Council of the European Union

Brussels, 13 March 2024
(OR. en)

7462/24

Interinstitutional File: 2022/0155(COD)

LIMITE

JAI 413
ENFOPOL 116
CRIMORG 43
IXIM 84
DATAPROTECT 128
CYBER 78
COPEN 126
FREMP 137
TELECOM 108
COMPET 279
MI 266
CONSOM 96
DIGIT 72
CODEC 704

NOTE

From:	Presidency
To:	Law Enforcement Working Party (Police)
No. prev. doc.:	6850/24
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – New approach suggested by the Presidency

With a view to the Law Enforcement Working Party (Police) meeting on 19 March 2024, delegations will find an explanatory note on the refined approach by the Presidency, Annex I with corresponding text proposals on Articles 1, 5, 5a, 7 and 10 of the above proposal, and Annex II with the risk categorisation table.

Explanatory note

During the LEWP meeting of 1 March 2024, the Presidency presented its new approach for the proposed Regulation laying down rules to prevent and combat child sexual abuse outlined in document 6850/24 and delegations discussed the specific questions included in that document. At the end of the meeting, the Presidency concluded that there was sufficient support to proceed with the further development of this new approach. In response to the request by some delegations for further explanations on certain parts of the new approach and taking into account the comments of the delegations (either expressed during the LEWP meeting or in writing), the Presidency further clarifies and develops its proposed approach in this explanatory note.

As set out in document 6850/24 and presented during the LEWP meeting of 1 March 2024, the proposed new approach is a combination of two interlinked building blocks: (1) more targeted detection orders, through enhanced risk assessment and risk categorisation and (2) protecting cyber security and encrypted data, while keeping services using end-to-end encryption within the scope of detection orders.

This note provides further details as well as adaptations to respond to the comments of some delegations on the first building block, divided into three main elements: (1) risk categorisation, (2) mitigation measures and (3) detection orders as possible consequences of that risk categorisation.

The Presidency has included concrete text proposals (see Annex I to this note) that reflect its proposed new approach as set out in document 6850/24 and further refined in this note. This explanatory note illustrates and explains these text proposals.

1) Risk categorisation

The Presidency suggests developing a methodology for determining the risk of specific services or parts or components thereof. The idea would be to establish three categories in which (parts or components of) services could be classified as high-risk, medium-risk, low-risk. This classification would be objectively defined following a specific procedure and based on a set of objective parameters (for example related to the type of service, the core architecture of the service, the provider's policies and safety by design functionalities and user tendencies). This process offers guidance to service providers how to self-assess the risks related to CSA on their services and provides a methodology and criteria to the Coordinating Authority to assess what kind of measures are needed to address these remaining risks. Depending on the category, the results will be different: A higher risk means a higher level of safeguards and a higher number of obligations for the providers.

The proposed procedure fits into the current procedure included in Articles 3-7 of the proposed regulation:

1. Risk assessment and "self-categorisation" by the service provider: This first step obliges the service providers to analyse their services in terms of risks related to CSA in line with Article 3, to take the necessary mitigation measures in line with Article 4 and to facilitate the risk categorisation by the Coordinating Authority using a template that would be part of the regulation as ANNEX I[1].

2. Reporting by the service provider: The service provider must report the result of the risk assessment, the mitigation measures, and the self-assessment to the Coordinating Authority. The Coordinating Authority is responsible for verifying the categorisation to ensure that the process has been followed and that no errors have been made. The Coordinating Authority can ask for additional information, explanations, or data to carry out its verification. The Coordinating Authority then validates the category proposed by the service provider or categorises the service in another category.

[1] In that regard, the presidency shared a working document (WK 3036/2024) and is still waiting for delegations' contributions.

At this stage, providers may indicate whether they have identified a risk in their service or a part or component thereof that might flag the possible need to receive a detection order (see more details below). This indication would not systematically trigger the issuance of a detection order. The decision to ask a judicial or independent administrative authority for the issuance of a detection order stays with the Coordinating Authority only.

The EU Centre would provide support to the Coordinating Authority as well as to the service providers. The involvement of the EU Centre throughout the risk assessment and mitigation procedure is already included in the text of the proposed regulation, and a specific reference to supporting the risk categorisation is added to Article 5. For example, the EU Centre could provide information or recommendations on the mitigation measures that could be implemented or offer to carry out sampling in order to draw certain trends from the data included in this service and match certain categorisation criteria.

