Council of the European Union
General Secretariat

Brussels, 22 April 2025

WK 4915/2025 INIT

LIMITE

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

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

WORKING DOCUMENT

From:	Presidency
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - working documents

In preparation of the meeting of JHA counsellors on 29 April 2025, delegations are provided in the annex with supporting documents to facilitate the work on the Presidency compromise texts as set out in 7080/25.

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

Presidency suggestion to incorporate the provisions of Article 5a in Article 27

Following the examination of Presidency compromise texts[1] at the meeting of the Law Enforcement Working Party – Police on 8 April 2025, the Presidency suggests incorporating the provisions of Article 5a on adjusted or additional risk assessment or risk mitigation prevention measures and Article 5b on redress and complaints into Article 27. This would help to avoid uncertainty and to benefit from the already established procedure and safeguards laid down in Article 27 on the enforcement powers conferred to competent authorities of the Member States in alignment with the Digital Services Act (DSA).

The Presidency is proposing the amendments to Article 27 and Recital 48 as outlined below while suggesting the deletion of Articles 5a and 5b, and of Recital 18a.

In accordance with Article 27(1)(b), competent authorities of the Member States have the power to order the cessation of infringements of this Regulation and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end or to request a judicial authority to do so. Thus, the coordinating authorities have the power to impose on the providers remedies which may include adjusted or additional risk assessment or risk mitigation measures. When imposing such remedies, the coordinating authorities should take into account the assessment and the determination of a significant level of remaining risk with respect to parts or components of a service referred to in Article 5(2).

The Presidency proposes to list explicitly the risk mitigation measures laid down in Article 4(1), points (b) to (g) as possible remedies to infringements in Article 27(2), points (ii) to (vii). Point (a) of Article 4(1) is not included in the list as that provision is very broad and elements thereof could still be imposed on the providers, if proportionate and appropriate, as the list of remedies is non-exhaustive.

The Presidency also proposes to include in the list the provisions from Article 5a regarding re-conducting or updating the risk assessment (Article 27(2), point (i)) and the obligation for specific providers to contribute to the development of risk mitigation technologies in a reasonable and targeted way (Article 27(2), point (viii)).

Finally, the Presidency stresses that there should be no detection order through the back door. Therefore, a new paragraph 4a to Article 27 is proposed to make clear that the measures imposed by competent authorities should not lead to an obligation for the providers to detect child sexual abuse on their services.

[1] 7080/25.

Proposed amendment to Recital 48:

(48) Given the need to ensure the effectiveness of the obligations imposed, ~~Coordinating~~ **competent a**uthorities should be granted enforcement powers to address infringements of this Regulation. **In particular, given the importance of ensuring that all possible risk mitigation measures have been taken in accordance with this Regulation, the competent authorities should be granted specific powers to require providers to adjust their risk assessment or mitigation measures so as to ensure compliance with the relevant requirements of this Regulation. However, they should not impose any obligation for providers to carry out detection, which should remain voluntary.** The enforcement powers should include the power to temporarily restrict access of users of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider on which the infringement takes place. In light of the high level of interference with the rights of the service providers that such a power entails, the latter should only be exercised when certain conditions are met. Those conditions should include the condition that the infringement results in the regular and structural facilitation of child sexual abuse offences, which should be understood as referring to a situation in which it is apparent from all available evidence that such facilitation has occurred on a large scale and over an extended period of time.

Proposed amendment to Article 27:

Article 27

*Investigatory **and enforcement** powers*

1. Where needed **in order to** ~~for~~ carrying out their tasks **under this Regulation**, **competent authorities** ~~Coordinating Authorities~~ shall have the following powers of investigation, in respect of **conduct by** providers of relevant information society services under the jurisdiction of ~~the~~ **their** Member State ~~that designated them~~:

   (a) the power to require those providers, as well as any other persons acting for purposes related to their trade, business, craft or profession that may reasonably be aware of information relating to a suspected infringement of this Regulation, to provide such information **without undue delay** ~~within a reasonable time period~~;

   (b) the power to carry out**, or to request a judicial authority to order,** ~~on-site~~ inspections of any premises that those providers or ~~the other~~ **those** persons ~~referred to in point (a)~~ use for purposes related to their trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information relating to a suspected infringement ~~of this Regulation~~ in any form, irrespective of the storage medium;

   (c) the power to ask any member of staff or representative of those providers or ~~the other~~ **those persons** to give explanations in respect of any information relating to a suspected infringement of this Regulation and to record the answers **by any technical means**;

   (d) the power to request information, including to assess whether the measures taken to ~~**prevent**~~ **mitigate the risk of online child sexual abuse or** execute a ~~detection order,~~ removal order~~, or~~ blocking order **or delisting order** comply with the requirements of this Regulation.

