Council of the European Union

Brussels, 26 May 2026
(OR. en)

9659/26

Interinstitutional File:
2022/0155 (COD)

LIMITE

ENFOPOL 187
JAI 655
CRIMORG 117
IXIM 119
DATAPROTECT 171
CYBER 249
COPEN 198
FREMP 188
TELECOM 262
COMPET 617
MI 523
CONSOM 174
DIGIT 141
CODEC 994

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - Presidency compromise texts on detection

The Presidency has prepared a compromise proposal in the annex to this note concerning the detection of online child sexual abuse which follows-on from the previous presentations by the Cyprus Presidency to JHA Counsellors and the suggestion by the Commission during the third trilogue on 16 April 2026 to establish separate regimes for detection/searches in public and non-public content.

The proposal incorporates elements from the mandates[1] of both the Council and the European Parliament (EP) and consists of the following components:

- a definition of 'content that is publicly accessible';
- own-initiative searches by providers in content that is not publicly accessible[2];
- detection orders for specific users in both publicly accessible and not publicly accessible content;
- own-initiative searches by the EU Centre in publicly accessible content; and
- common provisions applicable to both publicly accessible and not publicly accessible content.

Although the first three components are modular and not all of them might need to be included in the final legislation, the Presidency considers that their combined application would constitute a balanced solution and could facilitate reaching political agreement.

The Presidency invites delegations to examine the compromise texts and to provide their feedback to the issues stressed in this note at the meeting of JHA counsellors planned to take place on 10 June 2026.

---

1 The Council mandate foresees own-initiative searches by providers of number-independent interpersonal communications services for known and new CSAM as well as solicitation of children. In turn, the EP position provides for detection orders for known and new CSAM, issued by judicial authorities to providers of hosting services or number-independent interpersonal communications services and *"limited to individual users, a specific group of users, either as such or as subscribers to a specific channel of communication, in respect of whom there are reasonable grounds of suspicion for a link, even an indirect one, with child sexual abuse material".* The EP mandate also includes own-initiative searches by the EU Centre for known CSAM in public content.

2 The Presidency did not consider it necessary to make specific provisions for own-initiative scanning by providers on public content to mitigate the risk of online child sexual abuse on their service since there is no limitation to this under existing rules.

A. Scope of the detection/searches

The scope of application of the different components, i.e. whether they would apply to known child sexual abuse material (CSAM), new CSAM and/or grooming, remains bracketed[3] in this draft text because it remains subject to discussions. *Delegations are invited to indicate their flexibility concerning the appropriate scope of application for each of the components.*

B. Definitions

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

As regards non-public content, the Presidency proposes that all content that is not covered by the definition of 'content that is publicly accessible' and that is not encrypted[4] would fall into this category. Consequently, no definition is provided therefor.

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

---

3 Under Article 2 of the CSAR proposal, the term 'online child sexual abuse' refers to the dissemination of child sexual abuse material and the solicitation of children. CSAM means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e) of Directive 2011/93/EU. In principle, child sexual abuse material would cover both known and new CSAM, but it would not cover solicitation of children.

4 The co-legislators have provisionally agreed to include the following paragraph 4a in Article 1, which excludes encrypted content from the scope of the CSA Regulation and therefore does not allow own-initiative searches or detection orders for encrypted content: *"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."*

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

The text effectively reflects the provisions and safeguards of the CSA Interim Regulation[5], providing for a permanent derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC ('ePrivacy') for number-independent interpersonal communications services, in line with the Council mandate.

Since 'content that is not publicly accessible' extends beyond content shared in interpersonal communications, e.g. content stored in clouds, hosting service providers should also be allowed to conduct own-initiative searches on non-public content. Although no derogation from ePrivacy needs to be provided for hosting service providers because they do not fall within the scope of the abovementioned Directive, it is proposed to apply in analogy the same rules and safeguards as for providers of number-independent interpersonal communications services.

The reporting obligations on providers are proposed as part of Articles 83 and 84 of this Regulation and additional safeguards are proposed in Article Z and Article Z+1: –(a)that providers would have to inform the EU Centre in advance of conducting own-initiative searches, and (b) national authorities would be able to suspend any own—initiative search activities by providers if they consider that the conditions of the Regulation are not met. Technology safeguards reflecting the relevant provisions of the CSA Interim Regulation are included in Article 10.