3. Categorisation decision/ validation: The Coordinating Authority decides about the classification of the (part or component of the) service in one of the four categories. Depending on the category, different measures have to be taken by the provider (see below). The Coordinating Authority will inform as soon as possible the provider about its categorisation decision and the measures to be taken.

4. Recategorisation: Depending on the category allocated, the (part or component of the) service will need to be subjected to recategorisation, at least, after a certain period of time (See Annex II to this note). The regulation could provide a maximum term for each of the three categories in the current Article 3(4). For example:

   - High risk: up to 12 months
   - Medium risk: up to 24 months
   - Low risk: up to 36 months

   As these terms are maximum terms, the Coordinating Authorities would have the flexibility to determine the precise duration within the maximum time set. The Coordinating Authority could already inform the service provider of that term when issuing its categorisation decision. The Coordinating Authority can launch the recategorisation procedure at any time (for example when it learns about CSA on a service through flagging).

2) Additional mitigation measures

While all providers are obliged to carry out the mitigation measures outlined in Article 4, depending on the category the service is classified in, different types of tailored (depending on the specifics of the service) additional mitigation measures apply in accordance with the amended Article 5a, including consequences in case of non-compliance:

- High-risk and medium-risk services: obligatory additional mitigation measures. When issuing the categorization decision to the provider, the Coordinating Authority will justify the reasons why it requested the provider to apply additional mitigation measures. Non-compliance will result in penalties based on Article 35 of the regulation. The penalties imposed for high-risk services would be stricter and more severe than for medium-risk services;

- Low risk services: recommended additional mitigation measures to help the provider identify possible improvements for its service. No penalties for non-compliance. However, the Coordinating Authority can, at any time, ask the provider to launch a recategorisation procedure possibly resulting in the imposition of obligatory mitigation measures if the service would be recategorized as a high-risk or medium-risk service.

3) Detection Orders

Taking into account the comments from delegations, the Presidency proposes to subject only high-risk services (or parts or components thereof) to detection orders as a measure of last resort if the additional mitigation measures do not address the high risk identified in an effective way. The Coordinating Authority will have the discretion to tailor the detection order to the specific risks identified during the risk assessment/categorisation. The Coordinating Authority must, however, always aim for the least intrusive type of detection. Criteria that could be used for such tailoring and would be verified by the competent authorities issuing the detection order upon the request of a Coordinating Authority include:

- the period of application of the detection order;
- the technologies used;
- the impact on the protection of inter-personal communication;
- the possibility to limit the scope to parts or components of a service;
- other safeguards provided for in accordance with Art. 7(8)

(a) "Users of interest" based reporting

The risk categorisation allows for more targeted, and therefore non-indiscriminate, detection as only (parts or components of) services identified as high risk will be subjected to tailored detection orders. A further possible way to target the reporting is to only allow the report based on detection to be limited to certain users of interest.

A user of interest could be defined as a user who has already been flagged as potential sender or recipient of child sexual abuse material or grooming attempts. This would be automatically detected but not known to anyone (including the provider), until a certain number of hits in the users' accounts is reached on the sharing of possible CSAM or attempted grooming. This can be broken down into two phases:

Phase 1: determination of the user of interest

The provider having received a detection order for known CSAM, new CSAM and/or grooming would put in place the necessary mechanisms to detect the 'interest', i.e. hits with possible known CSAM/new CSAM and/or grooming, with the following conditions:

- The possible hit would be detected automatically, and it would not be reported.
- Therefore, no one, including the provider, would be aware of that hit.
- The only information extracted from that data processing would be whether a possible hit linked to that user has taken place. This information would be automatically recorded on the user's account, e.g. via a flag, and it would not be available to anyone, not even the provider.
- This would mitigate the concern of intrusion of privacy by the provider or anybody else on users that are not linked to any child sexual abuse activity.

In the case of adult users, a 'user of interest' would be a user for which hits have been automatically identified (and without anyone being aware) for a number of times depending on the type of CSA online, taking into account the different accuracy rates: for known CSAM: 1 time and for new CSAM and grooming: 2 times.

In the case of child users:

- When a possible hit of known, new material or grooming is detected, the child would be automatically and immediately warned of the possible known, new material or grooming, without the provider knowing. The child would be given the opportunity to report to the provider, which only then would know about the possible known, new CSAM or grooming.

Phase 2: reporting to the EU Centre only of users of interest.

