

With regard to risk assessment, we believe that the proposed texts and the obligation for the assessment to be carried out solely by the providers cannot guarantee the same level of quality, given the different capacities of each provider. This hides risks of reporting incorrect data. We see the solution to this issue by providing a possibility of some kind of monitoring by law enforcement authorities of the assessment carried out by the providers.

Bulgaria does not support the complete exclusion of content from encrypted channels from the scope of the Regulation. We believe that this is of key importance for the effective counteraction to this type of crime and therefore we are of the opinion that the current wording should be retained.

Overall, we are not convinced that the proposed amendments will ensure a sustainable counteraction to the distribution of materials containing scenes of sexual exploitation of children.

B. Comments of 03.2025

1. Obligations for providers

- *How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?*

In case the detection of CSA materials are excluded from the scope of the Regulation, the best way to prevent or reduce the risk should involve content moderation as well as other instruments (poping notifications to users, when possible grooming is detected, age verification, user reporting), with a view to limiting/preventing illegal content on the respective platform. All other preventive measures would hardly achieve a serious limitation of criminal content on the respective platforms. However, it should be taken into account that if a provider is to moderate content that is not public/distributed between two users regardless of their age or in private groups, this would be considered privacy intrusion.

Additionally, the regulation's scope includes different types of service providers with different services offered. In this regard the different measures imposed would be more or less effective, because we cannot apply the same measures to the providers of hosting and interpersonal communication service. Therefore these measures should be service specific.

It should be noted that detection orders are the best instruments to mitigate risk and in order to ensure that the Regulation will be futureproof, the scope should include all kinds of communications.

- *Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?*

In this context, we believe that the use of the term "risk mitigation" is more correct, since prevention should rather be aimed at children who could become victims of sexual exploitation, as well as perpetrators. We believe that regardless of the preventive measures that may be imposed, without the use of technologies to counteract and reduce the risk, the problem would be difficult and inefficient to solve.

- *Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?*

We prefer the previous version of Article 5a (1).

- *Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?*

In order to limit content with child abuse, we believe that the notification mechanism should be available on all services where there is a risk of dissemination. It should be noted that this is likely to help reduce the sharing of child sexual exploitation footage, but will not affect situations where two people with common interests share material with each other.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

- *How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?*

If the Council Legal Service does not see any legal obstacles, the inclusion of these provisions in the Temporary regulation would not be a problem.

- *Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?*

We are of the opinion that the discussions should continue. We look forward to a solution that will allow for the timely adoption of the necessary texts, so as to avoid a legislative gap.

- *Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.*

We believe that the scope could be extended if this would contribute to a more effective detection of illegal material. The scope of voluntary actions should not be limited to certain content.

3. Use of technologies by providers

- *How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?*

The technologies used for the purposes of the regulation should be neutral. They may be newly developed or already existing, but they should be approved/certified by the EU Center, the European Commission, or other competent institutions. It is important that their effectiveness is proven, and for this purpose the experience of numerous companies involved in developing technologies to combat the sexual exploitation of children can be used.

- *Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?*

We support the proposal the Commission to prepare an updated overview of the technologies currently used by providers under the derogation regime and to provide information on existing technologies for detecting grooming, without reducing the substance of the content.

4. Reducing complexities and administrative burden

- *How do you see the best way of reducing complexities and administrative burden in this Regulation?*

The regulation must be as simple and clear as possible, and the provisions should be easy to interpret.

- *Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?*

The risk categorisation should not create confusion in the obligations of providers. There must be sufficient guarantees that the risk assessment has been carried out correctly by each provider. The risk categorisation would help to more easily exclude providers whose services do not pose a particular risk of distributing illegal material. However, the possible administrative burden related to the risk categorization should be considered as well.

The sign for redused risk could help parents in choosing relatively safe applications for children. In this hypothesis, we believe that it could have added value to the proposal. However, no application should be considered fully safe, unless it has proven that it has implemented the necessary measures to prevent the usage of its services for CSA.

- *Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?*

Bulgaria is of the opinion that if the EU Centre is replaced by different structures, detailed information should be provided on how this could be carried out, highlighting the benefits of these changes. We support the addition of additional more functions to the EU Centre, such as preparing a communication strategy. We are of the opinion that the functions of the EU Centre should be defined very precisely in order to avoid overlapping with the functions of Europol. It is important that sufficient efforts are also made to identify victims of sexual exploitation, as this is currently an important part of the solution to the problem of such materials.

5. Review clause

- *How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?*

The review clause is a good idea to address the most controversial elements of the regulation after gathering enough information. If such clause is designed it should be opted for maximum period of 3 years.

In our opinion, detection orders (at least for already known content) and encrypted content (with user consent) should remain a core part of the proposal.

- *How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?*

The development of technologies must take place with the participation of leading companies, which are already working in this area, in cooperation with the EU Center.

CROATIA

A. Comments of 02.2025

Croatia generally considers that the removal of the detection orders from the text is in total contradiction to the initial and key intention of adopting an effective EU legislative framework which would define and improve the protection and rights of children more permanently and protect their best interest. It is also important to keep in mind that the entire process of creating a new EU legislative framework to regulate this field has been initiated because it has already been established that the voluntary cooperation of internet service providers turned out to be insufficient. We are of the opinion that such a solution would neither improve the present situation or the existing legal framework, nor protect the children and provide an adequate level of protection in the future. A regulation that neither obligates, nor in any way encourages internet service providers to contribute and cooperate in combating child sexual abuse and exploitation can hardly be considered a progress in the combatting these crimes. Therefore, the current text proposed in document 5352/25, from which key elements of the originally proposed Regulation were deleted, is not acceptable.

Considering the time frame of the validity of the current Temporary Regulation (April 2026), the importance of adopting regulations that regulate this field and the fact that so far no compromise has been reached because of the provisions at issue that define mandatory detection orders, we can exceptionally support the PL PCY text with some necessary amendments.

The currently proposed text would be acceptable only in the context of finding a compromise solution provided that certain parts referring to specific obligations of service providers and to the process of voluntary disclosure itself are amended as follows:

- the service providers have to have clear obligations to contribute to the effective containment of CSAM and the solicitation of children, whereby the use of general terms that may be interpreted broadly, leaving open the possibility to do nothing, should be avoided;

- the obligation of risk assessment and risk mitigation should be retained;

- voluntary detection by a simple process should be ensured;

- sanctions in case of non-compliance with the obligations of preventing the dissemination of CSAM should be defined;

- the role of EU Centre should be kept;

- encrypted services should be effectively included in the scope of the Regulation in the context of preventing the dissemination of CSAM, and it should be ensured that the service providers can voluntarily install “upload moderation”;

- the review clause should be kept.

As defined in **Article 4a, para 3(d)(vi)** of the currently proposed text, the materials that have not been previously identified as CSAM (new materials) are not reported to the EU Centre, law enforcement authorities or organisations acting in the public interest against child sexual abuse **without prior human confirmation**. Pursuant to the applicable positive regulations of the Republic of Croatia, child sexual abuse materials may only be examined by law enforcement institutions (police, prosecuting authorities, judicial authorities) for the purpose of conducting criminal investigations, and such verification is not possible.

It is therefore proposed, where national legislation does not allow for the aforementioned type of "human verification", to ensure the possibility of filing a report to the EU Centre, which would then verify the materials. It is proposed to add the following: „unless such verification is not possible by national legislation".

Article 4a, para 3(d)(vi)
(vi) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported to the EU Centre, law enforcement authorities or organisations acting in the public interest against child sexual abuse without prior human confirmation; unless such verification is not possible by national legislation

B. Comments of 03.2025

General comment

While appreciating the efforts of the PCY in creating a new text, it is important to bear in mind that the entire process of creating a new EU legislative framework that would regulate prevention and combatting child sexual abuse was initiated precisely because it had already been established that voluntary cooperation of Internet service providers has proven to be insufficient in protecting children online and combating the misuse of online services for the purpose of child sexual abuse.

Croatia generally believes that the removal of the detection order for CSA materials and grooming from the text of the Regulation is in complete contradiction with the original and key intention of adopting an effective EU legislative framework that would more permanently define and improve the protection and rights of children and protect their best interests. It is considered that such a solution is not a direction that will improve the currently existing regime, protect children and provide a sufficient level of protection for children in the future.

Croatia understands the need for compromise in order to reach an agreement, however, we believe that compromise need to ensure stronger and more effective measures than those which are currently in force, in order to ensure an effective fight against child sexual abuse.

1. Obligations for providers

Questions to delegations:

• How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

HR firmly believes that detection orders are the only effective mechanism to combat child sexual exploitation.

We consider that the text should include specific and clearly prescribed measures and responsibilities for service providers. If the provisions on detection orders are removed from the scope of the regulation, it is necessary to define the possibility of imposing obligations on service providers, as well as an effective mechanism to oblige service providers to take the responsibility in relation to the purpose of the use of their services and to take concrete actions to prevent CSA and child grooming content from being distributed on their services. Prescribing measures alone is unlikely to be sufficient as service providers will not apply them voluntarily. In this context, it would be necessary to enable national authorities to act adequately in this direction, to verify whether service providers are taking effective measures at their disposal to prevent abuse of the services they provide.

• Do you agree to keep the term “prevention” throughout the text as suggested by the Presidency or do you prefer to revert to the term “risk mitigation” as in the Commission proposal?

We are flexible in relation to the use of the terms "prevention"/"risk mitigation", and will support terminology that provides more adequate and stronger protection of children in the online environment.

• Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

• Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

We can support the proposal that the notification obligation applies to all services and service providers.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

Questions to delegations:

• How do you see the best way of designing the derogation from certain provisions of the e privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

• Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative

act to be amended and made permanent through this Regulation?

• Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

We consider it important to maintain the possibility of voluntary detection for service providers even after the deadlines set out in Regulation (EU) 2021/1232, regardless of the way in which this is implemented. Moreover, we would like to maintain flexibility concerning the manner in which we will implement this.

3. Use of technologies by providers

Questions to delegations:

• How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

We can support technologically neutral solutions. In this context, it is necessary to ensure that no type of service is excluded from the scope of the Regulation. We believe that the existence of an encrypted communication service cannot be a reason not to provide children with adequate protection in such an environment. By omitting encrypted communication from the scope of the Regulation, we risk creating a safe haven for perpetrators of this type of crime, within which perpetrators can freely abuse children without fear of being detected or prevented. We advocate the

use of technologies that will ensure and protect cybersecurity, but also enable the protection of children in such an online environment. In this context, it is important to emphasize that we are already witnessing significant changes in the way these crimes are committed, and it can be concluded that a large proportion of perpetrators use encrypted communication channels for sharing the CSAM and are thus simply beyond the reach of law enforcement authorities.

• Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

We can support that COM makes an updated list of technologies which are currently being used.

4. Reducing complexities and administrative burden

Questions to delegations:

• How do you see the best way of reducing complexities and administrative burden in this Regulation?

• Do you agree to keep the risk categorization and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

According to the current draft text, detection orders are out of the scope. If detection is kept voluntary, risk categorization will not provide added value to the text and in that case it is possible to omit such obligations. This would also ensure a reduction in the administrative burden.

• Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

We can support keeping the establishment of an EU Centre. We believe that the role of the EU center, besides giving strong support to MS in the fight against child sexual abuse, is also to function as a kind of center of excellence in this area.

5. Review clause

Questions to delegations:

• How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?

• How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?

We can support the provision on the review clause, and given that technology is changing very quickly, perhaps the deadlines should be even shorter than 3 years. In this context, the provisions on the establishment of a Technology Committee in the text of the Regulation are welcome and necessary.

CZECH REPUBLIC

A. Comments of 03.2025

The Czech Republic continues to have a scrutiny reservation on the PL PRES compromise proposal (issued under No 5352/25).

An issue that is still debated at national level is the scope of regulation and protection of end-to-end encryption. As regards encrypted communications, the proposal seems to be moving in the right direction.

- Ad 1) According to the Czech Republic, the key issue is the decision of the Member States whether the detection of CSAM will continue to be voluntary, as in the case of the so-called Interim Regulation, or whether the detection based on detection orders issued by the court will be limited to certain types of CSAM. In any case, the Czech Republic is of the opinion that the notification obligation should apply to all relevant providers, not only to high-risk services.
- Ad 2) It is not possible to have a legal vacuum in case of expiration of the Interim Regulation and at the same time it is desirable to have permanent legislation in the future as has been decided by Member States on several occasions in recent years. The current proposal for a Regulation contains not only possible obligations for online service providers, but also an obligation for Member States to establish a network of national competent authorities headed by a coordinating authority and to regulate the procedural amendments in the event of CSAM appearing on a provider's services. It also regulates the establishment of the EU Centre. There is, therefore, no reason to create a separate proposal which will be linked to the Interim Regulation, but it is desirable that one permanent legal act also regulates the scope of what it proposes.
- Ad 3) The Czech Republic would welcome a list of current technologies, as the seminar on technologies held during the Czech Presidency has been long time ago.
- Ad 4) Administrative burden can be expected especially at the beginning of the system launch. It cannot be avoided if we want to set up cooperation between providers, the national coordinating authority, the EU Centre and the Member States themselves.
- Ad 5) The EC has started collecting data according to a harmonised form, so in three years from the entry into force of the Interim Regulation it should have valid evidence-based information that are needed to decide whether it is needed to propose changes.

ESTONIA

A. Comments of 02.2025

We thank the Presidency for another drafted version and understand that it is intended to help move forward with CSAM before the temporary regulation expires. However, we acknowledge that from a child welfare perspective and to address this issue, the proposed version is likely to have a marginal impact and is not much different from the interim solution and situation proposed today. Additional comments:

1) draft article 2 f subparagraph (v) states that "relevant information society services" includes "online search engines". We have found the equivalent of this term in two places:

Article 2 (x) of the draft states that it is: '*online search engine' means an intermediary service as defined in Article 3, point (j), of Regulation (EU) 2022/2065*.

- content of the definition: *'online search engine' means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;*
- „intermediary service" as defined in Article 3(g)(iii) of Regulation 2022/2065;
- Directive (EU) 2022/2555 or the NIS2 Directive refers to another regulation: "online search engine" means an online search engine as defined in Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council. definitsiooni sisu: *'online search engine' means a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;*
- NIS2 refers to Directive (EU) 2015/1535 or Article 1(1)(b) of that Directive for "digital service".

If two pieces of EU legislation have the same definition for the same topic ("online search engine") then which reference should I prefer to use? Since both in the scoop of this draft also include "online search engine". It is also subject to NIS2 requirements.

2) In regards to "hosting service"

- its content/explanation in Regulation 2022/2065 is as follows: 'intermediation service' - one of the following information society services: (iii) a 'hosting' service consisting in the storage of information provided by and at the request of the recipient;
- if one reads Article 6 of the NIS2, it is defined in paragraphs 32 and 33:

(32) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(33) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

Do these entities, perhaps defined by NIS2, have any relation to this "hosting service" or not? Secondly, is it even necessary to make a connection to NIS2 in this draft? For example, in several places in the draft there are links to the General Data Protection Regulation, i.e. Regulation 2016/679, but from a cyber point of view there are no direct links to NIS2 (and by taking out the detection order topic, the cyber topics related to DO were also taken out) - so the question is, is there any need to make a link to NIS2? Or is there some need, given that both NIS2 and this draft seek to regulate, among other things, "online search engines"?

3) Article 4- previous texts used the word „risk mitigation“ mostly and now we see that the term is „preventive measures“. Is it only a change of wording or is it also a change of substance? The previous wording was perhaps a bit clearer for service providers, because the draft talks throughout about risk assessment, assigning a risk level to services or parts of services, etc. It is a logical extension that if a specific risk is identified, the à service provider will implement measures to mitigate that risk. Although preventive measures would also be linked to the risks identified, the fact remains that a service provider cannot fully prevent the misuse of its services and cannot be required to do so. However, the current wording would seem to create such an expectation. "The term 'prevention' also raises questions, for example, in relation to the evaluation of the measures (Article 25(7)(b) and (d)) - if risk mitigation is more or less straightforward, there is inevitably a suspicion that the effectiveness of prevention is more difficult and burdensome to measure.

4) Article 4a(6) of the draft introduces (maintains?) tasks for supervisory authorities- has the supervisory authorities and/or the European Data Protection Board been consulted on the content of this article?

5) Article 5(2b) - Obligation for high-risk service providers to contribute to the development of new technologies. What does this obligation actually mean? This question was also posed in the LEWP meeting autumn, but as far as we know there has been no answer . The point does say that the contribution will be proportionate to the 'financial, technical and operational capacity' of the provider, but it does not say what activities and to what extent the provider is expected to contribute. It is not good practice to include open-ended, unspecified commitments.

6) Article 13(1a) - Reporting of cases involving a risk to the health or life of a child to the EU Centre and its requirements. Such cases are also covered by Article 18 of the DSA, which requires the service provider to report directly to the member states law enforcement or judicial authority or, in certain cases, Europol. For the sake of clarity, the draft CSAM article could be complemented and aligned with Article 18 of the DSA that the service provider must report in parallel to the EU centre and the member state law enforcement or judicial authority/Europol. Also with regard to the temporal dimension of the case, the wording could be harmonised - Article 18 of the DSA says "Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place....", the content of the draft CSAM does not refer to the past ("there is likely to be an imminent threat to the life or safety of a child or when the information indicates ongoing abuse...").

7) Article 35- the words "fine", "penalty", "periodic penalty payment" are used interchangeably - is this ok and understandable? Or is it also necessary to include here in the recitals sentences similar to those in p. 151 of the GDPR?

8) Article 36(2) and (3) - "At the request of the EU Centre, where necessary to ensure the completeness, accuracy and timeliness of the data contained in the databases referred to in Article 44(1), the coordinating authorities shall verify with the competent authorities whether the conditions laid down in points (a) and (b) of paragraph 1 have been and, where appropriate, continue to be met in relation to the data submitted to a particular EU Centre in

accordance with that paragraph, or provide clarifications or additional information" - only the competent authority is meant here? Same thing for both paragraphs.

B. Comments of 03.2025

1. Obligations for providers

How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

Obligations for service providers should be clearly formulated and defined.

Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?

Risk mitigation. Prevention is a broader concept and requires knowledge of the theory to be effective. We cannot impose such a requirement on businesses and, furthermore, we cannot create a situation in which various activities start to be called and classified as prevention when they are not really prevention. Plus, the term "risk mitigation" is more in line with other digital and data economy regulations (e.g. AI Regulation, GDPR, DSA, NIS2), where such obligations are referred to as risk management.

Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

We propose a new wording which could be "may require". In our view, "may recommend" is too soft and does not achieve the desired result. "Shall require", on the other hand, creates a situation where we put on business pressure to find solutions in a situation where this may not be possible.

Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

A similar framework already exists today in the DSA Regulation. What is the added value of such wording in this draft?

2. Scope and design of the derogation from certain provisions of Directive 2002/58/

How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

Our general view on all these 3 questions is that all legal regulatiosn could be reflected in one piece of legislation. We would like the scope of the ePrivacy Directive exemption in the new CSA Regulation to be analogous to the scope of the provisional Regulation (EU) 2021/1232.