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

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

[5] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

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

The compromise proposal includes a new provision for public content detection orders. Public content detection orders could be issued by a national authority if a hosting service (or part of the service) is being misused for online child sexual abuse to an appreciable extent. There is no reference to any residual risk, since the order can be issued if there is content online, something that can be verified by national authorities. The order would contain the period of application, the information necessary for the provider to be able to execute the order and information regarding appeals. There is also a clarification that these provisions should not lead to a general monitoring obligation.

At the moment, the type of authority issuing the order is left open but, in line with its mandate on detection orders, the EP might insist on a judicial decision.

Given the limited interference of detection orders for public content with fundamental rights, the procedure for issuing these orders is less detailed than the procedure for detection orders on non-public content (see below). In particular, there is no reference to a draft implementation plan being prepared by the provider. Whether or not the procedures for the public content detection order and the non-public content detection order should be aligned largely, depends also on whether there would be a difference in the type of issuing authority.

Delegations are invited to provide feedback on the following:

(a) The conditions for issuing the order under Article X;
(b) The appropriate authority to issue the order, and whether there could be flexibility on this point, including on whether there might be scope to reach a compromise by having independent administrative authorities (in addition to judicial authorities) issuing these orders;
(c) any additional feedback on the suggested wording of Articles X and X+1.

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

The compromise text includes a provision for non-public content detection orders. The proposal is to move away from generalised scanning towards scanning of specific users, without a need for these users to be suspects in the criminal law sense, however, since the primary purpose of detection orders is to identify online child sexual abuse, which may or may not be used in criminal investigations after its verification.

To make it clear that detection orders do not interfere with criminal investigations by law enforcement, it is proposed to add a provision in Article 1 to specify that the CSA Regulation is without prejudice to Union law in the field of cooperation in civil and criminal matters and national law in civil and criminal matters.

Detection orders on non-public content should be issued by national authorities concerning specific users when there are clear indications, based on lawfully acquired information, that these users are related to the dissemination of child sexual abuse material or to the solicitation of children and that they have used the service in the past 12 months for online child sexual abuse. A detection order would only be issued if necessary and proportionate. Examples of "clear indications" should be specified in a recital and could inter alia be based on reports from users submitted directly to providers or hotlines, reports to national authorities, own-initiative searches by providers reported to the EU Centre or patterns of activities online.

The process for issuing non-public content detection orders would be as follows: The Coordinating Authority would send a draft request to the provider indicating the reasons for the order, the users in question, the EU Centre indicators to be used and the duration of the order. The provider would then submit comments within an appropriate period and a draft implementation plan. The EU Centre would also receive the draft request and be provided with a period to comment.

After hearing the provider, if it continues to consider that the requirements for a detection order are met, the Coordinating Authority could request the issuance of the order to a judicial/independent administrative authority of its Member State that should then issue the order if it considers that the conditions of the provision are met. The orders would contain the period of application (max. 24 months for CSAM/12 months for grooming), the information necessary for the provider to be able to execute the order and information on appeals.

As regards the types of authorities involved in the issuing of non-public detection orders, the Presidency sees merit in leaving it to independent administrative authorities and/or judicial authorities to issue these orders given the level of interference with the fundamental rights of the users concerned. When it comes to launching the procedure, the Coordinating Authority would be best-placed to assess – based on the information it receives from the provider, the EU Centre and the different competent authorities - whether a detection order is appropriate. It is left for further discussion whether all Coordinating Authorities or only the Coordinating Authorities of establishment of the provider should have the right to request a detection order for non-public content.

Delegations are invited to provide feedback on the following:

(a) the types of authorities involved in the issuing of the detection order for non-public content and whether such orders could be issued by all Member States or only by the Member State in which the provider is established;
(b) the text proposed for the detection order;
(c) the scope of material (known, new CSAM and/or grooming), of the users concerned and how this scope might interact with own-initiative detection, for example: would it be appropriate/necessary to allow own-initiative detection by providers, while in parallel having a detection order regime that has more restrictive conditions?
(d) any additional feedback on the suggested wording.

F. Searches by the EU Centre – Article 49

The text builds on the EP amendments in Article 49, providing for the EU Centre to conduct own-initiative searches for child sexual abuse on content that is publicly accessible and inform the provider of its findings, unless otherwise requested by the competent law enforcement authority of the Member State concerned to avoid interference with activities for prevention, detection, investigation and prosecution of criminal offences.