The provider would only become aware of the possible CSA once the user is identified as a user of interest, taking into account the above (or if the child decides to report, in the case of child accounts). Only users of interest would be reported to the EU Centre. The error rate for new CSAM and grooming would be significantly reduced by applying this additional step[2].

(b) Flagging of possible need to receive a detection order

Considering the feedback from delegations, the Presidency proposes granting high-risk service providers the ability to notify the Coordinating Authority about a risk identified by them related to their service or a part or component thereof that might require the issuing of a detection order. This notification could be included in the report submitted to the Coordinating Authority. Only high-risk services would be allowed to make this notification. This provision could be explicitly outlined in Article 5 of the text.

[2] E.g. for an error rate of 99.9%, i.e. 1 in 1000 files flagged as possible CSAM are not CSAM, the probability that a hit reported to the EU Centre is not CSAM would be 1/1000 x 1/1000 x 1/1000 = 1/1 000 000 000, i.e. 1 in a billion.

To clarify the intention behind this provision, a recital could be drafted to specify that the act of notifying the Coordinating Authority does not automatically lead to the request of issuance (and therefore much less to the automatic issuance) of a detection order. The decision to request a detection order from a judicial or an independent administrative authority remains solely with the Coordinating Authority.

It needs to be underlined that this notification mechanism would not lead to circumventing any mitigation measures. The intention behind allowing providers to flag their services for potential detection orders is to enhance transparency and collaboration within the regulatory framework, ensuring that appropriate measures are taken in accordance with the risk level of each service.

(c) Cybersecurity safeguards

Taking into account the comments from delegations received so far, the Presidency proposes a reinforcement of the safeguards related to cybersecurity concerning the execution of the detection orders. These new provisions could be added to Article 10(3) and (4) as part of the requirements that the technologies must fulfil when deployed to execute the detection orders. These requirements would include in particular a dedicated assessment by the provider of the cybersecurity risks and the cybersecurity risk mitigation measures taken. The EU Centre would be required to provide an opinion on such security risk assessment and mitigation measures.

In addition to the new provisions in Article 10(3) and (4) concerning the deployment of the technologies to execute the detection orders, the providers would be required to use certified technologies for the execution of the detection orders.

Just as it is necessary to add cybersecurity aspects, it is also important to be able to remain technologically neutral and future proof, while still giving clear indications to service providers on how to protect their technologies but at the same time allow them to achieve the objectives underlying this regulation.

With this in mind, it seems appropriate to adopt an approach focused on the risks and dangers that a solution may cause, by considering the corresponding technologies with which we are already familiar, and addressing the fears and dangers associated with them.

To carry out this exercise, the presidency expects to receive technical information from delegations on any concerns they may have regarding the relevant detection technologies. By listing these concerns, it will be possible to include additional safeguards on technical aspects into a recital or the operative part.

Similarly, we would also need consider the exact role of the EU-Centre and how it should intervene, considering the technology verification, analysis, and validation process. We also need to take into account the responsibilities and tasks of other EU agencies with cybersecurity responsibilities, and the potential cooperation of the EU-Centre with these EU agencies.

ANNEX I

Proposal for a Regulation laying down rules to prevent and combat child sexual abuse:

Text proposals for examination by LEWP on 19 March 2024[1]

Article 1

Subject matter and scope

1. This Regulation lays down uniform rules to **prevent and combat** ~~address~~ **in a targeted, carefully balanced and proportionate manner** the ~~mis~~use of relevant information society services for online child sexual abuse in the internal market.

   It establishes, in particular:

   (a) obligations on providers of relevant information society services to minimise the risk that their services are ~~mis~~used for online child sexual abuse;

   (b) obligations on providers of hosting services and providers of interpersonal communication**s** services to detect and report online child sexual abuse;

   (c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;

   (d) obligations on providers of internet access services to **prevent users from accessing** ~~access~~ child sexual abuse material;

   (da) obligations on providers of online search engines to delist websites indicating specific items of child sexual abuse;

   (e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member States, the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre') and cooperation and transparency.

2. This Regulation shall apply to providers of relevant information society services offering such services in the Union, irrespective of their place of main establishment.

~~**2a. This Regulation shall not apply to services or parts of the services used by the State for national security purposes, maintaining law and order or military purposes.**~~

~~**2b. The Regulation shall not apply to classified information and information and communication systems processing such information.**~~

---

1 Changes to the Commission proposal are marked in **bold** and ~~strikethrough~~. New changes to the Commission proposal in comparison to document 12611/23 are marked in **bold underline** and ~~strikethrough underline~~.