~~2. Member States may grant additional investigative powers to the Coordinating Authorities.~~

~~*Article 28*~~

~~*Enforcement powers*~~

2. ~~1.~~ Where needed for carrying out their tasks **under this Regulation**, **competent authorities** ~~Coordinating Authorities~~ shall have the following enforcement powers, in respect of providers of relevant information society services under the jurisdiction of ~~the~~ **their** Member State ~~that designated them~~:

(a) the power to accept the commitments offered by those providers in relation to their compliance with this Regulation and to make those commitments binding;

(b) the power to order the cessation of infringements ~~of this Regulation~~ and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end **or to request a judicial authority to do so.**

(c) the power to impose fines, or request a judicial authority in their Member State to do so, in accordance with Article 35 for **failure to comply with** ~~infringements of~~ this Regulation, including ~~non-compliance with~~ any of the orders issued pursuant to **paragraph 1 of this** Article ~~27 and to point (b) of this paragraph~~;

(d) the power to impose a periodic penalty payment**, or to request a judicial authority to do so,** in accordance with Article 35 to ensure that an infringement ~~of this Regulation~~ is terminated in compliance with an order issued pursuant to point (b) of this **sub**paragraph or for failure to comply with any of the orders issued pursuant to **paragraph 1 of this** Article. ~~27 and to point (b) of this paragraph~~;

(e) the power to adopt interim measures **or to request the competent national judicial authority to do so,** to avoid the risk of serious harm.

~~2. Member States may grant additional enforcement powers to the Coordinating Authorities.~~

As regards point (b) of the first subparagraph of this paragraph, the coordinating authorities shall take into account the assessment and the determination of a significant level of remaining risk with respect to parts or components of a service referred to in Article 5(2) when imposing such remedies, which may include:

(i) re-conducting or updating 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.

(ii) reinforcing the provider's internal processes or the internal supervision of the functioning of the service;

(iii) initiating or adjusting cooperation, in accordance with competition law, with other providers of hosting services or providers of interpersonal communications services, public authorities, civil society organisations or, where applicable, entities awarded the status of trusted flaggers in accordance with Article 22 of Regulation (EU) 2022/2065;

(iv) initiating or adjusting functionalities that enable users to notify online child sexual abuse to the provider through tools that are easily accessible and age-appropriate;

(v) initiating or adjusting functionalities that enable users to control what information about them is shared to other users and how other users may contact them, and introducing default suitable privacy settings for users who are children;

(vi) initiating or adjusting functionalities that provide information to users about notification mechanisms and direct users to helplines and trusted organisations, where users detect material or conversations indicating potential online child sexual abuse;

(vii) initiating or adjusting functionalities that allow the providers to collect statistical data to better assess the risks and the effectiveness of the mitigation measures. This data shall not include any personal data.

(viii) to take reasonable and targeted measures in cooperation with the EU Centre, in accordance with Article 50(1a), to develop relevant technologies to mitigate the risks of child sexual abuse identified on their services.

The ~~Coordinating Authority of establishment~~ competent authority may request the EU Centre for an opinion on technical aspects of the orders that it intends to impose pursuant to point (b) of the first subparagraph of this paragraph.

A provider that is required to perform the actions specified in points (ii) or (vii) of point (b) of the first subparagraph of this paragraph, shall, within a time period set by the competent authority, 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 the actions performed pursuant to this subparagraph.

By deviation from the time periods specified in Articles 3(4) and 5(1), the competent authority shall set a reasonable time period, taking into account the complexity of the required actions, for the performance of the actions including the reporting specified in point (b) of the first subparagraph of this paragraph.