3. **Use of technologies by providers**

How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

EE's position is that the encryption must not be broken, so the wording in the text is OK for us. For us, it's okay if privacy-preserving technologies are used that do not break the encryption. We are fine with technology neutrality.

In particular, we would like to point out that considering that E-privacy regulation has been withdrawn it poses a possibility to set the principles for the use of technological solutions in a general act, rather than being topic-specific. Otherwise we will start regulating possible technological solutions (for example E2EE) in each specific regulation.

Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

Yes we agree.

4. **Reducing complexities and administrative burden**

How do you see the best way of reducing complexities and administrative burden in this Regulation?

If detection arrangements are removed from the proposal, the risk-based approach and the reduced risk label should also be removed from the proposal as they no longer add value. At the same time, further risk assessment and identification, e.g. via the EU Centre, should remain if needed. We believe it is important to minimise the number of pieces of legislation that regulate essentially the same things.

Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

The reduced risk label has no added value if we remove the detection order.

Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

We are not opposed to the Centre per se, but we still do not have a clear understanding which role it will have. We have repeatedly expressed our wish to be involved in the discussions about the centre process logic.

We have also said that for us it is important that the work in the EU centre will not duplicate the work of other agencies. At the moment it is not clear what the exact tasks would be. There would be added value if there was research centre, advice on technologies, support on education among schools and

parents and a meaningful form of prevention work. The centre should not just play the role of information exchange.

5. **Review clause**

How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?
It is important for us that the Commission would reevaluate the regulation and therefore we support the review caluse although we understand that it does not oblige the Commission to do so.

How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?

In any case, from an EE perspective, the EU could be encouraged to take a more proactive stance, in cooperation with the technology sector and academia, in seeking and investing more seriously in the development of privacy-enhancing technologies, including by already cooperating in the process of developing sectoral standards (ETSI, ICT, etc). If cooperation starts at an early stage (on a "grass level" so to say) then service providers understand our needs better and would be willing to negotiate on a voluntary basis.

FINLAND

A. Comments of 02.2025

- The compromise proposal replaces the mandatory detection order for service providers with a voluntary-based model. FI considers this new approach to be better than the previous one, taking into account the problems in the previous model regarding fundamental rights.

- The direction of the PCY's compromise text is correct, and we support the further development of this proposal. FI's experts believe the proposal contains several important aspects that could enhance the fight against CSA.

- FI emphasizes that in the further work, we must ensure that the EU Charter of Fundamental Rights is properly taken into account.

- At the LEWP-meeting on 5th February the Council's Legal Service pointed out that the proposal should be examined from the perspective of whether it would lead to general and indiscriminate access to the content of messages. Finland also draws attention to this matter. In particular, we are unclear about the intent behind the wording "would require" in Article 1(6), and what its implications are for the entire regulation? Are we interpreting correctly that this wording would allow general and indiscriminate content filtering, even though companies are not mandated to do so? Finland is still assessing the text but is already sharing the following text proposal for consideration by the PCY:

  6. This Regulation shall not create any obligation that would ~~require~~ allow a provider of hosting services or a provider of interpersonal communications services to use technologies to detect or filter online child sexual abuse in generalised and indiscriminate manner.

- According to the proposal, each case would need to be reported not only to authorities but also to NGOs that protect the interests of children. What information would be reported to these organizations? Do they have a legally based task for which the information would be reported? Do they have a processing basis required by data protection regulation? At the same time, Finland notes that these organizations play a significant role in combating child sexual abuse, and this should be taken into account in such a way that the legislation does not create obstacles for their activities.

- FI is interested in hearing more information about the technologies referred to in Article 4a, paragraph 3(c).

- FI welcomes the elements included by the Presidency in the compromise text to strengthen the protection of data subjects under the GDPR. However, FI draws attention to the unclear relationship between Article 4a of the text and Article 22 of the GDPR. In particular, the unclarity is caused by points (v) and (vi) of paragraph 3(d). Whereas point (v) suggests that

the use of detection technologies would be entirely automated, and "human intervention" would only occur where necessary, point (vi) requires "human confirmation" always before reporting the detected material. FI would welcome clarification as to whether the use of automated technologies would be considered automated decision-making or profiling meant in Article 22 of the GDPR, and particularly whether "human intervention" in point (v) means the same safeguard as in Article 22 of the GDPR. (It would also be useful to ensure consistency of terminology whenever the same type of human action is meant in the different subparagraphs.)

In any case, irrespective of whether automated decision-making or profiling is meant, FI considers it important to include adequate safeguards for the rights of the data subject. In addition to those proposed by the Presidency, it could be useful to add e.g. "meaningful information about the technology used" in paragraph 3(d)(viii) (as in the deleted Article of the compromise text discussed last year). That would ensure that data subjects are aware of the nature of the detection measures.

B. Comments of 03.2025

FI proposal

Section 1a

Measures for voluntary detection

Article 6a – Derogation from Directive 2002/58/EC for voluntary processing

1. Articles 5(1) and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that:
   (a) the processing is:
      (i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it to [the EU Centre], law enforcement authorities and to organisations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to [the EU Centre], law enforcement authorities or organisations acting in the public interest against child sexual abuse;
      (ii) proportionate and limited to technologies used by providers for the purpose set out in point (i);
      (iii) limited to content data and related traffic data that are strictly necessary for the purpose set out in point (i);
      (iv) limited to what is strictly necessary for the purpose set out in point (i);
   (b) the providers ensure that the technologies and safeguards applied are in full conformity with the requirements set out in Article 6b.
   (c) in respect of any specific technology used for the purpose set out in point (a)(i) of this paragraph, a prior data protection impact assessment as referred to in Article 35 of

Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation have been conducted;

(d) the providers:

(i) have established appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views;

(ii) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC concerning the confidentiality of users' communications for the sole purpose set out in point (a)(i) of this paragraph, the logic behind the measures they have taken under the derogation and the impact on the confidentiality of users' communications, including the possibility that personal data are shared with law enforcement authorities and organisations acting in the public interest against child sexual abuse;

(e) where suspected online child sexual abuse has been identified, the content data and related traffic data processed for the purpose set out in point (a)(i), and personal data generated through such processing are stored in a secure manner, solely for the purposes of:

(i) reporting, without delay, the suspected online child sexual abuse to the competent law enforcement and judicial authorities or organisations acting in the public interest against child sexual abuse;

(ii) blocking the account of, or suspending or terminating the provision of the service to, the user concerned;

(iii) creating a unique, non-reconvertible digital signature ('hash') of data reliably identified as online child sexual abuse material;

(iv) enabling the user concerned to seek redress from the provider or pursue administrative review or judicial remedies on matters related to the suspected online child sexual abuse; or

(v) responding to requests issued by competent law enforcement and judicial authorities in accordance with the applicable law to provide them with the necessary data for the prevention, detection, investigation or prosecution of criminal offences as set out in Directive 2011/93/EU;

(i) the data are stored no longer than strictly necessary for the relevant purpose set out in point (h) and, in any event, no longer than 12 months from the date of the identification of the suspected online child sexual abuse;

(j) every case of a reasoned and verified suspicion of online child sexual abuse is reported without delay to the competent national law enforcement authorities or to organisations acting in the public interest against child sexual abuse.

Article 6b Technologies and safeguards

1. Providers of number-independent communications services shall put in place safeguards to ensure that the processing based on Article 6a is limited to what is strictly necessary and justified to the purpose of this derogation.

2. The providers shall:

(a) establish technical and organisational measures to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data processed in accordance with this Regulation,

(b) record, in respect of any processing of content and other data pursuant to Article 6a, necessary information for the verification of the lawfulness of the processing, such as the time and duration of the processing and, where applicable, the person performing the processing. Such logs shall only be used for the of the lawfulness of the processing, for self-monitoring, for ensuring data integrity and data security as well as for the purposes of criminal or disciplinary proceedings;

(c) keep the information contained in the logs referred to in point (ii) for no longer than necessary for the applicable purpose and, in any event, no longer than five years from the date of the measures taken that led to the obligation to preserve the information recorded in those logs. They shall subsequently irrevocably delete the information;

(d) keep the logs referred to in in point (b) for a further specified period if requested by the competent authority or court, set by that the requesting authority or court, where and to the extent necessary for one of the purposes referred to in point (b);

(e) diligently identify, analyse and assess the cybersecurity risks that could be introduced by the technologies used for detection, and take all reasonable mitigation measures, tailored to the possible cybersecurity risk identified, to minimise that risk;

(f) ensure human oversight of and, where necessary, human intervention in the processing of personal and other data using technologies falling under this Regulation;

(g) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported to the EU Centre, law enforcement authorities or organisations acting in the public interest against child sexual abuse without prior human confirmation.

3. The technologies used for the purpose set out in Article 6a, point (a)(i) shall meet the following conditions:

(a) are effective and suitable in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable,

(b) are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679,

(c) 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;

(d) do not introduce cybersecurity risks for which it is not possible to take any effective measures to mitigate such risk;

(e) are subject to a prior data protection impact assessment as referred to in Article 35 of Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation;

(f) with regard to new technology used for the purpose set out in point (a)(i) of this paragraph, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services in the Union before 2 August 2021, and with regard to technology used for the purpose of identifying possible solicitation of children, the provider shall report back to the competent authority on the measures taken to demonstrate compliance with written advice issued

in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation ('supervisory authority') in the course of the prior consultation procedure;

(g) are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online child sexual abuse and, where such occasional errors occur, their consequences are rectified without delay;

(h) in the case of technologies used to detect patterns of possible solicitation of children, are limited to the use of relevant key indicators and objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication, without prejudice to the right to human review.

4. The use of the technologies made available by the EU Centre shall not affect the responsibility of the provider to comply with the requirements set out in paragraph 3 and for any decisions it may take in connection to or as a result of the use of the technologies.

Article 6c Effective judicial remedies

1. In accordance with Article 79 of Regulation (EU) 2016/679 and Article 15(2) of Directive 2002/58/EC, users shall have the right to an effective judicial remedy where they consider that their rights have been infringed as a result of the processing of personal and other data for the purpose set out in Article 6a(1), point (a)(i), of this Regulation.

2. The providers shall inform the users of the following:

(a) the avenues for seeking redress from them;

(b) the possibility of lodging a complaint with a supervisory authority; and

(c) the right to a judicial remedy;

Article 6d Reporting on the processing of personal data

1. The providers shall, by 31 January [year after the entry into force of this Regulation] and every year thereafter, publish and submit to the competent supervisory authority, the Coordinating Authority of establishment, the Commission and the EU Centre a report on the processing of personal data under this Regulation, including on:

(a) the type and volumes of data processed;

(b) the specific ground relied on for the processing pursuant to Regulation (EU) 2016/679;

(c) the ground relied on for transfers of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable;

(d) the number of cases of online child sexual abuse identified, differentiating between online child sexual abuse material and solicitation of children;

(e) the number of cases in which a user has lodged a complaint with the internal redress mechanism or with a judicial authority and the outcome of such complaints;

(f) the numbers and ratios of errors (false positives) of the different technologies used;

(g) the measures applied to limit the error rate and the error rate achieved;

(h) the retention policy and the data protection safeguards applied pursuant to Regulation (EU) 2016/679;

(i) the names of the organisations acting in the public interest against child sexual abuse with which data has been shared pursuant to this Regulation;

2. The data included in the report referred to in this point shall be provided in writing by means of the standard form set out in Implementing Regulation (EU) 2024/2916. For amending the standard form, implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 87.

Article 6e Supervisory authorities for processing of personal data under Article 6a

The supervisory authorities designated pursuant to Chapter VI, Section 1, of Regulation (EU) 2016/679 shall monitor the processing pursuant to Article 6a in accordance with their competences and powers under that Chapter.

FRANCE

A. Comments of 02.2025

Pour faire suite à la réunion LEWP-P du 5 février, les autorités françaises adressent à la Présidence et au Secrétariat Général du Conseil les commentaires suivants au sujet de la version de compromis sur le Règlement « Abus sexuels sur mineurs ».

En préambule, les autorités françaises expriment leurs regrets de voir le texte vidé d'une grande partie de sa substance, avec la suppression de l'injonction de détection. Elles estiment que la valeur ajoutée de ce texte se limite désormais à pérenniser la détection volontaire existante. Dans une optique d'efficacité et de lisibilité, il apparaît donc nécessaire de limiter le règlement à cet objectif et de supprimer une grande partie des autres dispositions du texte, inutilement complexes et coûteuses à présent que la détection n'est plus obligatoire.

Le système de détection volontaire s'avère largement insuffisant pour lutter contre les abus sexuels sur enfants en ligne, comme en témoignent les chiffres alarmants de ces dernières années. Par conséquent, les autorités françaises, encouragent la Commission à proposer, à court terme, un nouveau texte qui permette de répondre aux enjeux opérationnels de protection des enfants en ligne.

De manière plus détaillée, elles estiment que la version de compromis doit être modifiée sur les points suivants :

1. Renforcement des obligations de prévention

Une obligation de prévention effective doit être clairement énoncée. Dans le cas contraire, les prestataires pourraient prétendre avoir pris des mesures de prévention, quelle que soit leur efficacité. A cet égard, les autorités françaises préconisent les reformulations suivantes :

- Article 1(a):

(a) obligations on providers of relevant information society services to ***make best efforts to*** **effectively prevent the use of** their services for online child sexual abuse;

- Article 4(1):

(1) If providers of hosting services and providers of interpersonal communications services have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall put in place appropriate and proportionate measures, tailored to that risk, to ***effectively*** prevent online child sexual abuse in their services. […]

Les mesures de prévention que les fournisseurs pourraient prendre ne doivent pas être indûment limitées et les entreprises doivent pouvoir prendre toute la gamme des mesures de prévention. Cela inclut les mesures de prévention qui nécessitent l'accès aux métadonnées ou à toute autre donnée stockée dans l'appareil, exclusivement dans le but de prévenir les abus sexuels d'enfants en ligne. Par conséquent, les références à l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques » figurant dans le document devraient être rétablies et incorporées au besoin dans le compromis, notamment en ce qui concerne le nouvel article 4a :

- Article 1(4):

4. This Regulation limits the exercise of the rights and obligations provided for in Article 5(1) ***and (3)*** *and Article 6(1) of Directive 2002/58/EC to the extent strictly necessary in accordance with Article 4a.*

- Article 4a(3):

3. Regarding the scope of the derogation, Articles 5(1) ***and (3)*** and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that: […]
3(d)(viii): inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) ***and (3)*** and 6(1) of Directive 2002/58/EC […]

Enfin, l'autorité de coordination doit avoir la possibilité d'exiger du fournisseur de service qu'il prenne des mesures supplémentaires si les mesures proposées initialement par le prestataire ne sont pas suffisantes. Pour ce faire, le texte de l'article 5a qui avait déjà été approuvé devrait être rétabli, faute de quoi les pouvoirs des autorités nationales pour veiller à ce que les prestataires respectent l'obligation de prévention seraient indûment limités.

- Article 5a :

1. Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it ***shall require*** ***may recommend to*** the provider of […].
The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to ***recommend*** ***require*** pursuant to the first subparagraph.

2. A provider that ***is required to*** perform***s*** the actions specified in points (b) or (c) of paragraph 1 shall re-conduct […].

En tout état de cause, l'essentiel est qu'il y ait une obligation claire de prévention (obligation de résultat) et des pouvoirs d'exécution pour les autorités nationales (comme ils sont déjà inclus). Ces pouvoirs garantissent que les autorités nationales peuvent imposer des amendes et même la

suspension du service en cas de non-respect par le prestataire de la prévention effective des MSTC et du toilettage.

Enfin, il faudra que ces mesures de prévention concernent également les familles, les jeunes enfants et soient élargies aux auteurs (notamment afin qu'ils soient sensibilisés aux peines encourues).

3. Avenir du Centre de l'UE

Les autorités françaises constatent que deux missions structurantes du centre de l'UE, dans lequel elles avaient placé beaucoup d'espoir, n'existent plus. Il s'agit d'une part du tri des faux positifs que les personnels du Centre devaient prendre en charge dans le cadre des injonctions de détection ; et d'autre part de l'étude et de l'approbation des technologies de détection qui devait être mises à disposition des fournisseurs de services. Dès lors, elles considèrent que les fonds (coûts ponctuels estimés à 5 millions d'euros et coûts annuels estimés à 25,7 millions d'euros selon l'étude d'impact) et les moyens humains (113 personnels selon l'étude d'impact) qui devaient être dédiés au Centre ne sont plus justifiés.

Elles plaident donc pour une réécriture complète des articles article 40 à 82 du règlement et pour que l'agence soit remplacée par une communauté d'experts et d'organisation (ONG de défense des mineurs, hotlines, représentants d'entreprises proposant des technologies de protection des mineurs sur internet, services répressifs spécialisés) à même de réaliser les missions d'aide aux victimes, de partager de bonnes pratiques et de réaliser des études et recherches prospectives sur l'état de la menace, les victimes et les auteurs.

En parallèle, Europol pourrait se voir confier l'hébergement de la base de données de contenus pédopornographiques. Néanmoins, les autorités françaises ne sont pas favorables à ce qu'Europol se voit octroyer des pouvoirs de cyber-patrouille et d'enquête sous pseudonyme, qui doivent demeurer des prérogatives nationales.

Enfin, le « EU Innovation Hub for Internal Security » pourrait être missionné pour accompagner la Commission dans la rédaction du rapport qu'elle devra publier trois ans après l'adoption du règlement pour évaluer la maturité et la précision de ces technologies, en publiant des études régulières à ce propos, comme il l'a déjà fait en 2024 sur le chiffrement ou l'intelligence artificielle.

4. Rapport de la Commission sur l'efficacité du règlement ASM

Les autorités françaises estiment que le règlement « Abus sexuels sur mineurs » doit être rapidement évalué après son adoption et qu'un autre texte devrait être proposé pour dépasser les limites opérationnelles qu'il ne manquera pas de rencontrer. Dès lors, elles soutiennent l'article 85-1a qui enjoint la Commission à présenter, au plus tard trois ans après l'entrée en vigueur du présent règlement un rapport évaluant la nécessité et la faisabilité de la détection du matériel pédopornographique et de la sollicitation d'enfants, y compris sur une base obligatoire. L'évaluation devra comprendre une analyse de l'état de développement et de préparation des technologies permettant de détecter le matériel pédopornographique et la sollicitation d'enfants, y compris les taux d'erreur. Elles plaident pour que cette analyse couvre spécifiquement le développement et la disponibilité de technologies permettant de détecter des contenus ASM dans des environnements chiffrés, dès lors que cette

détection constituerait le principal apport d'une éventuelle révision du texte. Elles plaident pour que ce rapport inclut également une étude complète sur l'état de la pédocriminalité numérique dans l'UE et sur l'évolution du phénomène depuis l'entrée en vigueur du règlement.