The reports resulting from own-initiative searches by the EU Centre should be treated by the provider in the same way as reports from the public, meaning that the provider would be obliged report it back to the EU Centre in accordance with Article 12 and 13 of this Regulation and, potentially, remove the reported content or disable access to it where it finds it to be incompatible with its own terms and conditions. The EU Centre would then be required to forward the report from the provider to the competent authorities for their assessment and possible launch of a criminal investigation and to Europol. The rationale for including this component is therefore not to complement or replace the work of law enforcement, but to facilitate it.

The Presidency requests feedback from delegations on the following:

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

G. Common provisions

Article 9 concerns redress, information, reporting and the modification of orders. It is suggested that the rules apply commonly to both public and non-public content detection orders.

Article 10 concerns technologies and safeguards **both for own-initiative searches** by providers **and detection orders** (both in public and in non-public content). The intention is to mirror the technology safeguards in the CSA Interim Regulation for own-initiative searches as much as possible.

The relevant text concerning technologies provided by the EU Centre is still to be agreed as part of Article 50 (see below).

Article 11 concerns guidelines to be drafted by the Commission on the application of detection orders as well as on Articles 9 and 10.

Article 50(1) concerns the provision of detection technologies by the EU Centre. It is proposed that the technologies can be used by providers both for the implementation of detection orders and to mitigate the risk of the dissemination of CSAM on the respective services.

Delegations are invited to provide feedback on the following:

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

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

---

[6] Article 50(2) corresponds to the Commission proposal, while Article 50(3) has been provisionally agreed.

ANNEX

Presidency compromise texts on detection and searches

Addition to Article 1:

This Regulation is without prejudice to Union law in the field of cooperation in civil and criminal matters and national law in civil and criminal matters.

Addition to Article 2 (definitions):

"*Content that is publicly accessible*" means information that has been made available, at the request of a content provider, to a potentially unlimited number of persons without requiring a human decision or selection of who is granted access.

Addition to Article 4 (1) [subparagraph]

"own-initiative searching for [online] child sexual abuse/[material] on their services"

Addition to Article 83(1) [subparagraph]

"For own-initiative searching under Article [Z], the type and volumes of data processed under Article [Z]; the number of cases of [online] child sexual abuse/[material] identified, [differentiating between child sexual abuse material and solicitation of children]; the number of cases in which a user has lodged a complaint with the internal redress mechanism or with a judicial or administrative authority and the outcome of such complaints; the numbers and ratios of errors (false positives) of the different technologies used; the measures applied to limit the error rate and the error rate achieved."

Article 84(1) would read:

"Each provider of relevant information society services shall draw up an annual report on its activities under this Regulation. That report shall compile the information referred to in Article 83(1). The providers shall, by 31 January of every year subsequent to the year to which the report relates, make the report available to the public and communicate it to the Coordinating Authority of establishment, the Commission and the EU Centre."

* * *

Article 49

Searches and notifications by the EU Centre

1. The EU Centre shall have the power to conduct searches on content that is publicly accessible for [online] child sexual abuse/[material], using the relevant indicators from the databases of indicators referred to in Article 44(1), in the following situations:
   […]

(ba) on its own initiative for [online] child sexual abuse/[material].

The technologies used by the EU Centre to conduct the searches referred to in paragraph 1 [shall comply with the requirements set out in Article 10, as applicable]. The European Data Protection Board shall issue guidelines regarding the compliance with Regulation (EU) 2016/679 of existing and future technologies that are used by the EU Centre to conduct the searches referred to in paragraph [1].

The EU Centre shall notify, after having conducted the searches referred to in paragraph 1, the Coordinating Authority [of establishment] of its findings.

2. Where the EU Centre has not received a request by a competent law enforcement authority of a Member State pursuant to paragraph 3 within [XX days/weeks] or where the suspension period of such request has expired, whichever occurs first, it shall notify, after having conducted the searches referred to in paragraph 1, providers of hosting services of the presence of one or more specific items of [online] child sexual abuse/[material] on their services. Providers shall take the notifications by the EU Centre under this paragraph into account for the purpose of their obligations under Article 12.