~~3.~~ As regards **t~~he first sub~~**~~paragraph 1~~, points (c) and (d) **of the first subparagraph of this paragraph**, **competent authorities** ~~Coordinating Authorities~~ shall **also** have the enforcement powers set out in those points ~~also~~ in respect of the other persons referred to in **paragraph 1** ~~Article 27~~, for failure to comply with any of the orders issued to them pursuant to that **paragraph** ~~Article~~. ~~4.~~ They shall only exercise those enforcement powers after having provided those other persons in good time with all relevant information relating to such orders, including the applicable ~~time~~ period, the fines or periodic payments that may be imposed for failure to comply and ~~redress~~ **the** possibilities **for redress**.

~~*Article 29*~~

~~*Additional enforcement powers*~~

3. ~~1.~~ Where needed for carrying out their tasks **under this Regulation**, **competent authorities** ~~Coordinating Authorities~~ shall ~~have the additional enforcement powers referred to in paragraph 2~~, in respect of providers of relevant information society services under the jurisdiction of the**ir** Member State**, where** ~~that designated them, provided that:~~

~~(a)~~ all other powers pursuant to **this** Article~~s 27 and 28~~ to bring about the cessation of an infringement ~~of this Regulation~~ have been exhausted~~;~~

~~(b)~~ **and** the infringement **has not been remedied or is continuing and is** ~~persists;~~

~~(c)~~ ~~the infringement~~ ~~causes~~ **causing** serious harm which cannot be avoided through the exercise of other powers available under Union or national law**, also have the power to take the following measures:**

~~2. Coordinating Authorities shall have the additional enforcement powers to take the following measures:~~

(a) **to** require the management body of the providers**, without undue delay,** to examine the situation**,** ~~within a reasonable time period and to:~~

~~(i)~~ adopt and submit an action plan setting out the necessary measures to terminate the infringement;

~~(ii)~~ ensure that the provider takes those measures; **and**

~~(iii)~~ report on the measures taken;

(b) **where the competent authorities consider that a provider of relevant information society services has not sufficiently complied with the requirements of point (a) <u>of the first subparagraph of this paragraph</u>, that the infringement has not been remedied or is continuing and is causing serious harm, and that that infringement entails a criminal offence involving a threat to the life or safety of persons or the infringement results in the regular and structural facilitation of child sexual abuse offences,** to request **that** the competent judicial authority or **other** independent administrative authority of its ~~the~~ Member State ~~that designated the Coordinating Authority to~~ order the temporary restriction of access of users of the service concerned by the infringement or, only where that is not technically feasible, to the online interface of the provider on which the infringement takes place**.** ~~, where the Coordinating Authority considers that:~~

~~(i) the provider has not sufficiently complied with the requirements of point (a);~~

~~(ii) the infringement persists and causes serious harm;~~

~~(iii) the infringement results in the regular and structural facilitation of child sexual abuse offences.~~

~~3.~~ The ~~Coordinating Authority~~ **competent authorities** shall, prior to submitting the request referred to in ~~**this** paragraph 2~~, point (b) **of the first subparagraph of this paragraph**, invite interested parties to submit written observations **within a period that shall not be less than two weeks, describing the measures that it intends to request and identifying the intended addressee or addressees thereof. The provider, the intended addressee or addressees and any other third party demonstrating a legitimate interest shall be entitled to participate in the proceedings before the competent judicial authority or other independent administrative authority.**

~~on its intention to submit that request within a reasonable time period set by that Coordinating Authority. That time period shall not be less than two weeks.~~

~~The invitation to submit written observations shall:~~

~~(a) describe the measures that it intends to request;~~

~~(b) identify the intended addressee or addressees thereof.~~

~~The provider, the intended addressee or addressees and any other third party demonstrating a legitimate interest shall be entitled to participate in the proceedings regarding the request~~.

~~4.~~ Any measure ordered ~~upon the request referred to in paragraph 2, point (b),~~ shall be proportionate to the nature, gravity, recurrence and duration of the infringement, without unduly restricting access to lawful information by users of the service concerned.