3. This Regulation shall not affect the rules laid down by the following legal acts:

(a) Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;

(b) Directive 2000/31/EC and Regulation (EU) **2022/2065** ~~…/… of the European Parliament and of the Council~~[2] [~~*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*~~];

(ba) Regulation (EU) 2022/… of … on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act);

(c) Directive 2010/13/EU;

(d) Regulation (EU) 2016/679, Directive 2016/680, Regulation (EU) 2018/1725, and, subject to paragraph 4 of this Article, Directive 2002/58/EC;

(e) Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

3a. This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and shall apply without prejudice to fundamental principles relating to the right for respect to private life and family life and to freedom of expression and information.[3]

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

~~**4a. This Regulation shall not lead to any general obligation to monitor the information which providers of hosting services transmit or store, nor to actively seek facts or circumstances indicating illegal activity.**~~

~~**5. 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 to decrypt data.**~~

---

2 Regulation (EU) ~~…/…~~ **2022/2065** of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (OJ L ….).

3 Wording copied from Art. 1(4) of TCO Regulation with an additional reference to the right to private life.

5. This Regulation shall not require a provider of hosting services or a provider of interpersonal communications services or a user to introduce systemic cybersecurity risks for which it is not possible to take any effective measures to mitigate such risks. This Regulation shall not create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to create access to end-to-end encrypted data.

Article 5

*Risk reporting **and categorisation***

1. Providers of hosting services and providers of interpersonal communications services shall transmit, by three months from the date referred to in Article 3(4), to the Coordinating Authority of establishment a report ~~specifying~~ **including** the following:

(a) the **premise for the risk assessment pursuant to Article 3(2), the** process and the results of the risk assessment conducted or updated pursuant to Article 3, including the assessment of any potential remaining risk referred to in Article 3(5);

(b) any mitigation measures taken pursuant to Article 4 **and, where applicable, Article 5a, Aand the results thereof including the effectiveness of these measures and how they comply with the requirements of Article 4(2), and in case of age assessment and verification measures, how they comply with the requirements of Article 4 (3);**

(ba) any other mitigation measures implemented before carrying out the risk assessment and, when available, complementary informations about the effectiveness of these measures;

~~**(bb) the effectiveness of these measures and how they comply with the requirements of Article 4 (2);**~~

(c) where potential remaining risk as referred to in Article 3(5) is identified, any available information relevant for identifying as precisely as possible the parts or components of the service, or the specific users or groups or types of users, in respect of which the potential remaining risk arises ~~and the planned further measures to mitigate this risk~~.

(ca) a self-assessment against the criteria established for the categorisation of risks of the service or the parts or components of the service, following the template laid down in ANNEX XIV;

(cb) whether a high risk concerning the service or the parts or components of the service is identified that might require the issuing of a detection order in accordance with Article 7(4);

(d) whether the provider ~~intends to~~ requests to the Coordinating Authority of establishment the authorisation to display the sign of ~~compliance~~ reduced risk as referred to ~~in accordance with~~ in Article 5b.

~~**(d) any other relevant measures taken to mitigate the risk and the results thereof.**~~

~~**When made available,** **t~~**This report ~~**should**~~ **shall include available statistical information to support and illustrate the development and effectiveness of mitigation measures.**

2. Within three months after receiving the report, the Coordinating Authority of establishment shall assess it and determine, on that basis and taking into account any other relevant information available to it, whether the risk assessment has been ~~**properly**~~ **diligently** carried out or updated and the mitigation measures have been taken in accordance with the requirements of Articles 3 and 4 **and evaluate the level of the remaining risk**.

Based on the evaluation of the level of the remaining risk and taking into account the self-assessment carried out by the providers of hosting services and providers of interpersonal communications against the criteria established for the categorisation of risks, the Coordinating Authority of establishment shall determine the risk category allocated to the service or the parts or components of the service, following the methodology and criteria outlined in ANNEX XV.

The service or the parts or components of the service shall be classified into the following categories:

(a) High risk;
(b) Medium risk
(c) Low risk

The decision of the Coordinating Authority of establishment determining the risk category shall be communicated to the providers concerned, including the date by when the provider is required to update the risk assessment.