- Article 85-1a :

  By [three years after the entry into force of this Regulation], and if necessary, every three years thereafter, the Commission shall present a report to the European Parliament and the Council assessing the necessity and feasibility of the detection of child sexual abuse material and the solicitation of children including on a mandatory basis**, for the purpose of a new legislative proposal**. The assessment shall include an analysis of the state of development and readiness of the technologies to detect child sexual abuse material and the solicitation of children, including ***within interpersonal communications services using end-to-end encryption***, ***and*** error rates. ***The report shall also include a comprehensive study on the state of online child sexual abuse in the EU and how this phenomenon has evolved since the Regulation came into force.***

5. Allègement du texte

Les autorités françaises plaident pour la suppression de l'article 5b sur le « Sign of reduced risk ». En effet, cet article introduit un risque important de report des pédocriminels sur ces services, dans la mesure où ils ne seraient pas sujets des mesures de prévention renforcées, et qu'ils donneraient un faux sentiment de sécurité aux mineurs qui les utilisent.

B. Comments of 03.2025

Pour faire suite à la réunion LEWP-P du 11 mars 2025, les autorités françaises adressent à la Présidence et au Secrétariat Général du Conseil les réponses suivantes aux questions soumises concernant le règlement « Abus sexuels sur mineurs ».

1. Obligation des fournisseurs :

- Comment voyez-vous le meilleur moyen de rendre les fournisseurs responsables de la prévention ou de l'atténuation du risque d'abus sexuels sur enfants dans leurs services sans déclencher une obligation de détection de facto pour les fournisseurs ?

Une obligation de prévention effective doit être clairement énoncée. Dans le cas contraire, les prestataires pourraient prétendre avoir pris des mesures de prévention, quelle que soit leur efficacité. A cet égard, les autorités françaises préconisent les reformulations suivantes :

Article 1(a):

(a) obligations on providers of relevant information society services to ***make best efforts to*** **effectively prevent the use of** their services for online child sexual abuse;

Article 4(1):

If providers of hosting services and providers of interpersonal communications services have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall put in place appropriate and proportionate measures, tailored to that risk, to ***effectively*** prevent online child sexual abuse in their services. […]

- Êtes-vous d'accord pour conserver le terme « prévention » dans l'ensemble du texte, comme le suggère la présidence, ou préférez-vous revenir au terme « atténuation des risques » comme dans la proposition de la Commission ?

Le terme de "risk mitigation" nous paraît plus approprié. Il s'agit en effet d'un terme figurant déjà dans le règlement sur les services numériques (« DSA », articles 34 et 35), qui poursuit une logique similaire d'évaluation et d'atténuation des risques. En l'état, il est difficile de comprendre ce que recouvre exactement la "prévention" qui devrait être mise en œuvre par les fournisseurs concernés, alors qu'une obligation d'évaluation et d'atténuation des risques semble en effet plus claire, engageante et facilement mesurable. En outre, si la présidence souhaite, par le terme "prévention", couvrir également des stratégies nationales dédiées et une communication du centre de l'UE, il semble possible d'introduire une disposition dédiée au sein du projet de texte, tout en conservant le terme de "risk mitigation" concernant les fournisseurs.

- Préférez-vous conserver le texte de la présidence ou rétablir le texte précédent à l'article 5 bis, paragraphe 1, et (2) en ce qui concerne l'évaluation des risques adaptée ou supplémentaire ou les mesures de prévention/d'atténuation des risques ?

L'autorité de coordination doit avoir la possibilité d'exiger du fournisseur de service qu'il prenne des mesures supplémentaires si les mesures proposées initialement par le prestataire ne sont pas suffisantes. Pour ce faire, le texte de l'article 5a qui avait déjà été approuvé devrait être rétabli, faute de quoi les pouvoirs des autorités nationales pour veiller à ce que les prestataires respectent l'obligation de prévention seraient indûment limités.

En tout état de cause, l'essentiel est qu'il y ait une obligation claire de prévention (obligation de résultat) et des pouvoirs d'exécution pour les autorités nationales (comme ils sont déjà inclus). Ces pouvoirs garantissent que les autorités nationales peuvent imposer des amendes et même la suspension du service en cas de non-respect par le prestataire de la prévention effective des contenus ASM et du grooming.

Enfin, il faudra que ces mesures de prévention concernent également les familles, les jeunes enfants et soient élargies aux auteurs (notamment afin qu'ils soient sensibilisés aux peines encourues).

Les propositions rédactionnelles demandées par les autorités françaises sont donc les suivantes :

Article 5a :

1. Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it ***shall require*** ***may recommend to*** the provider of […].

The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to ***recommend*** ***require*** pursuant to the first subparagraph.

2. A provider that ***is required to*** perform***s*** the actions specified in points (b) or (c) of paragraph 1 shall re-conduct […].

- Préférez-vous limiter le mécanisme de notification des utilisateurs prévu à l'article 12, paragraphe 3, aux services à haut risque ou cette obligation devrait-elle s'appliquer à tous les fournisseurs concernés ?

Il semble opportun qu'une obligation de prévoir un mécanisme de signalement s'applique à tous les fournisseurs quelle que soit leur catégorisation. En effet, sur tout service apparemment peu propice à cette forme de criminalité (ex : Vinted) il y a possibilité de trouver des contenus pédocriminels. Cette obligation s'ajouterait dans ce cas à l'obligation de prévoir un mécanisme de signalement prévue par le DSA pour les hébergeurs (article 16).

2. Champ d'application et conception de la dérogation à certaines dispositions de la directive 2002/58/CE :

- Comment voyez-vous la meilleure manière de concevoir la dérogation à certaines dispositions de la directive vie privée et communications électroniques afin qu'elle soit efficace, assortie de garanties suffisantes et correctement intégrée dans le fonctionnement du présent règlement ?
- Êtes-vous d'accord pour que la dérogation soit intégrée dans ce règlement en tant qu'article 4 bis, comme le suggère la présidence, ou préférez-vous que le règlement (UE) 2021/1232 reste un acte législatif distinct à modifier et à rendre permanent au moyen de ce règlement ?
- Êtes-vous d'accord pour que le champ d'application de la dérogation, tel que suggéré par la présidence, reste analogue au champ d'application du règlement (UE) 2021/1232 ? Si vous n'êtes pas d'accord, veuillez indiquer les écarts par rapport au champ d'application que vous souhaitez voir appliquer.

Les autorités françaises souhaitent avant tout que les possibilités offertes par le règlement dérogatoire soient préservées et pérennisées au-delà d'avril 2026, afin de préserver les activités opérationnelles des services d'application de la loi. Les autorités françaises se montreront donc flexibles sur l'outil juridique choisi.

3. Utilisation des technologies par les fournisseurs

- Comment voyez-vous la meilleure manière de réglementer l'utilisation des technologies par les fournisseurs, y compris celles mises à disposition par le centre de l'UE, en vue également de protéger la cybersécurité ?

Cette question soulève le problème plus global de la détection volontaire au sein des contenus chiffrés que les autorités françaises sont toujours en train d'expertiser et sur lequel elles émettent une réserve d'examen.

- Êtes-vous d'accord pour inviter la Commission à préparer une vue d'ensemble actualisée des technologies actuellement utilisées par les fournisseurs dans le cadre du régime dérogatoire et à fournir des informations sur les technologies existantes pour détecter le pédopiégeage sans que cela n'entraîne la déduction de la substance du contenu ?

Les autorités françaises sont favorables à cette proposition, qui permettrait d'évaluer les progrès technologiques depuis la publication de l'étude d'impact du règlement début 2022 et d'évaluer la conformité de ces technologies aux droits nationaux.

4. Réduire la complexité et la charge administrative

- Comment voyez-vous le meilleur moyen de réduire la complexité et la charge administrative dans ce règlement ?
- Êtes-vous d'accord pour conserver la catégorisation des risques et le signe de risque réduit comme proposé par la présidence ou préférez-vous ignorer ou modifier ces éléments ?

Les autorités françaises plaident pour la suppression de la catégorisation des risques, qui, en l'absence d'injonction de détection, ne présente plus de valeur ajoutée. En effet, les services sont déjà soumis à une obligation d'évaluation des risques (sans qu'il ne soit nécessaire de créer une étape supplémentaire, qui d'ailleurs n'existe pas dans le DSA et qui pourrait, en pratique, ralentir la mise en conformité des services). L'ANC pourrait avoir la possibilité de demander des mesures supplémentaires sur la base de cette analyse des risques (cf. proposition supra). Par ailleurs, les autorités françaises réinsistent sur le fait que les pédo-criminels peuvent être extrêmement mobiles d'une plateforme à une autre, rendant ainsi tous les sites potentiellement à haut risque.

Les autorités françaises plaident également pour la suppression de l'article 5b sur le « Sign of reduced risk ». En effet, cet article introduit un risque important de report des pédocriminels sur ces services, dans la mesure où ils ne seraient pas sujets des mesures de prévention renforcées, et qu'ils donneraient un faux sentiment de sécurité aux mineurs qui les utilisent.

- Êtes-vous d'accord pour que le centre de l'UE conserve le rôle et les tâches révisés proposés par la présidence, proposez-vous de modifier le rôle et les tâches du centre de l'UE ou préférez-vous remplacer le centre de l'UE par différentes structures ?

Les autorités françaises constatent que deux missions structurantes du centre de l'UE, dans lesquelles elles avaient placé beaucoup d'espoir, n'existent plus. Il s'agit d'une part du tri des faux positifs que les personnels du Centre devaient prendre en charge dans le cadre des injonctions de détection ; et d'autre part de l'étude et de l'approbation des technologies de détection qui devait être mises à disposition des fournisseurs de services. Dès lors, elles considèrent que les fonds (coûts ponctuels estimés à 5 millions d'euros et coûts annuels estimés à 25,7 millions d'euros selon l'étude d'impact) et les moyens humains (113 personnels selon l'étude d'impact) qui devaient être dédiés au Centre ne sont plus justifiés.

Elles plaident donc pour une réécriture complète des articles article 40 à 82 du règlement et pour que l'agence soit remplacée par une communauté d'experts et d'organisation (ONG de défense des mineurs, hotlines, représentants d'entreprises proposant des technologies de protection des mineurs sur internet, services répressifs spécialisés) à même de réaliser les missions d'aide aux victimes, de partager de bonnes pratiques et de réaliser des études et recherches prospectives sur l'état de la menace, les victimes et les auteurs.

En parallèle, Europol pourrait se voir confier l'hébergement de la base de données de contenus pédopornographiques. Néanmoins, les autorités françaises ne sont pas favorables à ce qu'Europol se voit octroyer des pouvoirs de cyber-patrouille et d'enquête sous pseudonyme, qui doivent demeurer des prérogatives nationales.

Enfin, le « EU Innovation Hub for Internal Security » pourrait être missionné pour accompagner la Commission dans la rédaction du rapport qu'elle devra publier trois ans après l'adoption du règlement pour évaluer la maturité et la précision de ces technologies, en publiant des études régulières à ce propos, comme il l'a déjà fait en 2024 sur le chiffrement ou l'intelligence artificielle.

5. Clause de réexamen

- Comment voyez-vous la meilleure manière de concevoir la clause de réexamen pour que la Commission puisse proposer une nouvelle législation dans un délai de 3 ans à compter de l'entrée en vigueur du présent règlement ?

Les autorités françaises estiment que le règlement « Abus sexuels sur mineurs » doit être rapidement évalué après son adoption et qu'un autre texte devrait être proposé pour dépasser les limites opérationnelles qu'il ne manquera pas de rencontrer. Dès lors, elles soutiennent l'article 85-1a qui enjoint la Commission à présenter, au plus tard trois ans après l'entrée en vigueur du présent règlement un rapport évaluant la nécessité et la faisabilité de la détection du matériel pédopornographique et de la sollicitation d'enfants, y compris sur une base obligatoire. L'évaluation devra comprendre une analyse de l'état de développement et de préparation des technologies permettant de détecter le matériel pédopornographique et la sollicitation d'enfants, y compris les taux d'erreur. Elles plaident pour que cette analyse

couvre aussi le développement et la disponibilité de technologies permettant de détecter des contenus ASM dans des environnements chiffrés, dès lors que cette détection constituerait le principal apport d'une éventuelle révision du texte.

Par ailleurs, elles plaident pour que ce rapport inclut également une étude complète sur l'état de la pédocriminalité numérique dans l'UE et sur l'évolution du phénomène depuis l'entrée en vigueur du règlement. Cela permettra de mesurer l'impact de ce texte sur l'évolution de la pédo-criminalité et ses éventuelles lacunes.

Article 85-1a :

By [three years after the entry into force of this Regulation], and if necessary, every three years thereafter, the Commission shall present a report to the European Parliament and the Council assessing the necessity and feasibility of the detection of child sexual abuse material and the solicitation of children including on a mandatory basis**, for the purpose of a new legislative proposal**. The assessment shall include an analysis of the state of development and readiness of the technologies to detect child sexual abuse material and the solicitation of children, including ***within interpersonal communications services using end-to-end encryption***, ***and*** error rates. ***The report shall also include a comprehensive study on the state of online child sexual abuse in the EU and how this phenomenon has evolved since the Regulation came into force.***

- Comment voyez-vous les rôles et responsabilités des fournisseurs, du centre de l'UE et de son comité chargé des technologies, ainsi que d'autres structures susceptibles de contribuer au développement de nouvelles technologies pour prévenir les abus sexuels sur enfants ?
-

Cf réponse sur l'avenir du centre de l'UE.

Traduction de courtoise :

1. **Obligations for providers**

How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

An effective prevention obligation must be clearly stated. Otherwise, providers could claim to have taken preventive measures, regardless of their effectiveness. In this regard, we recommend the following redraftings:

Article 1(a):

(a) obligations on providers of relevant information society services to ***make best efforts to*** **effectively prevent the use of** their services for online child sexual abuse;

Article 4(1):

If providers of hosting services and providers of interpersonal communications services have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they shall put in place appropriate and proportionate measures, tailored to that risk, to ***effectively*** prevent online child sexual abuse in their services. […]

Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?

The term "risk mitigation" seems to us to be more appropriate. It is indeed a term already included in the Digital Services Act ("DSA", Articles 34 and 35), which pursues a similar logic of risk assessment and mitigation. As it stands, it is difficult to understand exactly what "prevention" should be implemented by the providers concerned, when a risk assessment and mitigation obligation seems indeed clearer, more engaging and easily measurable. Moreover, if the Presidency wishes, by the term "prevention", also to cover dedicated national strategies and a communication from the EU Centre, it seems possible to introduce a dedicated provision within the draft text, while retaining the term "risk mitigation" with regard to providers.

Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

The Coordinating Authority should have the possibility to require the service provider to take additional measures if the measures initially proposed by the service provider are not sufficient. In order to do so, the already agreed text of Article 5a should be reinstated, failing which the powers of national authorities to ensure that providers comply with the duty of prevention would be unduly limited.

In any case, the main thing is that there is a clear obligation of prevention (obligation of result) and enforcement powers for national authorities (as they are already included). These powers ensure that national authorities can impose fines and even suspension of the service in case of non-compliance by the provider with the effective prevention of ASM content and grooming.

Finally, these preventive measures must also concern families and young children and be extended to include perpetrators (in particular so that they are made aware of the penalties incurred).

The drafting proposals requested by the French authorities are therefore as follows:

Article 5a :

1. Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or

parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it ***shall require*** ***may recommend to*** the provider of […].

The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to ***recommend*** ***require*** pursuant to the first subparagraph.

2. A provider that ***is required to*** perform***s*** the actions specified in points (b) or (c) of paragraph 1 shall re-conduct […].

Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

It seems appropriate that an obligation to provide for a reporting mechanism should apply to all providers regardless of their categorisation. Indeed, on any service apparently unsuitable for this form of crime (e.g. Vinted) there is a possibility to find paedocriminal content. This would be in addition to the obligation to provide a reporting mechanism under the DSA for hosts (Article 16).

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

Above all, we would like the possibilities offered by the derogating regulation to be preserved and perpetuated beyond April 2026, in order to preserve the operational activities of the law enforcement services. The French authorities will therefore be flexible on the legal tool chosen.

3. **Use of technologies by providers**

How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

This question raises the more general problem of voluntary detection in encrypted content, which the French authorities are still assessing and on which they have a scrutiny reservation.

Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

We are in favour of this proposal, which would make it possible to assess technological progress since the publication of the impact assessment of the Regulation in early 2022 and to assess the conformity of these technologies with national laws.

4. **Reducing complexities and administrative burden**

How do you see the best way of reducing complexities and administrative burden in this Regulation?

Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

We call for the removal of the risk categorisation, which, in the absence of a detection order, no longer has added value. Indeed, services are already subject to a risk assessment obligation (without the need to create an additional step, which moreover does not exist in the DSA and which could, in practice, slow down the compliance of services). The national coordination authority could have the possibility to request additional measures on the basis of this risk analysis (see proposal above). Furthermore, the French authorities insist that pedocriminals can be extremely mobile from one platform to another, thus making all sites potentially high-risk.

We also call for the deletion of Article 5b on the 'Sign of reduced risk'. That article introduces a significant risk of pedocriminals being transferred to those services, in so far as they are not subject to enhanced preventive measures, and they give a false sense of security to the minors who use them.

Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

The French authorities note that two structuring missions of the EU Centre, in which they had placed great hope, no longer exist. This concerns, on the one hand, the sorting of false positives that the Centre's staff had to take care of in the context of detection orders; and the study and approval of detection technologies to be made available to service providers. Therefore, they consider that the funds (one-off costs estimated at EUR 5 million and annual costs estimated at EUR 25.7 million according to the impact assessment) and human resources (113 staff according to the impact assessment) which were to be dedicated to the Centre are no longer justified.

They therefore call for a complete rewriting of Articles 40 to 82 of the Regulation and for the Agency to be replaced by a community of experts and organisations (NGOs for the defence of minors, hotlines, representatives of companies offering technologies for the protection of minors on the internet, specialised law enforcement authorities) capable of carrying out victim support missions, sharing best practices and carrying out prospective studies and research on the state of the threat, victims and perpetrators.

In parallel, Europol could be entrusted with hosting the database of child sexual abuse material. Nevertheless, we are not in favour of granting Europol powers of cyber-patrol and pseudonymous investigation, which must remain national prerogatives.

Finally, the EU Innovation Hub for Internal Security could be commissioned to assist the Commission in drafting the report to be published three years after the adoption of the Regulation to assess the maturity and accuracy of these technologies, by publishing regular studies on this subject, as it has already done in 2024 on encryption or artificial intelligence.

5. **Review clause**

How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?

The French authorities consider that the Regulation on child sexual abuse must be evaluated quickly after its adoption and that another text should be proposed to exceed the operational limits that it will not fail to meet. They therefore support Article 85-1a, which requires the Commission to submit, no later than three years after the entry into force of this Regulation, a report assessing the necessity and feasibility of detecting child sexual abuse material and soliciting children, including on a mandatory basis. The evaluation should include an analysis of the state of development and preparedness of technologies to detect child sexual abuse material and solicitation of children, including error rates. They argue that this analysis should also cover the development and availability of technologies to detect ASM content in encrypted environments, since such detection would be the main contribution of a possible revision of the text.