The ~~temporary~~ restriction **of access** shall **be** ~~apply~~ for a period of four weeks, subject to the possibility for the competent judicial authority **or other independent administrative authority of the Member State**, in its order, to allow the ~~Coordinating Authority~~ **competent authorities** to extend that period for further periods of the same lengths, subject to a maximum number of extensions set by **that** judicial authority **or other independent administrative authority**.

The ~~Coordinating Authority~~ **competent authorities referred to in the second subparagraph of this paragraph** shall only extend the period where ~~it considers~~, having regard to the rights and ~~legitimate~~ interests of all parties affected by ~~the~~ **that** restriction and all relevant ~~facts and~~ circumstances, including any information that the provider, the addressee or addressees and any other third party that demonstrated a legitimate interest may provide to **them** ~~it~~, **they consider** that both of the following conditions have been met:

(a) the provider has failed to take the necessary measures to terminate the infringement;

(b) the temporary restriction does not unduly restrict access to lawful information by users of the service, having regard to the number of users affected and whether any adequate and readily accessible alternatives exist.

Where the ~~Coordinating Authority~~ **competent authority,** considers that **the conditions set out in the points (a) and (b) of the fifth subparagraph of this paragraph** ~~those two conditions~~ have been met but it cannot further extend the period pursuant to the **fourth** ~~second~~ subparagraph **of this paragraph**, it shall submit a new request to the ~~competent~~ judicial authority **or other independent administrative authority**, as referred to in ~~**the first sub**paragraph 2.~~ point (b) **of the first subparagraph of this paragraph**.

~~*Article 30*~~

~~*Common provisions on investigatory and enforcement powers*~~

4. ~~1.~~ The measures taken by the ~~Coordinating Authorities~~ **competent authorities** in the exercise of their investigatory and enforcement powers **listed in paragraphs 1, 2 and 3** ~~referred to in Articles 27, 28 and 29~~ shall be effective, dissuasive and proportionate, having regard, in particular, to the nature, gravity, recurrence and duration of the infringement ~~of this Regulation~~ or suspected infringement to which those measures relate, as well as the economic, technical and operational capacity of the provider of relevant information society services concerned~~,~~ where **relevant** ~~applicable~~.

4a. The measures taken by the competent authorities in the exercise of their investigatory and enforcement powers listed in paragraphs 1, 2 and 3 shall not lead to an obligation for the providers to detect child sexual abuse on their services; such detection shall remain strictly voluntary.

5. ~~2.~~ Member States shall **lay down specific rules and procedures for the exercise of the powers pursuant to paragraphs 1, 2 and 3 and shall** ensure that any exercise of **those** ~~the investigatory and enforcement~~ powers ~~referred to in Articles 27, 28 and 29~~ is subject to adequate safeguards laid down in the applicable national law **in compliance with the Charter and with the general principles of Union law** ~~to respect the fundamental rights of all parties affected~~. In particular, those measures shall only be taken in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and of access to the file, and subject to the right to an effective judicial remedy of all ~~parties~~ affected **parties**.

ANNEX 2

Comparison of the provisions on voluntary detection in the Presidency compromise texts (7080/25) with Regulation (EU) 2021/1232

Presidency compromise texts (7080/25) Newly introduced text is marked in **bold**	Regulation (EU) 2021/1232 Text not reflected in Presidency compromise texts is marked in underlined
Article 6a Derogation from Directive 2002/58/EC for voluntary detection	Article 3 Scope of the derogation
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:	1. Articles 5(1) and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that:
(a) the processing is: (i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it **in accordance with Article 12** and of detecting solicitation of children 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);	(a) the processing is: (i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to law enforcement authorities or organisations acting in the public interest against child sexual abuse; (ii) proportionate and limited to technologies used by providers for the purpose set out in point (i); (iii) limited to content data and related traffic data that are strictly necessary for the purpose set out in point (i); (iv) limited to what is strictly necessary for the purpose set out in point (i);