The Coordinating Authority of establishment may request the EU Centre to assist in evaluating the mitigation measures taken by the provider, ~~as well as~~ evaluating the level of the remaining risk and in determining the risk category allocated to the service or the parts or components of the service.

If the provider has submitted the request referred to in point (d) of paragraph 1, the Coordinating Authority shall decide on the issuance of the authorisation to display the sign of ~~compliance~~ reduced risk in accordance to Article 5b.

The Commission shall be empowered to adopt delegated acts in accordance with Article to amend Annex XIV in order to revise and update the criteria laid down therein, and to amend ANNEX XV in order to revise the methodology and criteria laid down therein, if required in particular due to technological developments.

3. Where necessary for that assessment, that Coordinating Authority may require further information from the provider, within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than two weeks.

The time period referred to in ~~the first subparagraph~~ **paragraph 2 ~~of this Article~~** shall be suspended until that additional information is provided.

~~4. Without prejudice to Articles 7 and 27 to 29, where the requirements of Articles 3 and 4 have not been met, that Coordinating Authority shall require the provider to re-conduct or update the risk assessment or to introduce, **implement,** review, discontinue or expand, as applicable, the mitigation measures, within a reasonable time period set by that Coordinating Authority. That time period shall not be longer than one month. **The provisions of this Article shall also apply to risk assessments re-conducted or updated pursuant to this paragraph.**~~

~~**4a. If the Coordination Authority of establishement, after carrying out the assessments referred to in paragraphs 1 to 4, determines that the risk assessment has been satisfactorily carried out and that no further mitigation measures can be introduced, implemented, reviewed, discontinued or expanded, that Coordinating Authority shall authorise within one week the providers to display a distinctive and universal sign attesting to the optimised safety aspects of the assessed service, in accordance to article 6a.**~~

~~4~~ 5. Providers shall, when transmitting the report to the Coordinating Authority of establishment in accordance with paragraph 1, transmit the report also to the EU Centre.

5.~~6.~~ Providers shall, upon request, transmit the report to the providers of software application stores, insofar as necessary for the assessment referred to in Article 6(2). Where necessary, they may remove confidential information from the reports.

Article 5a

Adjusted or additional risk assessment or risk mitigation measures

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 ~~and~~ or 4 ~~have not been met~~, it shall require the provider of hosting services or the provider of interpersonal communications services to carry out one or several of the following actions, as appropriate:

(a) to re-conduct or update the risk assessment in accordance with Article 3, including where appropriate by modifying the methodology used to conduct the risk assessment, and report thereon in accordance with Article 5;

(b) to implement, review, modify, discontinue or expand some or all of the risk mitigation measures taken in accordance with Article 4;

(c) to introduce additional risk mitigation measures in accordance with Article 4.

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

2. **~~The~~ A provider that is required to perform the actions specified in points (b) or (c) of paragraph 1 shall re-conduct or update the risk assessment in accordance with Article 3 so as to take account of those actions, and report thereon in accordance with Article 5. In the report on the re-conducted or updated risk assessment the provider shall also specify and explain ~~inform the Coordinating Authority of~~ the actions performed ~~steps~~ taken ~~to ensure compliance with the measures required~~ pursuant to paragraph 1, within a time period set by the Coordinating Authority. That time period shall be reasonable, taking into account the complexity of the required actions measures.**

3. The Coordinating Authority of establishment shall, by deviation from the time periods specified in Articles 3(4) and 5(1), set a reasonable time period for the performance of the actions pursuant to paragraph 1 and for the reporting pursuant to paragraph 2. That time period shall be reasonable, taking into account the complexity of the required actions.

4. The Coordinating Authority of establishment may recommend to a provider offering a service or parts or components of a service classified as low risk to carry out one or several of the actions listed in paragraph 1, as appropriate.

Section 2
Detection obligations

Article 7

Issuance of detection orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 **for the sole purpose of** ~~to~~ detect**ing** the dissemination of online child sexual abuse on a specific service **or parts or components of the service, classified as high risk in accordance with Article 5(2), for a limited period of time as specified in paragraph 9**.

2. The Coordinating Authority of establishment shall, before requesting the issuance of a detection order, carry out the investigations and assessments necessary to determine whether the conditions of paragraph 4 have been met.