Furthermore, they call for this report to also include a comprehensive study on the state of digital child crime in the EU and on the evolution of the phenomenon since the entry into force of the Regulation. This will make it possible to measure the impact of this text on the evolution of pedocriminality and its possible shortcomings.

Article 85-1a :

By [three years after the entry into force of this Regulation], and if necessary, every three years thereafter, the Commission shall present a report to the European Parliament and the Council assessing the necessity and feasibility of the detection of child sexual abuse material and the solicitation of children including on a mandatory basis**, for the purpose of a new legislative proposal**. The assessment shall include an analysis of the state of development and readiness of the technologies to detect child sexual abuse material and the solicitation of children, including ***within interpersonal communications services using end-to-end encryption*****,** ***and*** error rates. ***The report shall also include a comprehensive study on the state of online child sexual abuse in the EU and how this phenomenon has evolved since the Regulation came into force.***

How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?

Please refer to the answer on the future of the EU Centre

GERMANY

A. Comments of 02.2025

General remarks

- We thank the Presidency for presenting a new compromise. We believe that it is extremely urgent to continue the negotiations on this important dossier in order to prevent any regulatory gaps when the Interim Regulation expires in April 2026.
- We stand by the same position we have held up to now and refer in particular to the Note from Germany in the December JHA Council.
- Germany welcomes the protection of (end-to-end) encryption in Article 1 (5); this provision corresponds to our Note of 12 December 2024.
- Following our initial preliminary assessment, we also welcome the fact that the Presidency's proposal comes closer to parts of the German position, particularly by deleting the mandatory detection orders.
- Germany does not want the new Regulation to provide for fewer possibilities for detecting CSAM than is currently the case, nor does Germany want the number of unreported cases to increase. That is why it is essential to ensure that CSAM can be reported to the same extent as today, in terms of both quality and quantity, after the CSA Regulation enters into force.
- As the Federal Government has not yet completed its examination, we maintain our **scrutiny reservation**.

Re st5352/25

Article 1:

- Para. 1 (a): In combating the sexual abuse of children, we believe it is essential to make the providers of relevant information society services more accountable. With this in mind, the previous wording seems preferable. Please explain why the wording has been changed.
- Paras. 5 and 6: Please explain the revisions, especially how they relate to the plans to make voluntary detection permanent (currently in the Interim Regulation).

Articles 3 and 4:

- We cannot support any changes that weaken providers' obligations to minimise risks.
- (See also our comment on Article 1 (1) (a)). Please explain why the term "mitigation" has been replaced by the term "prevention".
- Article 3 (5): We cannot support this deletion. The risk assessment should include an assessment of risks remaining after mitigation measures have been taken. These results should also feed into the review pursuant to Article 85 (1a).
- Article 4 (1) (2): We object to the deletion of "at least", as it weakens the risk mitigation obligations.

Article 4a:

- Please explain the proposed (permanent) continuation of the Interim Regulation. We kindly ask for answers to the following questions in particular:
  - Does Article 4a correspond to the currently applicable provisions of the Interim Regulation? If not: What is the reason for the proposed derogations?
  - Where are the reports to be sent – to the EU Centre, the Member States and/or to Europol? Para. 3 (f) seems unclear here. Is it possible to choose where the report is to be sent?

    Establishing a single European regulatory framework with effective and clearly defined reporting channels is a crucial step in the fight against the sexual abuse of children.
  - Which safeguards are to be observed in voluntary detection by providers?
  - Does the proposal provide for voluntary detection in encrypted services?
  - If so, which technologies may be applied?
  - We kindly ask the Council Legal Service whether there are any legal concerns about the proposal to permanently continue the provisions of the Interim Regulation.
- Although Article 4a provides for derogations from Article 5 (1) and Article 6 (1) of Directive 2002/58/EC, in order to ensure that the CSA Regulation provides effective added value in the fight against child sexual abuse, it seems necessary to check whether these voluntary measures (in the context of risk management, for example) should be more strongly integrated and whether incentives encouraging enterprises to apply them should be created.
- In any case, Germany believes it is necessary to ensure – also in view of technological developments in the design of digital services – that the new Regulation is no less effective than the Interim Regulation and that the number of unreported cases does not increase. Even after the CSA Regulation comes into force, it must be possible to report CSAM to the same extent as today, in terms of both quality and quantity.
- As far as Article 4a is able to prevent a regulatory gap in the fight against child sexual abuse, we welcome the proposal.
- Para. 3 (d) (x): We are still examining the reporting obligation. In Germany, the current reporting obligation requires a great deal of effort due to the different (federal and state-level) jurisdictions. We therefore reserve the right to propose revisions at a later date.

Article 5:

- Para. 1 (c) / para. 2 (see also above re Article 3): We cannot agree to this deletion. The risk assessment should include an assessment of risks remaining after mitigation measures have been taken. These results should also feed into the review pursuant to Article 85 (1a).

Article 5a:

- We cannot support weakening the Coordination Authority's discretion by replacing "*shall require*" with "*may recommend*". We believe it is crucial to make providers more accountable for protecting children and young people from sexual abuse. This includes robust and consistent risk management by the coordinating authorities which can also enforce necessary improvements as appropriate.

Articles 7–11:

- The proposal to delete Articles 7–11, which continue to be the subject of disagreement, from the proposed Regulation while permanently establishing voluntary detection takes up a proposal which Germany made during the negotiations. The German proposal was intended to prevent regulatory gaps after the Interim Regulation expires in April 2026. We therefore welcome this proposal.
- The Federal Government has not yet concluded its examination of Articles 7–11.
- We firmly believe that a high level of data protection and cyber security, including complete and secure end-to-end encryption in electronic communications, is essential.
- In particular, measures which lead to the scanning of private encrypted communications and measures which break, weaken, modify or circumvent end-to-end encryption must be excluded from the proposed Regulation.
- We have not yet concluded our critical examination of the permissibility and extent of server-side detection measures in unencrypted telecommunications and (cloud) storage services.
- In our view, the top priority for the rules to be retained is to take sufficient measures to ensure that the new Regulation is no less effective than the Interim Regulation and that the number of unreported cases does not increase Even after the CSA Regulation comes into force, it must be possible to report CSAM to the same extent as today, in terms of both quality and quantity. We kindly ask the Presidency to explain whether, in its view, the present compromise proposal meets this requirement.

Article 12:

- Para. 3: We do not see the reason for adding the text "*for a service or the parts or components of the service classified as high risk according to Article 5(2)*". A reporting mechanism that is easy to access and in particular child-friendly should have to be established for all services.
- Nor do we see a reason for the added text at the end of para. 3 ("The provider shall ensure that the receipt of users' notifications is acknowledged, and users are provided with effective feedback including about alternative means of reporting (including to organisations acting in the public interest against child sexual abuse and national law enforcement) and other relevant information, including assistance for victims.").

  Reactive, as appropriate: Is this addition similar to the approach recently taken by digital services, in which users are to report more (see newly introduced "community notes" on Meta), allowing the platforms to reduce their active moderation of content?

Article 39:

- We welcome the obligation to adopt a national CSA strategy. We would be in favour of setting a target date and requiring an implementation status report at regular intervals. We would also like to start a discussion of how to implement this proposal with a minimum of bureaucracy.

Article 40 and following articles:

- We kindly ask the Presidency to explain how the proposed changes would affect the tasks and role of the EU Centre.

Article 83:

- Para. 2 (h) (hb–hd): We are still examining the reporting obligation. In Germany, the reporting obligation requires a great deal of effort due to the different (federal and state-level) jurisdictions. We therefore reserve the right to propose revisions at a later date.
- Para. 3 (k): Here too, we ask that the previous version of (k) be retained, because the European Data Protection Board should still provide an opinion before technologies are applied.

Article 50:

- Para. 1 (3): The European Data Protection Board and the EU Centre's Technology Committee should still have to provide an opinion before the EU Centre makes technologies available to scan for CSAM. We therefore ask that subparagraph 3 be retained.

Article 85:

- Para. 1a: In response to the deletion of Articles 7–11, we welcome a review clause for (mandatory) detection orders.

B. Comments of 03.2025

General remarks

- We thank the Presidency for presenting the discussion paper. We believe that it is extremely urgent to continue the negotiations on this important dossier in order to prevent any regulatory gaps when the Interim Regulation expires in April 2026.
- Given that federal general elections took place on 23 February 2025, our current position is subject to change based on the position of Germany's new Federal Government.
- We stand by the same position we have held up to now and refer in particular to the Note from Germany in the December JHA Council.
- As the Federal Government has not yet completed its examination, we maintain our **scrutiny reservation**.

1. Obligations for providers

- How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

- Although Article 4a provides for derogations from Article 5 (1) and Article 6 (1) of Directive 2002/58/EC, in order to ensure that the CSA Regulation provides effective added value in the fight against child sexual abuse, it seems necessary to check whether these voluntary measures (in the context of risk management, for example) should be more strongly integrated and whether incentives encouraging enterprises to apply them should be created.

- Article 3 (5) and Article 5 (1) (c) and (2): We cannot agree to these deletions. The risk assessment should include an assessment of risks remaining after mitigation measures have been taken. These results should also be incorporated into the review pursuant to Article 85 (1a).

- Article 4 (1) subparagraph 2: We object to the deletion of "*at least*", as it weakens the risk mitigation obligations.

- Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?

- We cannot support any changes that weaken providers' obligations to minimise risks.

- In combating the sexual abuse of children, we believe it is essential to make the providers of relevant information society services more accountable. With this in mind, the previous wording, "*risk mitigation*", seems preferable.

- Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

Article 5a:

- We cannot support weakening the Coordination Authority's discretion by replacing "*shall require*" with "*may recommend*". We believe it is crucial to make providers more accountable for protecting children and young people from sexual abuse. This includes robust and consistent risk management by the coordinating authorities, which can also enforce necessary improvements as appropriate.

- Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

Article 12:

- Paragraph 3: We do not see the reason for adding the text "*for a service or the parts or components of the service classified as high risk according to Article 5(2)*". A reporting mechanism that is easy to access and in particular child-friendly should have to be established for all services.

- Nor do we see a reason for the added text at the end of para. 3 ("The provider shall ensure that the receipt of users' notifications is acknowledged, and users are provided with effective feedback including about alternative means of reporting (including to organisations acting in the public interest against child sexual abuse and national law enforcement) and other relevant information, including assistance for victims.").

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

- How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

Article 4a:

- Please explain the proposed (permanent) continuation of the Interim Regulation. We kindly ask for answers to the following questions in particular:
    - Where are the reports to be sent – to the EU Centre, the Member States and/or to Europol? Para. 3 (f) seems unclear here. Is it possible to choose where the report is to be sent?

Establishing a single European regulatory framework with effective and clearly defined reporting channels is a crucial step in the fight against the sexual abuse of children.

- Which safeguards are to be observed in voluntary detection by providers?
- Does the proposal provide for voluntary detection in encrypted services?
- If so, which technologies may be applied?
- We kindly ask the Council Legal Service whether there are any legal concerns about the proposal to permanently continue the provisions of the Interim Regulation.

- Although Article 4a provides for derogations from Article 5 (1) and Article 6 (1) of Directive 2002/58/EC, in order to ensure that the CSA Regulation provides effective added value in the fight against child sexual abuse, it seems necessary to check whether these voluntary measures (in the context of risk management, for example) should be more strongly integrated and whether incentives encouraging enterprises to apply them should be created.

- In any case, Germany believes it is necessary to ensure – also in view of technological developments in the design of digital services – that the new Regulation is no less effective than the Interim Regulation and that the number of unreported cases does not increase. Even after the CSA Regulation comes into force, it must be possible to report CSAM to the same extent as today, in terms of both quality and quantity.

- As far as Article 4a is able to prevent a regulatory gap in the fight against child sexual abuse, we welcome the proposal.

- Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

- Germany is open in principle to including the provisions of the Interim Regulation in the CSA Regulation.

- Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

- In our view, the top priority for the rules to be retained is to take sufficient measures to ensure that the new Regulation is no less effective than the Interim Regulation and that the number of unreported cases does not increase Even after the CSA Regulation comes into force, it must be possible to report CSAM to the same extent as today, in terms of both quality and quantity. We kindly ask the Presidency to explain whether, in its view, the present compromise proposal meets this requirement.

3. Use of technologies by providers

- How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

- Germany welcomes the protection of (end-to-end) encryption in Article 1 (5); this provision corresponds to our Note of 12 December 2024.
- We firmly believe that a high level of data protection and cyber security, including complete and secure end-to-end encryption in electronic communications, is essential.
- In particular, measures which lead to the scanning of private encrypted communications and measures which break, weaken, modify or circumvent end-to-end encryption must be excluded from the proposed Regulation.
- At the same time, in our view, the top priority for the rules to be retained is to take sufficient measures to ensure that the new Regulation is no less effective than the Interim Regulation and that the number of unreported cases does not increase Even after the CSA Regulation comes into force, it must be possible to report CSAM to the same extent as today, in terms of both quality and quantity.
- Article 50 (1) subparagraph 3: The European Data Protection Board and the EU Centre's Technology Committee should still have to provide an opinion before the EU Centre makes technologies available to scan for CSAM. We therefore ask that subparagraph 3 be retained.

- Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

- Germany agrees.

4. Reducing complexities and administrative burden

- How do you see the best way of reducing complexities and administrative burden in this Regulation?

- We are still examining the reporting obligation of the Member States. In Germany, the current reporting obligation requires a great deal of effort due to the different (federal and state-level) jurisdictions. We therefore reserve the right to propose revisions at a later date.

- Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

- We consider the risk categorisation to be a suitable instrument for differentiating the scope of obligations among the different providers.

- Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

- Germany is in favour of an EU Centre with comprehensive tasks, so that the EU Centre can also contribute to European proactive sovereignty and ability to act.

5. Review clause

- How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?

- Article 85 (1a): In response to the deletion of Articles 7–11, we welcome a review clause for (mandatory) detection orders.

- How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?

- The EU Centre and its Technology Committee, as well as the providers, are responsible for helping to develop new technologies to combat CSAM.

HUNGARY

A. Comments of 02.2025

Our general position is that the measures introduced by the future regulation must represent added value, they must establish a stricter and more effective mechanism than the current voluntary-based detection allowed by the temporary derogation.

We do not see this added value in the new proposal, and in fact, with regard to certain provisions, it even represents a significant step backwards compared to the previous compromise texts and the current voluntary-based detection mechanism.

We believe that as a result of the amendments of the new proposal, the direct procedural rights of the Member States against hosting and interpersonal communication service providers will be significantly reduced, particularly due to the removal of detection orders.

From a technological point of view, the proposed preventive measures alone would not allow service providers to use any effective tool.

The text currently does not allow for the voluntary detection of encrypted content either, which represents a step backwards compared to the current voluntary mechanism, therefore we cannot support it in its current form.

B. Comments of 03.2025

We would like to emphasise that our general position is that the measures introduced by the future regulation must represent added value, they must establish a stricter and more effective mechanism than the current voluntary-based detection allowed by the temporary derogation.

We do not see this added value in the new Presidency compromise texts, and in fact, with regard to certain provisions, it even represents a significant step backwards compared to the previous compromise texts and the current voluntary detection mechanism.

We provide the following replies to the questions below.

1. Obligation for providers

How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

Without a de facto detection obligation, the prevention or mitigation of the risk of CSA would not be effective. The main reason for the Commission's original proposal was that the current temporary derogation allowing voluntary-based detection is not sufficiently effective in preventing the dissemination of CSAM as the number of cases is increasing dramatically year on year.

We consider it important to note that, since service providers often use content detection technologies for various purposes (e.g., detecting malware or vulnerabilities on the user's endpoint device and reporting to the central server), the detection of CSAM in such cases would not represent a significant additional obligation for service providers, nor would it pose additional risks to the user from a data

protection perspective, as the service provider already has access to all of the user's encrypted and unencrypted communication data.

Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?

The term 'prevention' is elusive, too general and difficult to interpret. If the term prevention is to be used, it is necessary to define exactly what it means and what type of action it requires from providers. The term 'risk mitigation' is a more specific and targeted term. The term is clearer, easier to assess and measure.

The 'risk mitigation' related to CSAM content in the previous draft would have imposed a more targeted scope of obligations on service providers than the 'prevention' proposed by the Polish Presidency. The previous compromised text's Article 5(1)-(2) – in line with Article 4 – prescribed risk mitigation measures for service providers in relation to the risks they identified in connection with their services. However, the amendments proposed by the Polish Presidency would impose preventive measures on service providers against all potential risks – whether identified or not by the service providers (new Article 4(2a)).

This could raise legal interpretation questions regarding what individual service providers consider to be effective prevention measures, especially given that in the new draft's Article 1(6), would exclude the regulation from creating an obligation that would require hosting service providers or interpersonal communication service providers to apply technologies for the detection or filtering of online child sexual abuse in a general and indiscriminate manner.

In this context, the preventive measures to be imposed on service providers is difficult to interpret. We propose to maintain the previous Articles 5 – and 4 – due to their clarity (and to retain provisions on detection orders to enforce user rights if the service provider's risk mitigation measures have not been successful).

Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

To ensure the preservation of national authorities' powers, we advocate for the reinstation of the previous text. In article 5a, we propose the previously used and stronger „shall require" term instead of „may recommend", in order to make the request non-optional. The Coordinating Authority should maintain the power to request additional or adjusted prevention/risk mitigation measures and to enforce necessary improvements as appropriate, if it considers that those measures initially suggested and carried out by the provider were not sufficient.

Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

It should apply to all relevant providers. The platforms for the distribution of CSAM are changing dynamically and are not limited to high-risk platforms. It is in the best interests of children that this is a common option for users. We see no need for new amendments to Article 12(3)(a), because if a child makes a report, they should not be expected to provide a justification. The key to the

investigation is that the user sends the exact URL to the content, allowing the provider to identify the content.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented?

We do not agree with the amendments proposed by the Presidency and would prefer to keep the regulations separate, especially in view of their different legal bases (GDPR and internal market) and also keep the previous text, especially with regards to the review clause of the CSA Regulation.

3. Use of technologies by providers

How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

We consider the previous, technologically neutral compromised proposal to be the most effective.

While we agree with the proposition to invite the Commission to prepare an updated overview, we express a concern regarding the accessibility of this information to potential offenders. To mitigate this risk, it is essential that access to the report be limited to a specific group of qualified experts.

4. Reducing complexities and administrative burden

How do you see the best way of reducing complexities and administrative burden in this Regulation?

Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

In general, we propose to return to the previous text. The risk categorisation is of particular importance for the implementation of the provisions on detection orders, so the two should be considered together.

The sign of reduced risk can raise some concerns, since it can give users the false impression that they are completely protected and safe. It is important how this sign is being communicated and presented, and what the precise, specific message is to users. Therefore we propose to delete the provisions on the sign of reduced risk.

5. Review clause

How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?

The review clause should set out realistic and effective measures for the review of the CSA Regulation, without prejudice to an earlier revision than 3 years in case adaptation to technological developments require it.