(b) the providers use the corresponding indicators provided by the EU Centre in accordance with Article 46.	
(c) the providers ensure that the technologies and safeguards applied are in full conformity with the requirements set out in Article 6b.	
(d) the providers: (i) have established appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views; (ii) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC concerning the confidentiality of users' communications for the sole purpose set out in point (a)(i) of this paragraph, the logic behind the measures they have taken under the derogation and the impact on the confidentiality of users' communications, including the possibility that personal data are shared with law enforcement authorities;	(g) the providers: (iv) have established appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views; (v) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC concerning the confidentiality of users' communications for the sole purpose set out in point (a)(i) of this paragraph, the logic behind the measures they have taken under the derogation and the impact on the confidentiality of users' communications, including the possibility that personal data are shared with law enforcement authorities <u>and organisations acting in the public interest against child sexual abuse</u>;
(e) where suspected online child sexual abuse has been identified, the content data and related traffic data processed for the purpose set out in point (a)(i), and personal data generated through such processing are stored in a	(h) where suspected online child sexual abuse has been identified, the content data and related traffic data processed for the purpose set out in point (a)(i), and personal data generated through such processing are

secure manner, solely for the purposes of: (i) reporting, without delay, the suspected online child sexual abuse **in accordance with Article 12**; (ii) blocking the account of, or suspending or terminating the provision of the service to, the user concerned; (iii) creating a unique, non-reconvertible digital signature ('hash') of data reliably identified as online child sexual abuse material; (iv) enabling the user concerned to seek redress from the provider or pursue administrative review or judicial remedies on matters related to the suspected online child sexual abuse; or (v) responding to requests issued by competent law enforcement and judicial authorities in accordance with the applicable law to provide them with the necessary data for the prevention, detection, investigation or prosecution of criminal offences as set out in Directive 2011/93/EU;	stored in a secure manner, solely for the purposes of: (i) reporting, without delay, the suspected online child sexual abuse <u>to the competent law enforcement and judicial authorities or organisations acting in the public interest against child sexual abuse</u>; (ii) blocking the account of, or suspending or terminating the provision of the service to, the user concerned; (iii) creating a unique, non-reconvertible digital signature ('hash') of data reliably identified as online child sexual abuse material; (iv) enabling the user concerned to seek redress from the provider or pursue administrative review or judicial remedies on matters related to the suspected online child sexual abuse; or (v) responding to requests issued by competent law enforcement and judicial authorities in accordance with the applicable law to provide them with the necessary data for the prevention, detection, investigation or prosecution of criminal offences as set out in Directive 2011/93/EU;
(f) every case of a reasoned and verified suspicion of online child sexual abuse is reported without delay **in accordance with Article 12**.	(j) every case of a reasoned and verified suspicion of online child sexual abuse is reported without delay <u>to the competent national law enforcement authorities or to organisations acting in the public interest against child sexual abuse</u>.

	Article 6b Technologies and safeguards	
1.	Providers **of number-independent communications services shall put in place the following safeguards to ensure that the processing based on Article 6a is limited to what is strictly necessary and justified to the purpose of this derogation**:	(g) the providers:
	(a) **establish technical and organisational measures** to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data **processed in accordance with this Regulation**,	(i) <u>have established internal procedures</u> to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data;
	(b) record, in respect of any processing of content and other data pursuant to Article 6a, necessary information for the verification of the lawfulness of the processing, such as the time and duration of the processing and, where applicable, the person performing the processing. Such logs shall only be used for the of the lawfulness of the processing, for self-monitoring, for ensuring data integrity and data security as well as for the purposes of criminal or disciplinary proceedings;	
	(c) keep the information contained in the logs referred to in point (b) for no longer than necessary for the applicable purpose and, in any event, no longer than five years from the date of the measures taken that led to the obligation to preserve the information recorded in those logs. They shall subsequently irrevocably delete the information;	