To that end, it may~~, where appropriate,~~ require the provider to submit the necessary information, additional to the report and the further information referred to in Article 5(1) and (3), **and Article 5a(2),** respectively, within a reasonable time period set by that Coordinating Authority, or request the EU Centre, another public authority or relevant experts or entities to provide the necessary additional information. **It may also request the assistance of the EU Centre to conduct tests in accordance with Article 47a on the service in question to verify whether there are objective indications, as referred to in point (a) of paragraphs 5, 6 or 7, as applicable.**

3. Where the Coordinating Authority of establishment takes the preliminary view that the conditions of paragraph 4 have been met, it shall:

(a) establish a draft request for the issuance of a detection order, specifying the main elements of the content of the detection order it intends to request and the reasons **including the necessity** for requesting it;

(b) submit the draft request to the provider and the EU Centre;

(c) afford the provider an opportunity to comment on the draft request, within a reasonable time period set by that Coordinating Authority;

(d) invite the EU Centre to provide its opinion on the draft request, within a time period of four weeks from the date of receiving the draft request.

Where, having regard to the comments of the provider and the opinion of the EU Centre, that Coordinating Authority continues to be of the view that the conditions of paragraph 4 have met, it shall re-submit the draft request, adjusted where appropriate, to the provider. In that case, the provider shall do all of the following, within a reasonable time period set by that Coordinating Authority:

(a) draft an implementation plan setting out the measures it envisages taking to execute the intended detection order, including detailed information regarding the envisaged technologies and safeguards;

(b) where the draft implementation plan concerns an intended detection order concerning the solicitation of children other than the renewal of a previously issued detection order without any substantive changes, conduct a data protection impact assessment and a prior consultation procedure as referred to in Articles 35 and 36 of Regulation (EU) 2016/679, respectively, in relation to the measures set out in the implementation plan;

(c) where point (b) applies, or where the conditions of Articles 35 and 36 of Regulation (EU) 2016/679 are met, adjust the draft implementation plan, where necessary in view of the outcome of the data protection impact assessment and in order to take into account the opinion of the data protection authority provided in response to the prior consultation;

(d) submit to that Coordinating Authority the implementation plan, where applicable attaching the opinion of the competent data protection authority and specifying how the implementation plan has been adjusted in view of the outcome of the data protection impact assessment and of that opinion.

Where, having regard to the implementation plan of the provider and the **received** opinion**s** of the data protection authority **and the EU Centre, where applicable**, that Coordinating Authority continues to be of the view that the conditions of paragraph 4 have met, it shall submit the request for the issuance of the detection **order**, adjusted where appropriate, to the competent judicial authority or independent administrative authority. It shall attach the implementation plan of the provider and the opinions of the EU Centre and the data protection authority to that request **and, when appropriate, the reasons for diverging from the opinions received**.

4. The Coordinating Authority of establishment shall request the issuance of the detection order, and the competent judicial authority or independent administrative authority **may** ~~shall~~ issue the detection order where it considers that the following conditions are met:

(a) there is evidence of a significant and present or foreseeable risk of the **high risk** service **or parts or components of the service** being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable;

(b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties.

When assessing whether the conditions of the first subparagraph have been met, account shall be taken of all relevant facts and circumstances of the case at hand, in particular:

(a) the risk assessment conducted or updated and any mitigation measures taken by the provider pursuant to Articles 3 and 4, including any mitigation measures introduced, reviewed, discontinued or expanded pursuant to Article **5a** ~~5(4)~~ where applicable;

(b) any additional information obtained pursuant to paragraph 2 or any other relevant information available to it, in particular regarding the use, design and operation of the service, regarding the provider's financial and technological capabilities and size and regarding the potential consequences of the measures to be taken to execute the detection order for all other parties affected;

(c) the views and the implementation plan of the provider submitted in accordance with paragraph 3;

(ca) the necessity and proportionality in terms of the period of application, the technologies used, and the impact on the protection of inter-personal communication, the possibility to limit the scope to parts or components of a service and other safeguards provided for in accordance with paragraph 8;

(d) the opinions of the EU Centre and of the data protection authority submitted in accordance with paragraph 3.

As regards the second subparagraph, point (d), where that Coordinating Authority substantially deviates from the opinion**s received** of the EU Centre, it shall inform the EU Centre and the Commission thereof, specifying the points at which it deviated and the main reasons for the deviation.