How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?

Without strict obligations for detection of CSAM, it would not be effective enough for the Technology Committee to lead the development of new CSA prevention technologies.The dominant market players relevant to the CSA Regulation are mostly service providers seated in non-EU countries, using and developing their own leading new edge technologies.

IRELAND

A. Updated comments of 02.2025 (03.2025)

Ireland welcomes the efforts of the PL PRES to progress this important file. We wish to recall a primary rationale for the development of this proposal, as stated in the explanatory memorandum: "*voluntary action has thus proven insufficient to address the misuse of online services for the purposes of child sexual abuse."* Ireland has consistently advocated for a regulation that is technology-neutral and applicable to all forms of online child sexual abuse.

Ireland understands the need to compromise in order to reach agreement and has acted on that basis throughout negotiations. However, it is incumbent upon all Member States to ensure that in reaching agreement, we develop a text that provides for significantly more robust and effective measures than those currently in place, to ensure meaningful prevention and combatting of child sexual abuse.

IE Position on Document 5352/25

Following a review of document 5352/25, Ireland is not in a position to support the text as currently presented. The key areas of concern are as follows:

1. the language on provider prevention obligations is weak and will negatively impact on the ability of providers to effectively prevent CSAM as well as on authorities' abilities to sanction and penalise providers where CSAM continues to exist on, or is disseminated from, their platforms.
2. certain provisions of the temporary derogation are eliminated, such as the reference to Article 5(3) in the ePrivacy Directive, thereby preventing providers from putting in place prevention measures that require accessing metadata, or any other data stored on an individual device, as well as the exclusion of encrypted services from the scope of the regulation.
3. the current text creates legal uncertainty for providers in relation to carrying out prevention measures that are not related to encryption; for example, voluntary detection in a non-encrypted environment. The first sentence of Article 1(5) is broad and vague, resulting in legal uncertainty for providers.

Ireland also considers that a number of existing provisions in document 5352/25 must be retained, particularly because these ensure the overall "value add" of the text. Such provisions include:

- child safety by design obligations (risk assessment, risk reporting);
- voluntary detection;
- the EU Centre;
- the review clause;
- the temporary extension of the Interim Regulation for the transition period.

For Ireland, it is essential that the regulation brings substantial added value over and above the current provisions.

IE Proposed Amendments

In order to actively consider the PL PRES proposed text, Ireland believes that the following amendments must be incorporated:

1. Place a clear and enforceable obligation on service providers to effectively prevent the dissemination of CSAM and grooming.
2. Ensure the effective inclusion of encrypted services within the scope, notably when it comes to the obligation to prevent.

Below are specific amendments that Ireland considers essential in order to support the text:

Prevention Obligations on Service Providers

The obligation to effectively prevent should be clearly stated. Otherwise, providers could claim that they have taken some measures to prevent, regardless of their effectiveness.

- Article 1(a):

  (a) obligations on providers of relevant information society services to ~~minimise the risk that~~ **~~make best efforts to~~ effectively prevent the use of** their services ~~are misused~~ for online child sexual abuse;

- Article 4(1):

  (2) **If p**roviders of hosting services and providers of interpersonal communications services **have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they** shall ~~take **all** reasonable~~ **put in place appropriate and proportionate** ~~mitigation~~ measures, tailored to ~~the~~ **that** risk ~~identified pursuant to Article 3~~, **to effectively prevent online child sexual abuse in their services** ~~minimise that risk~~. […]

The possible prevention measures providers could take should not be unduly limited and should allow for providers to take a full range of prevention measures. This includes prevention measures requiring access to metadata or any other data stored on an individual device, exclusively for the purpose of preventing child sexual abuse online. Therefore, the references in the document to Article 5(3) of the e-Privacy Directive should be reinstated and incorporated as relevant in the compromise text, notably in the new Article 4a:

- Article 1(4):

  4. This Regulation limits the exercise of the rights and obligations provided for in Article 5(1) and (3) and Article 6(1) of Directive 2002/58/EC **to the extent strictly** ~~insofar as~~ necessary **in accordance with Article 4a.** ~~for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 **II** of this Regulation~~.

- Article 4a(3):

3. Regarding the scope of the derogation, Articles 5(1) and (3) and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that: […]

3(d)(viii):

(viii) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and (3) and 6(1) of Directive 2002/58/EC […]

Coordinating Authority Powers

There should be the possibility for the Coordinating Authority to require the provider to introduce additional measures if the measures initially suggested are not sufficient. To enable this, the text in Article 5a, which was previously agreed, should be reinstated; otherwise, there would be an undue limitation on national authority powers to ensure providers comply with the obligation to prevent. Specifically:

1. **Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it shall require ~~may recommend to~~ the provider of […].**

   The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to ~~recommend~~ require pursuant to the first subparagraph.

2. **A provider that is required to perform~~s~~ the actions specified in points (b) or (c) of paragraph 1 shall re-conduct […].**

Effective inclusion of encrypted services in the scope of the Regulation, in particular with regards to the obligation to prevent the dissemination of CSAM and grooming

The first sentence of Article 1(5), as it appears in document 5352/25, uses such broad wording (e.g. "weaken, circumvent, undermine…") that it de facto excludes encrypted services from the scope of the Regulation. In the previous version of the text, the reference to Article 10(1) ensured that upload moderation in encrypted services was possible, which allowed for a balanced approach, which had the potential for broad Member State agreement. Now that the reference to Article 10(1) (and Article 10 itself) has been deleted, such balance no longer exists.

Moreover, the first sentence of Article 1(5) is wide-ranging and vague and as such it introduces legal uncertainty for providers to carry out prevention measures other than those dealing with encryption; for example, voluntary detection in non-encrypted services.

A straightforward solution to address the two issues noted above would be to delete the first sentence of Article 1(5).

This would ensure that:

1. Encrypted data is out of the scope of the Regulation and there is an explicit acknowledgement that the Regulation does not prohibit encrypted services.
2. Encrypted services are in the scope of the Regulation. Providers should be free to implement encryption (or any other technology) if they so wish, but that should not be a way to circumvent the obligations of the Regulation, notably the obligation to prevent the dissemination of CSAM and grooming in their services.
3. The balanced approach which allowed a large group of Member States to support the compromise on encryption would be restored, and there would be legal certainty for providers to carry out prevention measures that are unrelated to encryption

The revised Article 1(5) would read as follows:

5. ~~**Without prejudice to Article 10(1), This Regulation shall not prohibit, make impossible, weaken, circumvent or otherwise undermine cybersecurity measures, in particular encryption, including end-to-end encryption, implemented by the relevant information society services or by the users.**~~ **This Regulation shall not create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to decrypt data or create access to end-to-end encrypted data, or that would prevent providers from offering end-to-end encrypted services.**

Ireland again welcomes the PL PRES efforts to progress this important file.

As noted, the content of the final agreed text for this proposed regulation must provide for a substantially more comprehensive and effective mechanism for the prevention and countering of child sexual abuse. Ireland is committed to delivering such a text and will engage with all parties to achieve this result. Should the text remain unchanged from that presented in document 5352/25, Ireland will not be in a position to support this proposal.

ITALY

A. Comments of 02.2025

Sexual abuse of minors constitutes one of the most heinous and detestable crimes that the legal system must combat. To this end, the implementation of increasingly effective measures for prevention and countering is a primary objective of general interest recognized by the Union, aimed at protecting the rights and freedoms of the victims.

At the same time, it is essential to ensure that this essential goal is pursued while fully respecting other fundamental rights, such as the protection of private and family life, the confidentiality of communications, and the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

From a methodological perspective, the draft proposed by the Polish Presidency seems to be aimed at introducing elements that were absent in the compromise text of the Hungarian Presidency. The reservations on such compromise text, shared by a blocking minority, prevented the adoption of a partial General Political Orientation draft at the December 2024 Justice and Home Affairs Council.

Nevertheless, the proposal, as for the current formulation by the Polish Presidency, **remains insufficient** and continues to be **vague, not fully developed, and inconsistent** in many of its most relevant points.

Initially, it is necessary to note that the absence of **recitals** makes it difficult to analyze the text, which instead requires a thorough and reasoned explanation of the reasons behind the legislative interventions, through their "concise justifications" normally contained in the recitals themselves.

For example, the system proposed by the new text claims to want to respect the confidentiality of users 1) by **limiting detection, reporting, and removal activities to content data** and related traffic data, 2) by **excluding audio materials and visual content** (Article 2 (y)), and, 3) above all, by **programmatically** declaring the intention **not to create obligations** that would de facto bypass **encryption techniques**, including **end-to-end**, or that would imply the use of technologies to detect or filter potential abuses in a **generalized and indiscriminate manner** (Articles 1.5 and 1.6). However, this approach, though commendable, risks remaining theoretical and being, in fact, weakened:

a) by the **renewed inclusion**, in the objective scope of the regulation, of **new material**[1] (NEW CSAM) and online **solicitation** of minors, alongside **known material** already identified through **hashing techniques**[2] (KNOWN CSAM) (in this regard, see Articles 4a.3 c (i), 13.1 (e) and (i), 44.1 (b) and (c), 44.2 (a) and (c)), and

[1] Article 4a.3, letter c) (i) once again includes *"new"* material (new child sexual abuse material) within the scope of the regulation. No objective criteria are provided regarding the technology that must be used for the detection of *"new"* material, considering that the term *"mitigation"* has been replaced with *"prevention,"* and therefore, a complete and massive analysis of the exchanged material could not be avoided.

[2] To verify the so-called "known material," one technology used is *"hash matching,"* which creates a unique "digital fingerprint" (*hash*) for each image or video of known CSAM; digital platforms compare the files uploaded by users with a database of 'hashes' of already identified illegal content. If a file matches, it is automatically flagged for removal.

b) by the greater emphasis placed on **prevention activities** and the need to **implement measures to reduce the risk of abuse**, including content moderation (Article 4.1 (a)).

As a result, attention should be focused, among other things, on the provision of Article 4a.3 (c) (ii), according to which **content scanning technologies** must **not be able to deduce the semantic content of communications**, but only have the capacity to detect **recurring patterns** (such as keywords) that may indicate possible sexual abuse of minors, including through the use of "**relevant key indicators**" (Article 4a.3 (c) (vii)) by the providers, for example, to determine an age difference that could constitute a risk factor for solicitation. It has in fact to be noted that such "relevant key indicators" remain so far **unspecified and generic**.

Furthermore, **the proposal for the regulation does not apply to the scanning of audio communications, and no definition is provided** for them within the text. However, Article 36 states: *"Competent authorities shall submit to the EU Centre, without undue delay and through the system established under Article 39(2), (a) specific items of material and* ***extracts of conversations*** *that the competent authorities of a Member State have identified, after a diligent assessment, subject to adequate judicial oversight, as constituting child sexual abuse material or solicitation of minors, as applicable, for the EU Centre to generate indicators in accordance with Article 44 (3)."*

In this regard, Article 2, point 35 of Directive (EU) 2018/1972 provides the following definition of a "**global conversation service**": ***"'total conversation service' means a multimedia real time conversation service that provides bidirectional symmetric real time transfer of motion video, real time text and voice between users in two or more locations"***. Therefore, **the reference to "extracts of conversations"** in the regulation, as defined, **should relate to real-time textual and voice communications between users in two locations**[3].

In this definitional uncertainty, **objective and measurable criteria** are currently lacking for the use of such patterns **through automated processes**, whose application does not seem to exclude the occurrence of **false positives or false negatives**. Therefore, a more **detailed indication of the such criteria** is needed, as well as **concrete safeguard measures**, including the implementation of **reliable age verification mechanisms** and **human oversight** to counterbalance the prevalence of the algorithm, especially in systems governed by artificial intelligence tools.

Respect for the **principles of necessity and proportionality** in the processing of personal data relating to users of electronic communications services remains, in fact, an indispensable requirement, which appears in clear contrast with scenarios of **massive and indiscriminate preventive controls** or those akin to systematic surveillance, such as **those made necessary by the generalized search for illicit material not already recognized and classified as such**[4].

Similarly, it is necessary to reiterate the need that, beyond the preliminary statements in Article 1.5, **cryptographic techniques should be concretely preserved**, especially **end-to-end encryption**, as

---

3 Moreover, recital 14 of Directive (EU) 2018/1972 defines a "voice communications service" as *"a publicly available electronic communications service for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international numbering plan, whether such a service is based on circuit switching or packet switching technology. It is the nature of such a service that it is bidirectional, enabling both parties to communicate."*

4 This is also due to the fact that the general criteria for the preventive identification of potentially suspicious individuals to be subjected to detection are not specified, as Article 3(4a) refers generically to *"specific types of channels of an interpersonal communications service, or to specific users or specific groups or types of users where possible, to the extent that such part, component, specific users or specific groups or types of users can be assessed in isolation for the purpose of mitigating the risk of preventing online child sexual abuse,"* without any indication of the criteria to be concretely implemented for selecting the groups or individuals to be subjected to checks.

a pillar of user trust in communication services, as any weakening of encryption techniques would also diminish online security and confidentiality. In this regard, the text does not clarify, in fact, how detection activities, to be carried out by private entities, could guarantee the integrity of encryption techniques and whether the safeguard applies only to the communication in transit or also to previous communications, as, in that case, the measure would be compromised "ab origine."

For the purposes of the regulation and its **subjective scope of application**, definitions of hosting service providers, interpersonal communication services, and number-independent interpersonal communication services; however, **the prevention and risk evaluation obligations (Article 3) are directed only at the first two categories of service providers**. Regarding interpersonal communication service providers, it is not specified whether this refers to a service connected to publicly assigned numbering resources (based on numbers) or one that is not connected to numbering resources (independent of numbers)[5].

That said, the following additions would be advisable:

1. given the **lack of definition of "audio communications,"** in Article 36.1 (a), replace the words **"extracts of conversations"** with **"extracts of textual communications,"** specifying whether the reference is to synchronous or asynchronous communications;
2. indicate the **criteria that the technology must meet for the prevention obligations**, i.e., **the freedom of communication and the secrecy of communications, which are constitutionally guaranteed rights**;
3. **define the entities to whom the regulation's obligations will apply**, considering that Directive (EU) 2018/1972 does not foresee a general authorization regime that includes number-independent interpersonal communication services.

Finally, it is necessary to further examine, in detail, **the procedural aspects related to the methods and powers that the competent authority would have**, as well as the **methods** to be adopted for **verifying the legality of the actions of providers** (Articles 15.3 (c), 18.4 (c), 18c.4 (b), 34), also in relation to other entities involved, starting with the establishing European Centre on Child Sexual Abuse (EUCSA), the decentralized agency responsible for implementing the new regulation.

Italy has a **general reserve**.

Moreover, we have expressed some doubts about the following point.

1) there is an absence of a legal framework, to impose the obligations on the providers and to enforce them

2) we are fearing that the introduction of a NEW material could endanger the proportionality of the proposal

3) we don't understand the reference to " extract of conversation " in article 36, this provision could be against the article where audio and written communication are not in the scope of the regulation;

4) there is a risk of forum shopping

5) the centre's tasks are not well defined

[5] Hosting service providers and number-independent interpersonal communication services are not subject to the general authorization regime under Directive (EU) 2018/1972. Furthermore, the aforementioned directive does not consider Video On Demand (VOD) services, websites, social networks, blogs, or machine-to-machine information exchange as interpersonal communication services.

6) it's not clear how the provision about " data protection and encryption" will be enforced

7) There is not a systematic vision: namely, the proposal has too many layers of changes that aren't harmonized

B. Comments of 03.2025

1) In order to hold providers accountable for preventing the dissemination of CSAM through the services they offer while avoiding a general surveillance, an obligation could be established requiring the creation of a hash file before the transmission of visual content. This hash would be matched against the known material database stored at the European Centre. This process would not require access to the content and would not circumvent end-to-end encryption. If a match occurs (i.e., a positive hit), a report would be sent to relevant law enforcement entities for further investigation.

We prefer to use the term "prevention" rather than "risk mitigation," as the former is more appropriate for focusing on the hindrance of the production and dissemination of CSAM, which should be the primary objective of this regulation. However, this does not mean that risk mitigation should be undervalued.

Regarding the question of whether to retain the Presidency's text or restore the previous one in Article 5a (1) and (2), we deem it essential to adopt a clear terminology that establishes direct and unequivocal obligations for providers, along with methods of control and verification of the procedures they adopt, under the supervision of public bodies at both the national and EU levels. The classification of providers according to the level of risk does not seem to be relevant in the new proposal.

We believe that providers should always allow users to flag suspected CSAM.

2) The derogation to the e-Privacy Directive should be retained within the new regulation to allow providers to report illegal content on a voluntary basis. This option should be provided in addition to the obligations described above. The same derogative provisions should apply to all providers.

3) The technologies used by providers must be tech-neutral, state-of-the-art, and strike the correct balance between the safeguard of privacy and the effective prosecution of CSAM.

We believe it would be useful to have a list of the existing technologies which are able to detect grooming without it leading to the deduction of the substance of the content.

4) The task assigned to the European Centre should focus on the management and distribution of information related to CSAM material. This includes:

- Effective monitoring and evaluation of the procedures implemented by providers;
- Custody of databases related to CSAM material;

- Conducting stress testing to verify the effectiveness of the measures taken by the providers;
- Identifying technical and technological solutions to ensure compliance with the regulation;
- Liaising with private entities and monitoring compliance with obligations.

5) We deem it useful to include a review clause, whose content will however depend on the final configuration of the regulation.

LATVIA

A. Comments of 02.2025

In LV view, **detection orders have been an essential component** of the proposed Regulation (already from the beginning of the discussions on the proposed Regulation LV was one of those Member States that supported the broad scope of detection orders covering known CSAM, new CSAM and solicitation of children [grooming]). Thus, the deletion of detection orders from the scope of the proposed Regulation **significantly reduces the added value of the proposed Regulation**, in particular with regard to **combatting child sexual abuse**. In this regard, LV notes that combatting child sexual abuse is equally important as preventing child sexual abuse.

LV highlights that in light of the previous experience **voluntary detection of CSAM and grooming performed by service providers has not been sufficient** (there are service providers that do not do anything in this regard). Thus, currently the Presidency in its compromise text for the proposed Regulation suggests to make voluntary detection that has not been effective enough in practice a permanent mechanism. In light of this, LV would still prefer having **an obligation for service providers to detect at least known CSAM**.

At the same time LV understands that the deadline for the application of the Interim Regulation is approaching very fast (in LV view, a gap in detection activities by service providers cannot be allowed). Thus, in light of this and in the spirit of compromise LV could accept the proposed Regulation without an obligation for service providers to detect at least known CSAM with **such conditions**:

1. A **clear obligation on service providers to effectively prevent** the dissemination of CSAM and grooming:
    - LV considers that the wording of the proposed Regulation regarding the prevention of the dissemination of CSAM and grooming by service providers **has to be strengthened.**
2. **Effective inclusion of encrypted services in the scope**, notably when it comes to the obligation to prevent:

In addition, LV continues to consider that **clear, effective and workable procedures** for preventing and combating child sexual abuse online that do not impose **disproportionate administrative burden** on competent authorities of Member States are needed. In light of this, LV believes that due to the deletion of detection orders **the proposed Regulation should be streamlined and simplified** (in particular, LV sees **risk categorization and a sign of reduced risk** (they were not included in the initial proposed Regulation) as those elements that could be deleted from the proposed Regulation).