	(d) keep the logs referred to in point (b) for a further specified period if requested by the competent authority or court, set by that requesting authority or court, where and to the extent necessary for one of the purposes referred to in point (b);	
	(e) diligently identify, analyse and assess the cybersecurity risks that could be introduced by the technologies used for detection, and take all reasonable mitigation measures, tailored to the possible cybersecurity risk identified, to minimise that risk;	
	(f) ensure human oversight of and, where necessary, human intervention in the processing of personal and other data using technologies falling under this Regulation;	(ii) ensure human oversight of and, where necessary, human intervention in the processing of personal and other data using technologies falling under this Regulation;
	(g) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported **in accordance with Article 12** without prior human confirmation.	(iii) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported <u>to law enforcement authorities or organisations acting in the public interest against child sexual abuse</u> without prior human confirmation;
2.	The technologies used for the purpose set out **in Article 6a**, point (a)(i), **including those made available by the EU Centre in accordance with Article 50(1), shall meet the following conditions**:	(b) the technologies used for the purpose set out in point (a)(i) of this paragraph
	(a) are effective and suitable in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable,	

(b) are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679,	are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679
(c) to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse;	and, to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse;
(d) do not introduce cybersecurity risks for which it is not possible to take any effective measures to mitigate such risk;	
(e) **are subject to** a prior data protection impact assessment as referred to in Article 35 of Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation;	(c) in respect of any specific technology used for the purpose set out in point (a)(i) of this paragraph, a prior data protection impact assessment as referred to in Article 35 of Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation have been conducted;
(f) with regard to new technology used for the purpose set out in point (a)(i) of this paragraph, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services in the Union before 2 August 2021, and with regard to	(d) with regard to new technology, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services ('users') in the Union before 2 August 2021, and with regard to technology used for the purpose of identifying possible

technology used for the purpose of identifying possible solicitation of children, the provider shall report back to the competent authority on the measures taken to demonstrate compliance with written advice issued in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation ('supervisory authority') in the course of the prior consultation procedure;	solicitation of children, the provider reports back to the competent authority on the measures taken to demonstrate compliance with written advice issued in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation (' supervisory authority') in the course of the prior consultation procedure;
(g) are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online child sexual abuse and, where such occasional errors occur, their consequences are rectified without delay;	(e) the technologies used are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online child sexual abuse and, where such occasional errors occur, their consequences are rectified without delay;
(h) **in** the **case of** technologies used to detect patterns of possible solicitation of children, are limited to the use of relevant key indicators and objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication, without prejudice to the right to human review.	(f) the technologies used to detect patterns of possible solicitation of children are limited to the use of relevant key indicators and objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication, without prejudice to the right to human review.
3. The use of the technologies made available by the EU Centre shall not affect the responsibility of the provider to comply with the requirements set out in paragraph 2 and for any decisions it may take in connection to or as a result of the use of the technologies.	

4.	In accordance with Article 79 of Regulation (EU) 2016/679 and Article 15(2) of Directive 2002/58/EC, users shall have the right to an effective judicial remedy where they consider that their rights have been infringed as a result of the processing of personal and other data for the purpose set out in Article 6a(1), point (a)(i), of this Regulation.	Article 5 Effective judicial remedies In accordance with Article 79 of Regulation (EU) 2016/679 and Article 15(2) of Directive 2002/58/EC, users shall have the right to an effective judicial remedy where they consider that their rights have been infringed as a result of the processing of personal and other data for the purpose set out in Article 3(1), point (a)(i), of this Regulation.
5.	The providers shall inform the users of the following: (a) the avenues for seeking redress from them; (b) the possibility of lodging a complaint with a supervisory authority; and (c) the right to a judicial remedy.	(g) the providers: (vi) inform users of the following, where their content has been removed or their account has been blocked or a service offered to them has been suspended: (1) the avenues for seeking redress from them; (2) the possibility of lodging a complaint with a supervisory authority; and (3) the right to a judicial remedy;