5. As regards detection orders concerning the dissemination of known child sexual abuse material, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

(a) ~~it is likely,~~ **there are objective indications that,** despite any mitigation measures that the provider may have taken or will take, ~~**that there is a genuine and present or foreseeable risk**~~, ~~that~~ the service **or parts or components of the service** is **or will be** used, to an appreciable extent for the dissemination of known child sexual abuse material**;**

(b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent for the dissemination of known child sexual abuse material.

6. As regards detection orders concerning the dissemination of new child sexual abuse material, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

(a) ~~it is likely~~, **there are objective indications that,** despite any mitigation measures that the provider may have **has** taken or will take, ~~**that there is a genuine and present or foreseeable risk**~~ ~~that~~ the service **or parts or components of the service** is **or will be** used, to an appreciable extent for the dissemination of new child sexual abuse material;

(b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent, for the dissemination of new child sexual abuse material;

(c) for services other than those enabling the live transmission of pornographic performances as defined in Article 2, point (e), of Directive 2011/93/EU:

(1) a detection order concerning the dissemination of known child sexual abuse material has been issued in respect of the service;

(2) the provider submitted a significant number of reports concerning known child sexual abuse material, detected through the measures taken to execute the detection order referred to in point (1), pursuant to Article 12.

7. As regards detection orders concerning the solicitation of children, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

(a) the provider qualifies as a provider of interpersonal communication**s** services ~~**excluding such services consisting of real-time audio communications**~~;

(b) ~~it is likely~~, **there are objective indications <u>that,</u>** despite any mitigation measures that the provider may have **has** taken or will take, ~~**that there is a genuine and present or foreseeable risk** that~~ the service **<u>or parts or components of the service</u>** is **or will be** used, to an appreciable extent for the solicitation of children;

(c) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent, for the solicitation of children.

The detection orders concerning the solicitation of children shall apply only to interpersonal communications where one of the users is a child ~~user~~ **and shall not apply to calls**.

8. The Coordinating Authority of establishment when requesting the issuance of detection orders, and the competent judicial or independent administrative authority when issuing the detection order, shall target and specify it in such a manner that the negative consequences referred to in paragraph 4, first subparagraph, point (b), remain limited to what is strictly necessary to effectively address the significant risk referred to in point (a) thereof.

To that aim, they shall take into account all relevant parameters, including the availability of sufficiently reliable detection technologies in that they limit to the maximum extent possible the rate of errors regarding the detection and their suitability and effectiveness for achieving the objectives of this Regulation, as well as the impact of the measures on the rights of the users affected, and require the taking of the least intrusive measures, in accordance with Article 10, from among several equally effective measures.

In particular, they shall ensure that:

(a) where that risk is limited to an identifiable part or component of a service, the required measures are only applied in respect of that part or component;

(b) where necessary, in particular to limit such negative consequences, effective and proportionate safeguards additional to those listed in Article 10(4), (5) and (6) are provided for;

(c) subject to paragraph 9, the period of application remains limited to what is strictly necessary.

9. The competent judicial authority or independent administrative authority shall specify in the detection order the period during which it applies, indicating the start date and the end date.

The start date shall be set taking into account the time reasonably required for the provider to take the necessary measures to prepare the execution of the detection order. It shall not be earlier than three months from the date at which the provider received the detection order and not be later than 12 months from that date.

The period of application of detection orders concerning the dissemination of known or new child sexual abuse material shall not exceed 24 months and that of detection orders concerning the solicitation of children shall not exceed 12 months.

10. A detection order shall not create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to create access to end-to-end encrypted data.

11. **Providers of hosting services and providers of interpersonal communications services shall carry out the detection orders in a way that only users of interest detected repeatedly on the sharing of potential child sexual abuse material or attempts to solicate children are reported in accordance with Articles 12 and 13.**

The detection of potential child sexual abuse material or attempts to solicitate children shall result in a hit to be flagged in the users' accounts of the affected service without the provider being notified. A child using the service shall be automatically and immediately warned of detected potential child sexual abuse material or attempts to solicate children, without the provider being notified. The child shall be enabled to notify the provider thereof through tools that are easily accessible and age-appropriate.

Users on whose accounts hits related to known child sexual abuse material have been flagged once, and users on whose accounts hits related to potential new child sexual abuse material or attempts to solication of children have been flagged twice, shall be considered as users of interest.

Article 10

Technologies and safeguards

1. Providers of hosting services and providers of interpersonal communication**s** services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.

2. The provider shall be entitled to acquire, install and operate, free of charge, technologies made available by the EU Centre in accordance with Article 50(1), for the sole purpose of executing the detection order.