B. Comments of 03.2025

A general remark

Latvia **maintains its position** on the new Presidency's approach to the CSA proposal (5352/25) submitted in writing to the Presidency and General Secretariat of the Council on 20 February 2025.

Latvia's written replies to the questions posed by the Presidency (6475/25)

1. Obligations for providers

– *How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?*

In Latvia's view**, a clear obligation for service providers** to effectively prevent the dissemination of child sexual abuse materials (CSAM) and grooming in their services **is the best way to ensure that service providers take responsibility**.

– *Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?*

In light of the discussion held at the last LEWP-P meeting on this issue, Latvia **would prefer to use the term "*prevention*"** that, in comparison with the term "*risk mitigation*", is more results oriented.

– *Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?*

In Latvia's opinion, **the previous text of Article 5a (1) and (2) should be reinstated**.

– *Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?*

In Latvia's opinion, this **obligation should apply to all relevant service providers**.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

– *How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?*

Latvia has no proposals.

– *Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?*

Latvia can **support the proposal to include the derogation as Article 4a**. In Latvia's view, it would be more appropriate from the perspective of judicial technique, namely, to have all related provisions in one legislative act.

– *Do you agree to keep the scope of the derogation as suggested by the Presidency, analogous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.*

Latvia can **agree to maintaining the scope of the derogation proposed by the Presidency** analogous to the scope of Regulation (EU) 2021/1232.

3. Use of the technologies by providers

– *How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?*

Latvia believes that **technological neutrality** has to be maintained in the CSA proposal. In this regard, Latvia finds it particularly important to ensure that **encrypted services are not excluded from the scope of the CSA proposal** at least with regard to the obligation of service providers to effectively

prevent dissemination of CSAM and grooming. In Latvia's view, **the current wording of the CSA proposal, in particular its Article 1(5), does not ensure that**.

Thus, in light of the deletion of detections orders from the scope of the CSA proposal and integration of the derogation in the CSA proposal, Latvia believes that also **the wording on the end-to-end encryption from the Regulation (EU) 2021/1232**[6] could be integrated in the CSA proposal instead of its Article 1(5). In any event, Latvia considers that at least the **balanced compromise** proposed by the previous Presidency **with regard to cybersecurity measures, in particular encryption** (included a reference "without prejudice to Article 10(1)" in Article 1(5) of the CSA proposal) **should be maintained**.

- *Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?*

Latvia **agrees with the relevant proposal.**

4. Reducing complexities and administrative burden

- *How do you see the best way of reducing complexities and administrative burden in this Regulation?*
- *Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?*

In Latvia's view, risk categorization has been closely linked to detection orders. Removing detection orders from the CSA proposal should also **eliminate risk categorization requirements**, as categorizing risk without detection orders places an undue administrative burden on authorities of Member States. Likewise, Latvia believes that **a sign of reduced risk should also be removed** from the CSA proposal, as it **imposes an excessive administrative burden on Member States and could be misleading for the users of relevant services**.

- *Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?*

Latvia **sees an added value in establishing the EU Centre** as a decentralized agency and, thus, **supports it**. Latvia believes that this is the most effective way to ensure the efficient execution of its wide-ranging functions. In addition, Latvia also notes that additional functions for the EU Centre in the area of prevention and assistance to victims have initially been assigned to it in the proposed CSA Directive[7].

6 End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption.

7 Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast) (COM (2024) 60 final).

5. Review clause

- *How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?*

Latvia **supports** having review clause in the CSA proposal. As regards its wording, Latvia considers that it would be more appropriate to revert back to it when there is a more stable text of the CSA proposal.

- *How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?*

Latvia **emphasizes the responsibility of all above mentioned stakeholders in developing new technologies** to prevent child sexual abuse.

LITHUANIA

A. Comments of 02.2025

LT has always firmly expressed its opinion that the security of children both online and in virtual reality is of essential priority. LT has always been one of the strongest supporters of this Proposal for a Regulation.

During the negotiation, although, it has been continuously pointed out that the Proposal by the Commission has lost its initial ambition.

Despite of that, LT was prepared to support the text proposed by the HU Presidency for the Coreper and Council of December, 2024, taking into account that the term of interim Regulation was approaching towards the end. The new regulation is of utmost importance.

In the compromise text proposed by the PL Presidency, with the deletion of detection orders, the document has lost its practical added value. Despite the fact that preventive measures are relevant, they are not effective, especially giving non-binding nature. The aim of Regulation, provided for in the Article 1 is to prevent and combat the use children sexual abuse online, however, the newly proposed text is neither ambitious nor clear. With the development of technology and AI, all the proportionate and appropriate measures to detect the content and prevent its dissemination shall be taken into consideration.

Despite of that, interim Regulation deadline is approaching, hence, a document with clear rules is necessary as soon as possible. In this case, as the detection orders are deleted from the scope of the Regulation, we stress for the clear and robust provisions regarding the obligations to the service providers to perform the preventive measures for searching, detecting, deleting CSAM online and providing information to the competent authorities.

LT is ready to work in the spirit of compromise, however, with the text which provisions would bring an added value. Also, LT supports other MS that continuously have expressed their views towards more ambitious document.

B. Comments of 03.2025

1. Obligations for providers

- How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?

It is important to set clear obligations for providers in the field of preventing CSA in their services. It is understood that the establishment of obligation of detection orders may not be fully achievable, but every effort should be made to prevent such content from being hosted using their services and the response to the reports of such content has to be swift and effective.

- Do you agree to keep the term “prevention” throughout the text as suggested by the Presidency or do you prefer to revert to the term “risk mitigation” as in the Commission proposal?

The term "prevention" implies the implementation of real measures to prevent the distribution of CSA content through the use of services, so we would support the term "prevention".

– Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?

We would support reinstatement of the previous text

– Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

It would be preferred that the user notification mechanism laid down in Article 12(3) would be applied to all relevant providers. If there is no obligation to detect the content for the providers, at least there should be an effective mechanism to report it from users side.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

– How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

– Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

Embedding the derogation within CSA Regulation would ensure that all obligations and exceptions exist within the same legal framework, making it easier for the stakeholders to interpret and apply the rules. It would also avoid fragmentation by keeping all related provisions in one comprehensive document, thus we would support it to be integrated in this Regulation.

3. Use of technologies by providers

– How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?

– Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

We agree to invite Commision to prepare an updated overview of the technologies as it would make it easier to determine what would be the best way of regulating the use of them.

4. Reducing complexities and administrative burden

– How do you see the best way of reducing complexities and administrative burden in this Regulation?

– Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

– Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

We would agree to keep the EU Centre..

MALTA

A. Comments of 02.2025

Malta welcomes the efforts of the Polish Presidency to continue working on this file and working on a revised proposal as a basis for discussions. It needs to be underlined from the beginning that the ultimate scope of this proposal is that of preventing and combatting the sexual abuse of children online. This ever-evolving reality, with an amount of online material which only continues to proliferate must constantly be kept in perspective. Hence further justifying the need for this Regulation.

With regards to the revised text set out in document 5352/25, Malta makes the following written comments;

1. Encryption

With the text as it stands and the deletion of Article 10, Malta calls for legal certainties that encrypted services remain in the scope of the Regulation, in particular with regards to the obligation to prevent the dissemination of Child Sexual Abuse Material (CSAM) and grooming. It is important to get the wording right so that while ensuring the protection of encryption, it is be simultaneously ensured that encrypted channels are included within the scope and that, therefore, the obligation to prevent CSAM appearing online would be countered with the necessary technology – even on such channels.

2. Clarification of what "prevention" means in the text.

We support the inclusion of "prevention" in the operative part of the text, however, there needs to be a common understanding on its meaning.
Furthermore, it is essential that the prevention methods, including the specific forms of risk mitigation, are clearly outlined to ensure a comprehensive and effective approach. A well-defined framework for prevention will help identify and address potential threats before they escalate, thereby reducing the risk of harm to children in digital environments. These measures should encompass technological safeguards, educational initiatives, industry obligations, and collaboration mechanisms to create a multi-layered system of protection.
These measures **should be mandatory**, as without mandatory implementation, disparities in enforcement and protection levels may arise, leaving vulnerabilities that could be exploited by offenders. A harmonized approach will ensure that children across all Member States benefit from the same level of safeguarding, regardless of national differences in legislation or enforcement capacity.
Stronger prevention measures could potentially include **Robust Age Verification and Parental Controls**. Implementing effective age verification mechanisms can reduce children's exposure to harmful content and interactions.

3. Provision of a clear obligation on Service Providers to effectively prevent the dissemination of CSAM and grooming

In our view, the Regulation should contain a clear obligation (including the consideration of applicable sanctions) on service providers to ensure that they combat and prevent the presence of child sexual abuse on their services. Use of such wording as "make best efforts" to prevent the use of their services for online child sexual abuse is not indicative of clear obligations.
Potential obligations could include:

- **Proactive Content Moderation**: SPs should be required to implement advanced AI-based and human moderation techniques to detect and remove CSAM-related content.
- **Stronger Reporting Mechanisms**: Platforms must establish streamlined and accessible reporting mechanisms for users to flag suspicious behaviour or content, with strict obligations to act swiftly.
- **Mandatory Transparency and Accountability**: Regular public reporting on CSAM-related actions taken by SPs should be required to ensure accountability.

4. The role of the EU Centre

Regarding the setting up of the EU Centre, we must ensure that there is added value for this to be included in the proposal. It should to be evaluated whether the functions of the Centre could be carried out by already existing setups in the EU.

5. Temporary derogation

Malta welcomes the inclusion of the temporary derogation in the revised text however questions the impact on its effectiveness with the exclusion of Article 5(3) of the e-privacy directive. In view of this, we believe that there is a need to ensure that what is currently covered by the temporary derogation, remains so covered.

6. Procedures for preventing and combating child sexual abuse which were not in the original proposal should be reviewed

MT considers that due to the deletion of the detection orders, aspects of the proposed Regulation should be streamlined and simplified reflecting the latest developments (risk categorisation) to ensure that they do not impose disproportionate administrative burden.

THE NETHERLANDS

A. Comments of 02.2025

General comment to the Presidency

The Netherlands fully recognizes the urgency of combating child sexual abuse material and strongly supports a collaborative approach to preventing its distribution. We therefore remain committed to the task of establishing a sustainable legal framework to address child sexual abuse as soon as possible. We express our gratitude to the Polish Presidency for its efforts in presenting a new proposal and striving to reach a compromise. Balancing technical and substantive discussions with political considerations is a complex challenge. It is recalled that in previous proposals that included mandatory detection measures, the Netherlands raised concerns about the potential impact on fundamental rights, particularly regarding privacy, confidentiality of correspondence and telecommunications, and digital security. The new proposal addresses some of these concerns, most notably through the removal of mandatory detection provisions, which we view as a positive development. We are committed to continue exploring this direction together and to engage in further discussions to achieve a balanced and effective approach. As stated in the Council working group, political decision-making on this compromise proposal is still pending.

In view of the upcoming Council discussions, we propose the improvements below and have questions and comments for the Presidency.

Comments on Presidency's new proposal

Removal of detection orders (Articles 7 to 11)

- We welcome and support the exclusion of the detection orders. Last November, the Dutch cabinet concluded that it could not support proposals that can de facto only be implemented through client-side scanning because of the implications on digital resilience and the impact on fundamental rights.

Article 3(4)

- Under the DSA (Article 34), VLOPs and VLOSEs are required to conduct annual risk assessments for all forms of online content. It may be undesirable if, under this regulation, they are classified as low risk and are only required to conduct an assessment once every three years. How does the presidency view this? Are VLOPs and VLOSEs exempt from the high-risk/low-risk classification?

Article 4(3): age verification

- This would be the first European legislation to make online age verification so widely mandatory. Other regulations and directives mention online age verification as a possible mitigating measure (e.g. DSA), but do not make age verification mandatory. This could have a significant impact. By making this obligation so broad, it could lead to providers or app stores pre-emptively applying online age verification to all users in order to comply with this obligation. We welcome the newly added terms regarding privacy, proportionality and transparency, but for now maintain a scrutiny reservation.

Article 4a: derogation from certain provisions of Directive 2002/58/EC

- The Netherlands previously welcomed the extension of the derogation regime so that companies would retain the ability to voluntarily detect child sexual abuse material online. Technology is critical to tackling this harm at scale.
- Some questions for the Presidency:
    - In an opinion of January 24, 2024, the EDPS recommended clarifying which legal basis of the General Data Protection Regulation (GDPR), applies to the voluntary processing of content or traffic data to detect online child sexual abuse. Does the presidency have more insight on this by now?
    - The Netherlands would like more insight on the detection techniques and technologies that platforms currently use under the derogation regime. Can the presidency present an overview of this? Previously, an overview of potential technologies was shared (at that time for mandatory detection). Is this overview still applicable, and/or does the presidency and/or Commission intend to update it?
    - The Netherlands is curious about the scope of Article 4a. This article refers to 'number-independent interpersonal communication services', while other articles of the compromise proposal refer to 'interpersonal communication services and hosting services'. Can the Presidency clarify how these definitions relate to each other and which platforms fall under which category?
    - The Netherlands has previously expressed concerns about the detection of unknown online child sexual abuse material and grooming. In the Netherlands' view, no technology is currently available that can detect unknown material and grooming in a manner that is both proportionate and justified. We are still assessing whether these concerns are alleviated when detection is voluntary rather than mandatory.
    - Can the presidency provide more insight into what technology exists that allows for the scanning of text with the purpose of the detection of grooming without it leading to the “deduction [of] the substance of the content” (article 4a(3)(c)(ii))?

Article 5(b)

- Under the DSA, no stamps or endorsements are handed out if a VLOP complies with its obligations. A “sign of reduced risk” included in this particular article could possibly act as an invitation to abusers, who might perceive it as a signal that a platform attracts certain target groups. Could the presidency provide some more insight into the purpose and background of the proposed categorization in this context?

Article 12 (3)

- We would like to note that the obligations in the DSA appear to be more clearly defined. It is not only required that reported material be "acknowledged," but also that the platform specifies the decision made regarding it: it should be clear whether the platform has removed the material or made it inaccessible. Additionally, we are of opinion that there should be an option to challenge this decision, in line with Articles 16 and 17 of the DSA.
- What is the motivation for limiting the obligation in Article 12(3) for service providers to establish and operation an "easy to access, accessible, effective, age-appropriate and user-friendly, in particular child-friendly mechanism" to high-risk services?

Article 13 (1a)

- In cases of an imminent threat to a child's life or safety, or when information suggests ongoing abuse, the Netherlands believes there should be a stronger alignment with the provisions on imminent threats to life in Article 18 of the DSA. In such situations, the Regulation should ensure that platforms and services immediately notify the appropriate authorities if they can identify an acute case of abuse.

Article 66

- The Netherlands welcomes the presidency's idea regarding the victims' board. It would be beneficial if support, like prevention, were made more concrete in the proposal, such as through a multidisciplinary approach.

B. Comments of 03.2025

1. Obligations for providers

- How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?
    - Providers should be **required** to assess the risks of CSAM on their services and take concrete risk mitigation measures, such as improving platform design, strengthening moderation policies, and offering user tools like reporting mechanisms. Accountability should focus on these proactive steps and regular transparency reporting, without linking accountability directly to detection, to avoid creating a de facto detection obligation.

- Do you agree to keep the term “prevention” throughout the text as suggested by the Presidency or do you prefer to revert to the term “risk mitigation” as in the Commission proposal?
    - The Netherlands prefers to keep the term ‘risk mitigation’ throughout the text, as it provides more clarity.

- Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?
    - (1) We believe it is crucial to make providers more accountable for protecting children and young people from sexual abuse. Preference for ‘shall require’ instead of ‘may recommend’. Thus reinsert previous text.
      (2) Preference for risk mitigation. Thus reinsert previous text.

- Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?
    - The obligation to ensure a user notification mechanism should apply to all relevant providers, not just high-risk services. This is especially important now that detection is no longer mandatory under the current proposal. As a result, the reporting of CSAM will rely more heavily on the willingness of platforms to voluntarily detect such content, but also — and crucially — on reports made by users themselves. Data from NCMEC clearly shows that a significant portion of reports originates from user notifications, underlining the importance of ensuring that all providers offer accessible and effective reporting mechanisms.

- We would also like to note that the obligations in the DSA appear to be more clearly defined. It is not only required that reported material be "acknowledged," but also that the platform specifies the decision made regarding it: it should be clear whether the platform has removed the material or made it inaccessible. Additionally, we are of opinion that there should be an option to challenge this decision, in line with Articles 16 and 17 of the DSA.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

- How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?
  - The derogation from certain provisions of the e-Privacy Directive should be designed with a clear focus on enabling the detection and prevention of the further spread of CSAM. To protect fundamental rights, greater transparency is needed on how platforms currently conduct voluntary detection, as this often remains unclear.
  - The conditions for detection must be defined and linked to clear safeguards, leaving no room for companies to interpret when and how exceptions to the e-Privacy Directive apply.

- Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?
  - Preference to keep the derogation integrated in this Regulation

- Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.
  - The Netherlands has previously expressed concerns about the detection of unknown online child sexual abuse material and grooming. At the moment, we are still assessing whether these concerns are alleviated when detection is voluntary rather than mandatory.

3. Use of technologies by providers

- How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?
  - A way to regulate the use of technologies by providers is to build on the longstanding practice of voluntary detection. Many large platforms have already developed their own detection systems to actively detect and remove CSAM, which reflects both their societal responsibility and their obligations under for instance Directive 2011/93/EU to combat CSAM.
  - The focus of regulation should be on strengthening safeguards, particularly through increased **transparency** about how detection works, **which technologies** are used, and what measures are in place to **protect users' rights**.

- At the same time, the use of detection technologies on the basis of this proposal should remain voluntary for platforms, ensuring that regulation does not impose such burdensome conditions that it discourages platforms from scanning altogether or constitutes a disproportionate infringement on the fundamental rights of users. The regulation must strike a balance between minimizing the infringement on fundamental rights (through conditions) on one side, and on the other side avoiding excessive requirements that would remove the incentive for platforms to engage in voluntary scanning. A balanced approach is crucial to protect both cybersecurity and fundamental rights while ensuring effective detection.

- Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?
  - Yes.

4. Reducing complexities and administrative burden

- How do you see the best way of reducing complexities and administrative burden in this Regulation
  - A way to reduce complexities and administrative burden in this Regulation is to ensure clear and straightforward task-setting.
  - For example, under the DSA, very large online platforms (VLOPs) are not given any form of stamp or endorsement when they comply with their obligations. Introducing a "sign of reduced risk" in this Regulation adds unnecessary complexity and does not provide clear added value. We recommend removing such elements to keep the framework focused, practical, and easy to implement.

- Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?
- Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?
  - The Netherlands has consistently supported the idea of establishing an EU Centre and continues to do so.
  - We welcome the Centre's adjusted focus as a knowledge hub, its role in developing a communication strategy, fostering dialogue between stakeholders, strengthening prevention efforts, and supporting providers' activities under Article 4a. We also see value in giving Member States the option to request the Centre to assess the effectiveness of prevention measures.
  - At the same time, we are still considering whether under this proposal sorting out false positives before forwarding materials to law enforcement should fall within the Centre's scope. This seems to overlap with tasks that are traditionally the responsibility of law enforcement authorities. Moreover, it is important to note that a human review by the provider itself is already a required step when potential CSAM is detected.

5. Review clause

- How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?
    - The Netherlands supports the idea of including a review clause. It would be valuable if the review not only assessed the technology but also took a broader perspective, evaluating the overall approach, including its impact and effectiveness. While the Commission inherently has the flexibility to adapt to future regulations, the review could help ensure a well-informed and timely response if adjustments are needed. The EU Centre could play a role in this process. A strong foundation for this review could lie in annual reporting on voluntary detection, where the quality and consistency of reporting could be further improved.

PORTUGAL

A. Comments of 02.2025

In general, it can be said that the Presidency presents an innovative and drastic solution to a compromise, which provides effective tools to limit the spread of Child Sexual Abuse (CSA) online, while ensuring full respect for Fundamental Rights and at the same time addressing concerns related to the protection of cyber-resilience and cybersecurity.

The new document proposes more emphasis on prevention, voluntary detection and the strengthening of privacy and cybersecurity safeguards, taking advantage of national capacities and reinforcing the role of the EU Centre as an important entity in the child protection system.

More specifically, the main elements of the compromise are highlighted:

a) detection orders are removed from the scope of the regulation (Articles 7 to 11);

b) a review clause is maintained which invites the Commission to evaluate, within three years of the entry into force of this Regulation, the legal and technological possibilities of mandatory detection in the future (Article 85);

c) The derogation from certain provisions of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) is included in the regulation as a permanent measure (Article 4a);

d) The amendments resulting from the change in the scope of the proposal, focused on strengthening prevention aspects, are introduced throughout the text, in particular with regard to the functions of the coordinating authorities, other competent authorities and the EU Centre;

e) Greater emphasis is placed on child protection measures in the digital environment. High-risk service providers, in cooperation with the EU Centre, should be required to contribute to the development of reliable and accurate technologies to detect CSA online. Collaboration between service providers, Member States, other stakeholders and the EU Centre should support efforts to prevent CSA online and contribute to the wider child protection framework.

Having analysed the first 28 articles, the following can be seen:

- Chapters I and II have been profoundly modified, and the remaining articles have been moulded to this new proposal;
- A first reading raises many questions about the proposed articles, which are very complex to read and not always apparently coordinated. There are also technical questions that need to be resolved with those who can answer them on a sectoral basis;
- So the questions we have to ask for now, and which can serve as a general comment, are as follows:
  - **Article 1(1) in particular** uses concepts that are difficult to apply: for example, paragraph 1(d) '*obligations on providers to prevent users from accessing child sexual abuse material*.' This paragraph in particular, which is more like a recital, needs to be reworded;

- **Article 3**: in this article, the obligations of the receivers of this regulation remain undefined. Who is obliged to carry out the risk assessment? These organisations provide services at a multinational level, so to impose obligations only on the basis of the service provision criterion is confusing to say the least (paragraph 1), *i.e.* are they obliged to carry out a risk assessment wherever they provide services? And what implications does this solution have for the final systemic organisation of the proposal? The same applies to Article 6;
- Article 4: this article on prevention needs to interact with article 5 and subsequent articles, as it is unclear what order these articles should be applied in: do they apply article 3 on prevention and then the risk assessment and risk categorisation? and what is the point of risk categorisation? is it only to adopt the necessary measures (article 3(4) and article 5(2b)), as these are not identified? And what to do in the event of multiple situations of a transnational nature? We don't think this situation has been resolved.
- **The regime of Articles 14 and 14a** are apparently still overlapping, since the former has as a condition of application the possibility of an entity asking different entities for removal in several member states and Article 14a contains precisely the regime of transnational removal orders. These rules apparently also contain a different regime from Article 16 on blocking orders, since they refer to subjection to national jurisdiction; but again, when it comes to the regime of Article 18, it is similar to that of Article 14. We'd also like to understand the reason for this differentiation.
- **The terminology used** continues to pose problems: in particular the use of the word "suspects", which is specific to criminal proceedings (Art. 4 a al.))c)));
- **"Delegated powers"** are often considered. We already pointed this out in the previous negotiations, and in our opinion it's too large.

For all the reasons set out and analysed so far, Portugal expresses :

- regret at the lack of ambition of this compromise solution, but recognises that the fight against online sexual abuse must remain a priority.;
- positive analysis reservation, and considers it is essential that the amputation of Articles 7 to 11 should be counterbalanced with a rule such as Article 85, the exact terms of which will have to be negotiated.

B. Comments of 03.2025

Regarding Doc. 05352/25:

Portugal, although it considers that this Proposal falls short of expectations, recognises and recognises and is grateful for the efforts of this Presidency (as well as the previous ones) in trying to find consensus and compromises on such a sensitive issue that has been the subject of multiple debates.

This is why, as stated in LEWP meeting of March 11, Portugal remains in favour of the negotiations, but stresses that this new proposal does not added value to the regime that exists today, in different dimensions, namely in terms of Prevention and Combat, with regard to what is crucial and fundamental: the best interests of child protection.

Thus, in line with the position expressed several times, it is considered necessary to find an appropriate balance between the various rights in question, while considering that the effectiveness

of this proposal is non-negotiable, both in terms of prevention and in terms of combating a phenomenon that must be eradicated as soon as possible.

As a result of the lengthy negotiations, we recognise the merit of PRES PL, like all previous Presidencies, in seeking to bring the negotiations to a close, promoting new approaches to this end.

it is reiterated that this proposal does not add value to its main purpose. In other words, it does not contain measures to guarantee a minimum level of protection for children, since it removes detection orders, but does not does not establish any measure that, in any way, compensates for such removal, just as it does not establish any measures that could compel (de facto oblige) providers to act in defence of the most basic objectives of the Regulation.

It can be concluded that this proposal does not add value to the regime currently in force, namely because: *(i)* it does not establish an effective system that promotes the earliest possible detection of CSA situations (and material); *(ii)* it does not create clear requirements for providers that encourage them to minimise the risk of their services being used for CSA; and/or *(iii)* to develop (collaborate in the development of) technologies that make it possible to move towards the detection of new material and grooming situations in the future, while guaranteeing the privacy of communications and the protection of E2EE.

Regarding Doc. 06475/25:

1. Obligations for providers

First of all, it should be noted that the reformulation makes use of vague / generic and poorly defined concepts, such as such as:

- the obligation to make 'best endeavours' which, in practice, allows innocuous measures to be taken, especially as it is not accompanied by obligations / sanctions in the event of such measures being taken.;
- the obligation to contribute effectively, especially as it is not linked to 'incentivising' sanctioning measures;
- the use of recommendations instead of obligations;
- the use of the terminology prevention, which differs greatly from risk mitigation measures, which in a risk analysis system require reducing the degree of risk previously determined (remember that the Regulation is aimed at preventing and combating CSA).

- ***How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?***
  - The best way to hold service providers accountable for preventing and mitigating the risk of child sexual abuse and exploitation, without this translating into an obligation to detect it, is to adopt a model based on risk assessment and proportionate mitigation measures, regulated by independent supervision and sanctioned by a well-defined accountability regime, which includes:

- Mandatory Risk Assessment;
- Implementation of Mandatory Mitigation Measures (proactive moderation of published content, effective and user-friendly reporting systems, parental controls and age verification, Safety by Design);
- Independent Supervision (European Centre) and preparation of Compliance Reports;
- Accountability and sanctions regime.

➢ We advocate a regime that obliges providers to adopt risk assessment and mitigation measures, but that continues to consider the existence of detection orders.

➢ We advocate the adoption of a mechanism that makes it possible to issue court orders for detection whenever there are indications that a platform is being used to disseminate CSAM.

➢ Providers who do not co-operate in implementing mitigation measures or removing detected CSAM should be subject to significant sanctions.

Portugal defends that a common regulatory framework is essential including a sound regulation of ICT companies and internet intermediaries . This would be including legal content moderation, content removal, transparency, risk assessments and safety by design organized accordingly to article 28 .1 of DSA that mentions the following:

Article 28

Online protection of minors

1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.

2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.

3. Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.

4. The Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1.

In this way both providers and users could to understand with no doubts what they are supposed to do, and what is the major objective of their actions .

Portugal believes that the proposed rules on content moderation, trusted flaggers, users rights, report and risk assessment, liability and electronic notification system would benefit from a more oriented framework and that safety by design rules would need more attention (this is only mentioned on article 5,2,a),b) (ST 5352en.25)).

- ***Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?***

  - The term 'prevention' suggests a broad and absolute obligation to avoid any risk, conveying the idea of a stronger commitment to eliminating the problem. The concept of 'risk mitigation' recognises that risk cannot be completely eliminated, but can be reduced through proportionate and effective measures.

To summarise:

We agree with the adoption of the term 'prevention' and suggest that the Regulation specify concrete prevention measures (*e.g.* warning systems based on predefined and periodically reassessed risk indicators).

we agree to keep the term prevention because it gives a better finalistic perspective. It also paves the way to the strategic perspoective that the PCY mentions. Neveretheless we have to be careful in order not to create any confusion with other legal realities like risk assessemnt on article 34 of DSA. Calling the same obligations differentlty would create a bigger confusion.

- ***Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?***

  - The Commission's original text established clearer and more objective criteria on how service providers should assess and mitigate risks. The Presidency's version is more pragmatic and could allow faster intervention by the authorities on platforms that represent a high risk. It is suggested that response deadlines be set so that providers provide information quickly and incur significant fines if they do not comply.

- ***Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?***

  - We argue that the obligation to notify the user laid down in Article 12(3) should apply to all service providers (not only the relevant or high- risk services), since there is always a risk that criminals will migrate to platforms that are not obliged to provide such notification.

2. <u>Scope and design of the derogation from certain provisions of Directive 2002/58/EC</u>

• How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?

- The derogation from certain provisions of the E-Privacy Directive is fully justified when the grounds are based on the protection of children, in particular with regard to sexual abuse and exploitation, and must comply with the Principles of Necessity and Proportionality and be based on defined deadlines.

• Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?

The inclusion of the derogation as part of the existing regulation ensures the coherence of the legislative framework, creating a more cohesive and unified structure for the management of privacy regulations. It facilitates understanding and compliance by stakeholders. On the other hand, including derogations in an existing regulation can increase the complexity of its interpretation and application, especially if those derogations are very specific and require certain conditions to be met.

In this sense, from a regulatory point of view, PT would prefer to have this derrogation integrated in this Regulation, having a unique instrument to deal with all the subject

• Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

- If the scope of the derogation is kept analogous to the current regulation, it will reflect the specific need to process personal data in contexts of legitimate public interest, such as the prevention and investigation of serious crime, including combating the sharing of child sexual abuse and exploitation content.
- We do agree with the scope of the derrogation as suggested by the Presidency.

3. <u>Use of technologies by providers</u>

From the discussion so far on the use of technologies by providers, it appears that all MS agree that there should be no obligation for service providers to carry out detection "in a generalised and indiscriminate manner». The problem is that they (and other organisations, such as the Legal Services of the Council and the Commission) have completely different views on what should be considered as such. Even so, in view of the argument made by some MS that detection should only focus on 'suspects', the legal basis of the Proposal for a Regulation is recalled, and the use of that concept refers to the application of criminal law (and not the future Regulation resulting from this proposal).

As for the exclusion of encryption from the scope of this regulation, it is felt that this would render it ineffective and obsolete in the very short term, thus making it undeserving of future discussion, namely because it goes in the opposite direction to what Chiefs of Police and other organisations have repeatedly said (see the conclusions and recommendations of the HLG on access to data) have been warning of as urgent and absolutely necessary.

- ***How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?***

- The best way to regulate the use of technologies by providers, with a focus on cybersecurity, is to create a set of rules that guarantee the protection of personal data and security in cyberspace and encourage transparency and accountability. Regulation must be proportionate, so as not to stifle innovation, but to ensure that the risks associated with

cyberspace are properly managed, with robust security measures and continuous vigilance to ensure compliance with cybersecurity and data protection principles.

- PT believes that on this subject platform reporting mechanisms are to be specially importante.

- ***Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?***

- Yes, we agree with the proposal to invite the Commission to prepare a list of the technologies used by suppliers under the derogation regime, as well as to provide information on existing technologies to detect grooming;

- But we should also ask why this overview is going to be prepared only to grooming detecting tech?

4. <u>Reducing complexities and administrative burden</u>

• How do you see the best way of reducing complexities and administrative burden in this Regulation?

- Language clarification and simplification;
- Harmonisation of requirements;
- Automation and digitalisation;
- Simplification of compliance procedures;
- Avoiding bureaucracy: Reducing reports and other documentation requirements;
- Specialised training and support for Service Providers.

- The documents should be redrafted envisaging only a simpler proposal. IT would also be important to have in mind the differences from EUROPOL competences and the Center competences.

• Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?

- Maintaining the classification of risks and the reduced risk signal, as proposed by the Presidency, seems to be an efficient way of balancing security, flexibility and effectiveness in complying with the regulation, which implies a structure that allows for risk differentiation and proportional mitigation without creating an excessive administrative burden;

- Yes to the sign of reduced risk, we see no harm aboout it. We also think that risk categorisation provision should be more clear namely on the consequences.

• Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

- Maintain the EU Centre with the aim of centralising functions and responsibilities related to the prevention of online abuse, the monitoring of technologies to combat the sexual exploitation of children and cybersecurity, in order to facilitate the coordination and implementation of consistent policies across the European Union;

- PT believes that the EU Center is an adequate mean to obtain what we want. It is not in the penal orbit, and it can provide prevention (in the broadest sense), a sound connection with NECMEC, and could also create an excellent bridge with law enforcement and security issues (EUROPOL, INTERPOL). IT can create sinergies with all these entities . It should also be in connection with tech and create a path to assisting. Again, it would be essential to have a clear comparison of the competeneces of both structres (EUROPOL/ Center).

5. <u>Review clause</u>

• How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?

- The review clause is a key mechanism to ensure that the regulation remains relevant and effective as circumstances change and new technologies or challenges emerge.

In order to ensure that the European Commission can propose new legislation within 3 years of the entry into force of this Regulation, the review clause should be clear, flexible and ensure a comprehensive evaluation. The clause should include:

- Clear objectives and assessment criteria;
- Flexibility for occasional adjustments without jeopardising stability;
- Clear deadlines and procedures to guarantee a timely review;
- Consistency with other European regulations and guarantee of legal stability.

- ***How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?***

  - A clear definition of the roles and responsibilities of each of these entities is essential to guarantee an integrated, coordinated and effective approach to preventing and combating CSA.

ROMANIA

A. Comments of 02.2025

- In RO view, in the current form proposed by the PL PRES the instrument is not likely to be effective and does not represent the direction in which it should have been moving. Thus, RO considers that the **removal of detection orders** from the Regulation raises significant problems. If Detection Orders, when all other prevention or mitigation measures have failed, were strictly applied with all appropriate data protection and fundamental rights safeguards, they would be an essential tool to ensure a prompt and effective response in identifying and removing CSA material. Without this provision, the ability of authorities and providers to pro-actively detect illegal content is reduced, which could actually favor criminals.
- RO does not see detection orders as an issue that would affect fundamental rights as long as they are implemented in such a way as to avoid abuse and to protect user privacy. Moreover any abuse would be a separate offense which would in turn be punishable by law. RO believes that the complete **removal of orders undermines the effectiveness of efforts** to combat online child sexual abuse. In other words it undermines the responsiveness and prevention necessary to protect children online.
- With regard to Art 4a, the impressions are mixed. On the one hand, RO appreciates that the text is detailed and comprehensive, emphasizing strict safeguards, accountability mechanisms and transparency. There is an effort to balance law enforcement objectives with the protection of fundamental rights. However, on the other hand, contrary to the name of the article, much of the text seems to be a reiteration of the existing framework established by Directive 2002/58/EC and even the GDPR Regulation. The focus remains on ensuring strict compliance with existing practices, rather than exploring new methods to adapt to the evolving technological landscape. In essence, the text appears to codify and clarify current obligations, rather than push the boundaries or introduce new tools to combat CSAM online more effectively. That said, the text does not appear to bring revolutionary advances in the fight against online child sexual abuse, but rather reinforces already established standards.
- The **technology** is advancing rapidly and therefore it is essential that the rules in the Regulation are flexible and allow for rapid updates to maintain an adequate level of data security. In other words the legal text must be adapted for the future.
- For the above reasons, RO cannot support the current version of the compromise text put forward by the Presidency and hopes that an alternative will be found to make this Regulation a truly effective instrument.

B. Comments of 03.2025

1. Obligation for providers

➢ **How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?**

We have always mentioned and will continue to do so that we need to balance the protection of children against sexual abuse (CSA) with fundamental rights such as privacy and data protection. Thus, providers should be obliged to carry out risk assessments, tailored to the specifics of their

services, which should identify the likelihood of CSA risks and set out appropriate mitigation measures. We believe that strict content moderation policies, reporting mechanisms and user vetting processes should continue to be implemented and maintained, just as they are now in place for voluntary detection. In relation to e2e communications, they need to be protected, but at the same time the development of technologies that allow the detection of CSA risks without violating users' privacy should be encouraged.. Metadata analysis, the hash value of shared files, but also behavioral habits, such as an account of an adult frequently contacting minors, should be considered.

Working with authorities to establish best practices for detecting patterns of abuse without compromising privacy is vital. It is clear that we need to establish by regulation that providers should have a legal obligation to take reasonable and proportionate steps to prevent and mitigate CSA risks, but leave no room for interpretation, as to imply that there is a general monitoring obligation.

- **Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?**

Although the terms appear to be the same, they are quite different, and when implemented in legislation can be determinative of the purpose of the legislation. Thus, using only the term "*prevention*" may imply an absolute obligation to eliminate CSA risks, which is not realistic, as all CSA risks should be stopped before they occur. This may lead to requirements such as blanket monitoring. It would basically affect fundamental rights. On the other hand the term "*risk mitigation*" is already used in the DSA and implies measures to reduce the impact of CSA risks once they have been identified. It seems more flexible so that other fundamental rights can be respected. It may lead to the development of the technologies needed to detect illegal content without compromising encryption or confidentiality of communications.

- **Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?**

We prefer the previous text with the term "*risk reduction*".

- **Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?**

We don't necessarily see a problem with limiting it to high-risk services, if this classification is maintained in the regulation, but we would prefer it to apply to all relevant providers.