The notification to providers shall clearly set out the identification details of the EU Centre and a contact point, the necessary information for the identification of the item or items, as well as the reasons for the request. The notification shall also clearly state that it is for the provider's voluntary consideration.

3. Where so requested by a competent law enforcement authority of a Member State in order to avoid interfering with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences, the EU Centre shall suspend the notification to the provider in question, for a maximum period of 18 months.

* * *

Article Z

Own-initiative searches for [online] child sexual abuse/[material] on content that is not publicly accessible

By way of derogation, 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 technologies for the sole purpose of searching for [online] child sexual abuse/[material] and reporting it in accordance with Article 12;

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) They use the corresponding indicators provided by the EU Centre in accordance with Article 44[7] and ensure that the technologies and safeguards applied are in full conformity with the requirements set out in Article 10.

(c) They inform the EU Centre of their intention to conduct own-initiative searches under [this Section] [5 days] in advance of doing so.

Article Z+1

Suspension of own-initiative searches on content that is not publicly accessible

If [Coordinating Authorities [of establishment]/supervisory authority[8]] obtain information that leads them to consider that the conditions of Article Z are not met by providers, they shall have the power to order providers to suspend own-initiative searches for [online] child sexual abuse/[material] on content that is not publicly accessible, until such time that providers can satisfy the authority in question that the conditions in Article Z are fulfilled.

7 Transitional provisions (still to be added) should apply for the period until the EU Centre database of indicators will be created.

8 This would be the competent supervisory authority designated pursuant to Regulation (EU) 2016/679. A reference to this could be made in a recital.

Article Z+2

The conditions for providers pursuant to Article Z and the powers of [Coordinating Authorities [of establishment]/data protection authorities] pursuant to Z+1 shall apply *mutatis mutandis* to providers of hosting services that conduct searches on content on their services that is not publicly accessible.

* * *

Article X

Issuance of detection orders for content that is publicly accessible

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

2. A public content detection order shall only be issued if the service or part of the service is being misused for [online child sexual abuse] to an appreciable extent.

3. The application of this article shall not lead to any general monitoring obligation.

Article X+1

Procedure for the issuance of public content detection orders

1. Before [issuing/requesting the issuing of] a public content detection order, the Coordinating Authority [of establishment] shall:
   (a) communicate a draft order to the hosting service concerned, specifying the reasons for its intention to [issue/request the issuing of] the order, the specific parts of the service the order concerns, the EU Centre indicators to be used, the duration of the order and an appropriate period for the provider to submit comments; and
   (b) communicate its draft order to the EU Centre, with an appropriate period for comments.
2. If, having regard to the comments of the provider and the EU Centre, the Coordinating Authority [of establishment] continues to be of the view that the conditions of Article X are met, it shall [issue/submit a request for the issuance of the order, adjusted where appropriate, to the judicial [or independent administrative] authority] using the template set out in Annex XV. [The judicial [or independent administrative] authority shall adopt the order in question, when it considers that the conditions of Article X are met.]

3. The [Coordinating Authority of establishment] / judicial [or independent administrative] authority shall issue the detection orders referred to in Article X using the template set out in Annex [XV]. An order shall contain:
   (a) the period during which it applies, indicating the start date and the end date;
   (b) information necessary for the provider to be able to execute the order, including the EU Centre indicators and the relevant safeguards; and
   (c) information about the right to appeal to a court in accordance with national law.
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annex [XV] where necessary to improve the templates in view of relevant technological developments or practical experiences gained.

* * *

Article Y

Issuance of detection orders for content that is not publicly accessible

1. The Coordinating Authority [of establishment] shall have the power to request a judicial [or independent administrative] authority of its Member State to issue an order requiring a provider of hosting services or a provider of number-independent interpersonal communications services under the jurisdiction of that Member State to detect [online] child sexual abuse/[material]] on a part of its service that contains content that is not publicly accessible ('non-public content detection order') using indicators from the databases operated by the EU Centre pursuant to Article 44 and technologies for detection that fulfil the requirements of Article 10.

2. A non-public content detection order shall only be issued if:

   (a) it concerns specific users;

   (b) there are clear indications, based on information lawfully acquired, that those specific users are related to [online] child sexual abuse/ [material] and that they have used the service in the 12 months prior to the request for [online] child sexual abuse/[material];

   (c) issuing the detection order is necessary and proportionate and outweighs negative consequences on 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.