~~The provider shall not be required to use any specific technology, including those made available by the EU Centre, as long as the requirements set out in this Article are met.~~ The use of the technologies **referred to in paragraph 1** ~~made available~~ **approved** by the EU Centre shall not affect the responsibility of the provider to comply with ~~those~~ **the** requirements **set out in this Article** and for any decisions it may take in connection to or as a result of the use of the technologies.

3. The technologies shall ~~be~~:

(a) **be** effective **and suitable** ~~**and not easily circumvented**~~ in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;

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

(b) not be able to **deduce the substance of the content of the communications nor to** extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;

(c) **be** in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and to protection of personal data;

(d) **be** ~~sufficiently~~ reliable **and accurate**, in that they limit to the maximum extent possible the rate of errors regarding the detection **and, where such errors occur, do not prevent** ~~**facilitate**~~ **the rectification of the consequences without undue delay**.

4. The provider shall:

(a) take all the necessary measures to ensure that the technologies and indicators, as well as the processing of personal data and other data in connection thereto, are used for the sole purpose of detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, insofar as strictly necessary to execute the detection orders addressed to them. **In particular, the provider shall:**

(i) diligently identify, analyse and assess any systemic cybersecurity risks that could be introduced by the technologies used for the execution of the detection orders;

(ii) take all reasonable mitigation measures, tailored to the possible systemic cyberscurity risk identified, to minimise that risk;

(b) establish effective internal procedures to prevent and, where necessary, detect and remedy any misuse**, including misuses caused by breaching cybersecurity measures,** of the technologies, indicators and personal data and other data referred to in point (a), and unauthorized access to, and unauthorised transfers of, such personal data and other data;

(c) ensure regular human oversight as necessary to ensure that the technologies operate in a sufficiently reliable manner **and, where necessary, in particular when potential errors and potential solicitation of children are detected, human intervention**;

(d) establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it, within a reasonable timeframe, complaints about alleged infringements of its obligations under this Section, as well as any decisions that the provider may have taken in relation to the use of the technologies, including the removal or disabling of access to material provided by users, blocking the users' accounts or suspending or terminating the provision of the service to the users, and process such complaints in an objective, effective and timely manner;

(e) inform the Coordinating Authority, at the latest one month before the start date specified in the detection order, on the implementation of the envisaged measures set out in the implementation plan referred to in Article 7(3);

(f) regularly review the functioning of the measures referred to in points (a), (b), (c) and (d) of this paragraph and adjust them where necessary to ensure that the requirements set out therein are met, as well as document the review process and the outcomes thereof and include that information in the report referred to in Article 9(3).

5. The provider shall inform users in a clear, prominent and comprehensible way of the following:

(a) the fact that it operates **~~automated~~** technologies **~~(automated profiling)~~** to detect online child sexual abuse**,** to execute the detection order, the ways in which it operates those technologies, **meaningful information about the logic involved**, and the impact on the confidentiality of users' communications;

(b) the fact that it is required to report potential online child sexual abuse to the EU Centre in accordance with Article 12;

(c) the users' right of judicial redress referred to in Article 9(1) and their rights to submit complaints to the provider through the mechanism referred to in paragraph 4, point (d) and to the Coordinating Authority in accordance with Article 34.

~~(d) the users' rights as data subjects under Regulation (EU) 2016/679.~~

The provider shall not provide information to users that may reduce the effectiveness of the measures to execute the detection order.

6. Where a provider detects potential online child sexual abuse through the measures taken to execute the detection order, it shall inform the users concerned without undue delay, after ~~Europol or~~ the national law enforcement authority of a Member State that received the report pursuant to Article 48 has confirmed that the information to the users would not interfere with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

ANNEX II

Risk categorisation table

RISK CATEGORISATION	LEVEL OF DETECTION ORDER (DO)	MITIGATION MEASURE(S) (MM)	PROVIDER FLAGGING NEED FOR DETECTION ORDER	FREQUENCY OF (RE)CATEGORISATION
Risk + + High	**DO** - Including services using E2EE - "Users of interest" based reporting	Obligatory additional MM Sanction(s) ++	Flagging, by the provider, of possible need to be subject to a detection order	Up to 12 months
Risk + Medium	None	Obligatory additional MM Sanction(s) +	None	Up to 24 months
Risk - Low	None	Recommended additional MM	None	Up to 36 months