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

- **How do you see the best way of designing the derogation from certain provisions of the privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?**

We believe that there should be a balance between clarifying and strengthening existing obligations and stimulating innovation in the detection and prevention of CSAM, without requiring blanket monitoring. We believe that voluntary detection is already a system that should be protected because it works, thousands of victims have been saved because of voluntary detection, so the text needs to recognize its role and provide a framework that supports providers in this practice without

discouraging existing initiatives. Our idea is that we need to strengthen existing standards, but it is necessary to create a framework that stimulates technological progress and collaboration to combat CSA more effectively.

- **Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?**

We believe that a solution must be found in this regard, whatever it will be, to continue with the provisional regulation or to keep it within the text of the CSA Regulation.

- **Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.**

At the moment it is not very clear. From a legal point of view we do not know whether it is possible for the two regulations to operate in parallel given their purpose. The text proposed by PL PRES is detailed and comprehensive and this possibility could also be taken into account.

3. Use of technologies by providers

- **How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?**

First of all it is clear that a mass monitoring system should be avoided. Then if upload moderation and "client side scanning" will not be used we are left with only metadata analysis, material hash value analysis and client behaviour analysis. It is clear that we have to keep that much at least for the time being otherwise we will have no chance of stopping this criminal scourge. By encouraging innovative technologies, ensuring transparency and imposing robust cybersecurity measures, the regulation can create a safer and more secure online environment without introducing systemic risks. At the same time, we believe that the regulation should already now establish the basis for permanent collaboration between cybersecurity experts, providers and law enforcement, to adapt measures and best practices as technology evolves.

- **Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?**

Yes, of course.

4. Reducing complexities and administrative burden

- **How do you see the best way of reducing complexities and administrative burden in this Regulation?**

We believe that alignment with other legal instruments, the DSA, GDPR and even the cybersecurity directives could reduce the excess work as well as the administrative burden. Moreover, reporting should be centralized and at longer periods than many periodically. The text should leave as little room for interpretation as possible, so the rules must be clear to prevent legal uncertainty.

- **Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?**

We have supported this in the past and we support it now. Only when they are implemented will we see whether they are counterproductive or not.

- **Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?**

We are dealing with a criminal phenomenon that we do not see disappearing any time soon. We believe the Centre is needed, whatever roles it will ultimately play. Replaced by more structures would slow down the process of fighting these crimes. We prefer the collaboration with these structures and network of experts.

5. Review clause

- **How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?**

The review clause should require an evaluation covering several aspects: - the effect on the fight against CSAM; the impact on fundamental rights; the assessment of whether new technologies or their risks require legislative adaptations; feedback from stakeholders.

We believe that we should also have a partial Commission assessment before the full review report. At the same time, developments in other legislation in relation to CSA Regulation should also be taken into account.

- **How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?**

The development of new technologies for the prevention of CSA requires a multi-stakeholder approach in which stakeholders must have a clearly defined role. We believe that the Centre should work with partners in the technology industry to provide guidance for the development of standards for CSA detection technologies. NGOs can also work with academia and industry to conduct independent research, providing important insights into the effectiveness and ethical implications of different technologies. Moreover, they should promote the development of technologies that not only combat CSA, but also protect privacy and freedom of expression.

SLOVAKIA

A. Updated comments of 02.2025 (03.2025)

Firstly, we wish the Polish Presidency a success in making progress on this important dossier, also in the view of the deadline for expiry of the temporary legislation.

We also thank the Polish Presidency for the work on the new compromise text.

From the beginning of the negotiations, Slovakia has consistently supported the proposal, endorsing its original comprehensive scope, which included both known and unknown CSAM, as well as the solicitation of children. This also extends to the issuance of detection orders, provided that a balance between the involved fundamental rights is achieved and adequately robust safeguards are in place.

On one hand, we welcome the endeavour to empower the prevention aspects of the proposal. However, by removing the central part of the proposal - the detection orders and building on voluntary detection the current text changes the basic logic of the original proposal by the Commission.

Acknowledging the significant added value in the voluntary detection of CSAM and grooming by online services providers under the Temporary Regulation regime, our aim should be an effective long-term legal framework applicable to all providers of relevant online services and to all forms of online child sexual abuse.

At the last JHA Council in December 2024, in order to move forward with the negotiations, Slovakia was in a position to support, with reservations, the HU Presidency´s compromise proposal, which already substantially narrowed the scope of the original proposal.

This said Slovakia, considers the new approach of the PL PRES insufficient to combating the different forms of online child sexual abuse and sexual exploitation.

Following the discussion at the LEWP on 5 February, these elements are essential from our perspective in order to move forward with the current text:

- a clear obligation on service providers to effectively prevent the dissemination of CSAM and grooming needs to be included,
- effective inclusion of encrypted services in the scope in relation to the prevention obligation,
- the proposal cannot worsen the current situation under the temporary and bring an added value,

- therefore, these elements should be maintained in the text:
    - the child safety by design obligations (risk assessment, risk reporting);
    - voluntary detection;
    - the EU Centre;
    - the review clause;
    - the temporary extension of the Interim Regulation for the transition period.

In the light of recent technological developments, the EU should not lag behind in the effective fight against child sexual abuse and exploitation; moreover, human dignity and the best interests of the child should remain a high political priority.

Slovakia is willing to continue further work on the proposed Regulation with the aim to reaching a partial general approach, however conditioned that the legal framework is legally sound, efficient and achieves real progress.

Following the discussion at the LEWP on 11 March we would like to make these additional comments:

We believe that, if the proposal is to be a step forward from the status quo, the obligation for providers to carry out prevention should be more clearly defined in Articles 1(a) and 4(1).

We prefer the term “risk mitigation” over “prevention”, in line with the wording of the DSA Regulation, as proposed in the original proposal by the Commission. We would agree that the term provides greater clarity and is easier to assess and measure (also following the application of Article 35 of the DSA).

We prefer reinstating the previous text in Article 5a (1) and (2).

We think the user notification mechanism in Article 12(3) should apply to all relevant providers not only to high-risk services.

We support strong protection of encryption. The proposal should not be interpreted as a prohibition or weakening of end-to-end encryption.

At the same time, Slovakia also advocates for the technological neutrality of the proposal, in our view, there is a need to achieve effective implementation of prevention by all providers, including encrypted platforms, so that encrypted platforms do not become an impunity haven.

Despite the deletion of the detection order from the scope of the proposal, we still see added value in the establishment of the EU Centre.

We also see added value in the risk categorisation of the services – where some simplification could be considered.

On the other hand, we do not see much of an added value in keeping the sign of reduced risk.

We support the inclusion of the review clause in the proposal, the content as such shall reflect and depend on the final text of the proposal.

SPAIN

A. Comments of 02.2025

After analysing the proposal, Spain does not consider it acceptable due to the lack of elements ensuring that it will meet the established objectives of protecting children through the prevention and fight against online child sexual abuse content. To this end, it is necessary to introduce measures that guarantee the protection of minors, just as measures have been introduced to ensure the privacy of communications.

For Spain to consider that the regulation adds value and represents a step forward from the current situation and in the protection of minors, it is essential to establish a general and clear obligation for service providers to combat CSAM content, serving as a countermeasure against the removal of detection orders. Additionally, this general obligation must be enforceable through the imposition of sanctions under Article 35 in cases of inaction within 24 hours following a user's report through the available 24/7 channels, or failure to immediately communicate to the competent authorities or through the European Centre in cases of verified CSAM content or grooming practices.

In line with the above and to ensure that the obligation of providers is clearly established, the following changes are considered necessary:

- Article 1(a):

  (a) obligations on providers of relevant information society services to ~~minimise the risk that~~ **~~make best efforts to~~ effectively prevent the use of** their services ~~are misused~~ for online child sexual abuse;

- Article 4(1):

  (1) **If p**roviders of hosting services and providers of interpersonal communications services **have identified a risk of the service being used for the purpose of online child sexual abuse pursuant to Article 3, they** shall ~~take **all** reasonable~~ **put in place appropriate and proportionate** ~~mitigation~~ measures, tailored to ~~the~~ **that** risk ~~identified pursuant to Article 3~~, **to effectively prevent online child sexual abuse in their services** ~~minimise that risk~~. […]

The possible prevention measures that providers could take should not be unduly limited and companies can take the full range of prevention measures. This includes prevention measures that require accessing metadata or any other data stored in the device, exclusively for the purpose of preventing child sexual abuse online. Therefore, the references in the document to Article 5(3) of the e-Privacy Directive should be reinstated and incorporated as needed in the compromise, notably on the new Article 4a:

- Article 1(4):

  (4) This Regulation limits the exercise of the rights and obligations provided for in Article 5(1) and (3) and Article 6(1) of Directive 2002/58/EC **to the extent strictly** ~~insofar as~~ necessary **in accordance with Article 4a.** ~~for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 **II** of this Regulation~~.

- Article 4a(3):

(3) Regarding the scope of the derogation, Articles 5(1) and (3) and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that: […]

3(d)(viii):

(viii) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and (3) and 6(1) of Directive 2002/58/EC […]

In order for the National Coordination Authority to fulfill its role and establish additional risk mitigation measures, it should have the possibility to require the provider to introduce such measures if it considers that those initially suggested by the provider were not sufficient. For that, the text in **Article 5a** that had already been agreed should be reinstated as otherwise there would be an unduly limitation **of the powers of national authorities** to ensure that providers comply with the obligation to prevent. Specifically:

1. **Without prejudice to Articles 27 to 29, where on the basis of its assessment referred to in Article 5(2), the Coordinating Authority of establishment determines that a provider offering a service or parts or components of a service classified as high risk or medium risk has not met the requirements of Articles 3 or 4, it shall require ~~may recommend to~~ the provider of […].**
   The Coordinating Authority of establishment may request the EU Centre for an opinion on technical aspects of the possible actions that it intends to ~~recommend~~ require pursuant to the first subparagraph.
2. **A provider that is required to perform~~s~~ the actions specified in points (b) or (c) of paragraph 1 shall re-conduct […].**

Following the necessary modifications and after the elimination of Article 10(1), the previous wording of Article 1(5) should be reinstated because, with the current wording, it discourages the initiative of providers who, without endangering the encryption of communications, decide to implement innovative technologies to detect CSAM content and grooming. In this regard, we propose the following wording for Article 1(5):

(5) ~~Without prejudice to Article 10(1), This Regulation shall not prohibit, make impossible, weaken, circumvent or otherwise undermine cybersecurity measures, in particular encryption, including end-to-end encryption, implemented by the relevant information society services or by the users.~~ This Regulation shall not create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to decrypt data or create access to end-to-end encrypted data, or that would prevent providers from offering end-to-end encrypted services.

To strengthen the response of the provider, it is proposed to modify Articles 12(3), 13(1), and 13(1a) to introduce the need to establish reporting mechanisms that are always available to users and that such information is promptly communicated to the Control Authority or law enforcement agencies. Therefore, we propose the following wording:

12(3) The provider shall establish and operate **for a service or the parts or components of the service classified as high risk according to Article 5(2)** an **easy to access,** ~~accessible~~**, effective,** age-appropriate and user-friendly, **in particular child-friendly**, **24/7** mechanism that allows users to **notify** ~~flag~~ to the provider **information that indicate** potential online child sexual abuse on **its** ~~the~~ service. **Those mechanisms shall allow for the submission of notices by individuals or entities exclusively by electronic means.**

13(1) Providers of hosting services and providers of interpersonal communications services shall submit the report referred to in Article 12, **within 24 hours of notification,** using the template set out in Annex III.

13 (1a) By deviation from paragraph 1, where the information referred to in Article 12(1) reasonably justifies the conclusion that there is likely to be an imminent threat to the life or safety of a child or when the information indicates ongoing abuse, the report referred to in paragraph 1 of this Article has to be immediately submitted and shall include: […].

Once the obligation of providers has been established with the aforementioned changes, the previous wording of **Article 19** should be reinstated, although the additional inclusion of prevention in the list of provider actions included in the article can be accepted.

B. Comments of 03.2025

From Spain, we continue to strongly support the Commission's initiative. We believe that it is essential to reach an agreement on a compromise text that offers added value and goes further in the protection of our minors, since, unfortunately, the voluntary basis established in the Interim Regulation has proved to be insufficient.

Having reiterated Spain's commitment to combating CSAM content, and before addressing the Presidency's questions, please consider the following observation:

It is clear that the proposals made during the Belgian and Hungarian presidencies came very close to agreement. However, the current text has reopened debates that were previously considered closed and has introduced new issues that did not exist in the previous proposals. We therefore see it as a step backwards in the efforts to reach agreement. Instead, we believe it would be more productive to build on these earlier texts, proposing amendments only in areas where disagreements persist, rather than undertaking such an extensive revision, which will inevitably prolong the process of reaching consensus.

Questions to delegations:

1. **Obligations for providers**

- **How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?**

If an adequate countermeasure to the removal of detection orders is to be established, a clear and unambiguous obligation to combat CSAM content should be placed on service providers. For them, it should be possible to sanction those who are proven not to have complied with it due to a lack of due diligence, e.g. for not having detected the case when it was notorious (e.g. through risk patterns provided by the EU Centre or the LEAs) or had the technical capacity to do so (e.g. in the case of unencrypted or open communications) or was reported by the user and did not take the necessary measures. Another way to measure the outcome of mitigation measures is through the collection of statistical data on complaints or cases discovered, so that the outcome of such mitigation measures can be translated into a measurable numerical result, e.g. on an annual basis.

- **Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?**

We prefer the terminology proposed by the Commission as it is more in line with the terminology used in risk analysis and the DSA.

- **Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?**

Not only Article 5a(1) and (2), we consider that the previous proposal as a whole was better aligned with Member States' positions. The current proposal is now further away from agreement than it was in December, depriving authorities of the necessary tools to be able to oblige service providers to take risk mitigation measures.

- **Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?**

Limiting reporting obligations to high-risk services is an unacceptable step backwards in the scope of the regulation, which is already severely limited by other requirements, and would increase the risk of not being able to respond adequately to CSAM in services classified as medium or low risk.

2. **Scope and design of the derogation from certain provisions of Directive 2002/58/EC**

- **How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?**

We consider that the regulations should always be as clear as possible, trying to make them self-contained in order to avoid having to deal with different regulatory texts in order to fully understand them.

- **Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?**

It is considered that a reference to the temporary regulation should be avoided when the regulation is adopted, so that the provisions of the directive that need to be extended over time should be incorporated into the regulation.

- **Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.**

We agree with the Presidency's proposal.

3. **Use of technologies by providers**

- **How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?**

With the current wording, even the use of content-screening technologies by providers on a voluntary basis is limited. As mentioned above, we consider that previous texts dealt with this issue in a better way.

In any case, the proposal should ensure technological neutrality, which is not the case with the current proposal.

- **Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?**

It is agreed to invite the Commission to update the status report on existing technologies.

4. **Reducing complexities and administrative burden**

- **How do you see the best way of reducing complexities and administrative burden in this Regulation?**

Categorisation is still a good measure if suppliers are incentivised to apply it because it adds to the bureaucratic burden and streamlines the application of risk mitigation measures, but there must be an incentive for suppliers to do so, beyond being able to attach a label, for example by reducing the amount of fines in case of non-compliance.

- **Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?**

Risk categorisation was introduced by the Belgian Presidency as a measure to ensure the proportionality of detection orders and thus to try to bring closer together those states that considered detection orders necessary in all cases and those that did not agree with this measure. Once detection orders have been eliminated, it makes no sense to maintain risk categorisation except as a measure to modulate sanctions or to rationalise the application of risk mitigation measures.

- **Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?**

With the role proposed by the presidency, the main functions it should assume have been removed, although it is still seen as adding value.

5. **Review clause**

- **How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?**

Article 17(2) of the Treaty on the Functioning of the European Union confers legislative initiative upon the Commission. Consequently, any invitation to draft new legislation is regarded as lacking substantive effect, amounting merely to a statement of intent without binding force, and thus more appropriately placed in the recitals of a regulation rather than within the operative provisions.

- **How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?**

The EU Centre can become a driver for new initiatives and a point of contact between providers, authorities, academia, civil society, etc., as well as remaining the central point for receiving alerts and reports.

SWEDEN

A. Comments of 02.2025

Sweden has a scrutiny reservation. The positions below are therefore preliminary.

SE regrets the lower level of ambition resulting from the deletion of all references to a mandatory detection order (art. 7-11). SE is open to solutions that are less far-reaching than deleting the detection order, while emphasising the importance of reducing the risks of undesirable effects on secure communications and cybersecurity in the EU.

SE sees positively on the proposal to make the possibility of voluntary tracing permanent (Article 4a), especially in combination with the mandate to the EU Centre to promote measures to combat online abuse (Article 43(7)) and to provide information on available technologies (Article 50).

As regards the proposal to strengthen preventive measures, SE would like the Presidency to clarify the purpose of replacing the wording *risk mitigation* with *prevention* throughout (e.g. Art. 4) and what is intended to be achieved in practice with those changes.

B. Comments of 03.2025

Sweden has a scrutiny reservation. The positions below are therefore preliminary.

Obligations for providers

There should be requirements on service providers to implement measures, and SE therefore prefers that the previous wording indicating obligations, such as Article 5a(1) and (2) (*shall require* instead of *may recommend to*), is retained.

Service providers should also can also make improvements themselves. SE therefore wonders why this possibility has been deleted in Article 3(5) and Article 5(1)(c) and why the Coordinating Authority is no longer able to order service providers to take additional measures (Article 5a(1)).

SE prefers the concept of "risk mitigation" because we perceive it as more focused on actual measures. In some places the change to "prevention" is also a bit strange, see e.g. art 4.2 (a) or art 44 and 50 where *detection* has been replaced with *prevent* even though (voluntary) detection remains an option.

SE prefers that the notification mechanism for users applies to all service providers, i.e. not limited to only high-risk providers.

Scope and design of the derogation form certain provisions of Directive 2002/58/EC

If the proposal only includes voluntary detection, SE argues that the exemption from Directive 2002/58/EC should be included in the CSAM Regulation, not remain as a separate regulation. The scope of the derogation should be similar to that of the temporary regulation, but the exact form of the derogation needs to be discussed further. However, SE would still prefer to keep the mandatory detection order in the regulation.

Use of technologies by providers

The proposal should be as technology-neutral as possible. SE would not like to exclude encrypted services from the scope of the regulation. At the same time, we would like to stress the importance of reducing the risks of undesirable effects on secure communication and cybersecurity within the EU.

SE welcomes the proposal that the COM makes an updated overview of technologies.

Reducing complexities and administrative burden

Any new proposals that may increase the administrative burden for companies need to be analysed in terms of impact, especially for SMEs.

The risk categories were introduced in order to strengthen the risk assessments and increase proportionality in relation to the mandatory detection order. If the mandatory detection order is deleted, the wording should be reviewed again in order to allow for simplification.

SE welcomes the proposal that the EU Centre should also promote measures to combat online abuse (Article 43(7)) and provide information on available technologies (Article 50). The Centre should also continue to be able to assess the remaining risk level (Article 43(1)(d)).

Review clause

SE sees positively on the proposal to include an evaluation clause.