3. [In the case of non-public content detection orders concerning the solicitation of children, the order shall apply where one of the users that participates in the interpersonal communication is a child.]

4. [The application of this article shall not lead to any generalised and indiscriminate monitoring.]

Article Y+1

Procedure for the issuance of non-public content detection orders

1. Before requesting the issuing of a non-public content detection order, the Coordinating Authority [of establishment] shall:

   (a) communicate a draft request to the provider, specifying the reasons for its intention to request the order, the specific users the order concerns, the EU Centre indicators to be used, the duration of the order and an appropriate period for the provider to submit its comments.

   Within a period set by the Coordinating Authority [of establishment], the provider shall submit a draft implementation plan setting out the measures it envisages taking to execute a possible detection order, including detailed information regarding the envisaged technologies and safeguards.

   If the draft implementation plan concerns possible detection of [new child sexual abuse material or solicitation of children], it must include the data protection impact assessment and the opinion of the data protection authority as referred to in Article 10(6)(c) below, unless the draft request concerns a renewal of a previously issued detection order.

   (b) communicate the draft request to the EU Centre, with an appropriate period for comments.

   [The provider may consult the EU Centre to obtain support in the creation of its draft implementation plan.]

2. If, having regard to the comments of the provider and the EU Centre, the [Coordinating Authority [of establishment] continues to be of the view that the conditions of Article Y are met, it shall submit a request for the issuance of the order to a judicial [or independent administrative] authority, using the template set out in Annex YI and attaching the draft implementation report with any appropriate amendments and the comments of the EU Centre.

3. The judicial [or independent administrative] authority shall adopt the order in question, when it considers that the conditions of Article [Y] are met.

4. The judicial [or independent administrative] authority shall issue the detection orders referred to in Article Y using the template set out in Annex YI. An order shall contain:

   (a) the period during which it applies, indicating the start date and the end date. The period of application of detection orders concerning known or new child sexual abuse material shall be proportionate and shall not exceed 24 months [and that of detection orders concerning the solicitation of children shall not exceed 12 months].

   (b) information necessary for the provider to be able to execute the order, including the relevant users, the EU Centre indicators and the relevant safeguards.

   (c) information about the right to appeal to a court of law in accordance with national law.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to amend Annexes YI and YII where necessary to improve the templates in view of relevant technological developments or practical experiences gained.

* * *

Article 9

Redress, information, reporting and modification of orders pursuant to Articles X and Y

1. Providers of hosting services and providers of number-independent interpersonal communications services that have received an order pursuant to Articles X or Y, as well as users concerned by the measures taken to execute it, shall have a right to information and effective redress. That right shall include the right to challenge the order before the courts of the Member State of the judicial [or independent administrative] authority that issued the order.

2. When the order becomes final, the issuing authority shall, without undue delay and where relevant, transmit a copy thereof to the Coordinating Authority of establishment. The Coordinating Authority of establishment shall then, without undue delay, transmit a copy thereof to all other Coordinating Authorities through the system established in accordance with Article 39(2).

   For the purpose of the first subparagraph, a detection order shall become final upon the expiry of the time period for appeal where no appeal has been lodged in accordance with national law or upon confirmation of the detection order following an appeal.

3. Where the period of application of the detection order exceeds 12 months, [or six months in the case of a detection order concerning the solicitation of children], the Coordinating Authority of establishment shall require the provider to report to it on the execution of the detection order at least once, halfway through the period of application.

4. Those reports shall include a detailed description of the measures taken to execute the detection order, including the safeguards provided, and information on the functioning in practice of those measures, in particular on their effectiveness in identifying [online] child sexual abuse/[material] on their service, as applicable, and on the consequences of those measures for the rights and legitimate interests of all parties affected.

5. The Coordinating Authority of establishment shall, where necessary and in any event following receipt of the reports referred to in paragraph 3, assess whether any substantial changes to the grounds for issuing the detection orders occurred and, in particular, whether the conditions of Articles X or Y respectively continue to be met. In that regard, it shall take account of additional measures that the provider may have taken to prevent the misuse of their service for the purpose of [online] child sexual abuse.

6. That Coordinating Authority shall request the issuing authority to to amend or revoke the order, where appropriate. Articles [X and X+1] shall apply mutatis mutandis for the amendment or revocation of an orders that were issued pursuant to Article X, while Articles [Y and Y+1] shall apply mutatis mutandis to orders that were issued pursuant to Article Y.

Article 10

Technologies and safeguards for the application of Articles X, Y and Z

1. Providers of hosting services and providers of number-independent interpersonal communication services that have received a detection order according to Articles X and Y [or that conduct own-initiative searches according to Article Z] shall use secure and privacy-friendly technologies to identify known or new child sexual abuse material [or the solicitation of children], as applicable, on their services.

2. The provider shall not be required to use any specific technology as long as the requirements set out in this Article are met.

3. Where the provider operates technologies made available by the EU Centre in accordance with Article 50(1), the use of these technologies shall not affect the responsibility of the provider to comply with the requirements set out in this Article and for any decisions it may take in conncection to or as a result of the use of the technologies.

4. [The technologies relied on for the purpose of executing the orders under Articles X and Y [or for own-initiative searches according to Article Z], shall be audited independently at the cost of providers as regards their performance, reliability and security. The audit shall be made publicly available.]

5. The technologies shall:

   (a) be effective in identifying [online] child sexual abuse/material, as applicable;

   (b) not allow for the acquisition of knowledge of the content of the communications or any information from the relevant communications other than that which is strictly necessary for the purpose referred to in paragraph 1, including patterns pointing to [online] child sexual abuse/[material], as applicable;

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

(d) be sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the identification of [online] child sexual abuse/[material].

6. The provider shall:

(a) take all the necessary measures to ensure that the technologies, as well as the processing of personal data and other data in connection thereto, are proportionate and limited to what is strictly necessary for the sole purpose of identifying known or new child sexual abuse material [or the solicitation of children], as applicable;

(b) establish effective internal procedures to prevent and, where necessary, identify and remedy any misuse of the technologies, indicators and personal data and other data referred to in point (a), including unauthorised access to, and unauthorised transfers of, such personal data and other data;

(c) in respect of any specific technology used for the purpose set out in point (a) 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) provide for 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 identified, [immediate] human intervention;

(e) 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 about 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; and

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

(g) rectify without delay the consequences of errors regarding the detection of content representing [online] child sexual abuse/[material] which result from the use of the technology

7. The provider shall inform users concerned in a clear and easily comprehensible way of the following:

   (a) the fact that it operates technologies to identify [online] child sexual abuse/ [material] to execute the detection order or that is searches for [online] child sexual abuse/[material] on its own initiative, the ways in which it operates those technologies 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; and

   (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 6, point (e) and to the Coordinating Authority in accordance with Article 34.

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

8. Where a provider identifies potential [online] child sexual abuse/[material] through the measures taken under this Regulation, 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.

Article 11

Guidelines regarding detection obligations

The Commission, in cooperation with the Coordinating Authorities and the EU Centre and after having consulted the European Data Protection Board and having conducted a public consultation, may issue guidelines on the application of Articles [X, Y, 9, 10], having due regard in particular to relevant technological developments, trends reported by law enforcement, hotlines and civil society and the manner in which the services covered by those provisions are offered and used.

Article 50

Technologies, information and expertise

1. The EU Centre shall make available, free of charge, technologies that providers of hosting services and providers of number-independent interpersonal communications services may use free of charge, where relevant subject to reasonable licensing conditions, to identify known or new child sexual abuse material [or the solicitation of children] or to mitigate the risk of the dissemination of child sexual abuse material on their services. The EU Centre shall make publicly available the relevant information related to the making available of these technologies or tools, including the names of the manufacturers of the technologies.

2. To that aim, the EU Centre shall compile lists of such technologies, having regard to the requirements of this Regulation and in particular those of Article 10(5).

3. Before including specific technologies on those lists, the EU Centre shall request the opinions of its Technology Committee and Victims Consultative Forum, and through the Commission, the opinion of the European Data Protection Board. The Technology Committee, the Victims Consultative Forum and the European Data Protection Board shall deliver their respective opinions within eight weeks. That period may be extended by a further six weeks where necessary, taking into account the complexity of the subject matter. The Technology Committee and the European Data Protection Board shall inform the EU Centre of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay. Where the EU Centre substantially deviates from those opinions, it shall inform, where applicable, the Technology Committee, the Victims Consultative Forum, or the European Data Protection Board and the Commission thereof, specifying the points where it deviated and the main reasons for that deviation.