Article 6c Transparency obligations	
1. The providers shall, **by 31 January [year after the entry into force of this Regulation]** and every year thereafter, publish and submit to the competent supervisory authority**, the Coordinating Authority of establishment**, the Commission **and the EU Centre** a report on the processing of personal data under this Section, including on:	(g) the providers: (vii) by 3 February 2022, and by 31 January every year thereafter, publish and submit to the competent supervisory authority and to the Commission a report on the processing of personal data under this Regulation, including on:
(a) the type and volumes of data processed; (b) the specific ground relied on for the processing pursuant to Regulation (EU) 2016/679; (c) the ground relied on for transfers of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable; (d) the number of cases of online child sexual abuse identified, differentiating between online child sexual abuse material and solicitation of children; (e) the number of cases in which a user has lodged a complaint with the internal redress mechanism or with a judicial authority and the outcome of such complaints; (f) the numbers and ratios of errors (false positives) of the different technologies used; (g) the measures applied to limit the error rate and the error rate achieved; (h) the retention policy and the data protection safeguards applied pursuant to Regulation (EU) 2016/679.	(1) the type and volumes of data processed; (2) the specific ground relied on for the processing pursuant to Regulation (EU) 2016/679; (3) the ground relied on for transfers of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable; (4) the number of cases of online child sexual abuse identified, differentiating between online child sexual abuse material and solicitation of children; (5) the number of cases in which a user has lodged a complaint with the internal redress mechanism or with a judicial authority and the outcome of such complaints; (6) the numbers and ratios of errors (false positives) of the different technologies used; (7) the measures applied to limit the error rate and the error rate achieved; (8) the retention policy and the data protection safeguards applied pursuant to Regulation (EU) 2016/679; (9) the names of the organisations acting in the public interest against child sexual abuse with

	which data has been shared pursuant to this Regulation;
2. The data included in the report referred to in this point shall be provided in writing by means of a standard form. **The Commission shall adopt implementing acts to establish that form**. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 87.	4. The data included in the report referred to in paragraph 1, point (g)(vii), shall be provided in writing by means of a standard form. By 3 December 2024 at the latest, the Commission shall determine the content and presentation of that form by means of implementing acts. In doing so, the Commission may divide the data categories listed in paragraph 1, point (g)(vii), into subcategories. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 9a(2).
Article 6d Supervisory authorities **for the processing of personal data**	Article 6 Supervisory authorities
The supervisory authorities designated pursuant to Chapter VI, Section 1, of Regulation (EU) 2016/679 shall monitor the processing **pursuant to this Section** in accordance with their competences and powers under that Chapter.	The supervisory authorities designated pursuant to Chapter VI, Section 1, of Regulation (EU) 2016/679 shall monitor the processing falling within the scope of this Regulation in accordance with their competences and powers under that Chapter.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
laying down rules to prevent and combat child sexual abuse

Correlation table between Articles and Recitals

(Updated: 7080/25, 4 April 2025)

Correlation table		
Chapters	**Articles**	**Recitals**
1	Article 1 (Subject matter and scope)	Recitals 1-12a
	Article 2 (Definitions)	Recital 13
2	Article 3 (Risk Assessment)	Recitals 14-15
	Article 4 (Risk Mitigation)	Recitals 16, 16a
	Article 5 (Risk Reporting)	Recitals 17-18
	Article 5a (Adjusted or additional risk assessment or risk mitigation measures)	Recital 18a
	Article 5b (Redress and complaints)	
	Article 6 (Obligations for software application stores)	Recital 19
	Articles 6a (Derogation from Directive 2002/58/EC for voluntary detection)	Recitals 20a[1], 20b[2], 20c[3], 20d[4]
	Article 6b (Technologies and safeguards)	Recitals 20e[5], 20f[6], 23, 23b, 23c[7], 23d[8], 26, 26a[9], 26b[10], 26d, 27, 28
	Article 6c (Transparency obligations)	Recitals 20g[11], 20h[12]
	Article 6d (Supervisory authorities for the processing of personal data)	Recitals 20g[13], 20i[14], 26c[15]
	Article 12 (Reporting obligations and notification by the users)	Recital 29
	Article 13 (Specific requirements for reporting)	Recitals 29, 29a, 29b
	Article 14 (Removal orders)	Recitals 30, 31, 31a, 31b
	Article 14a (Procedure for cross-border removal orders)	Recital 31c
	Article 15 (Redress and provision of information)	Recitals 30, 32
	Article 16 (Blocking orders)	Recitals 32, 33-34
	Article 17 (Additional rules regarding blocking orders)	Recitals 33, 34
	Article 18 (Redress and provision of information)	Recital 33

[1] See Recital 7 of Regulation (EU) 2021/1232.
[2] See Recital 8 of Regulation (EU) 2021/1232.
[3] See Recital 9 of Regulation (EU) 2021/1232.
[4] See Recital 11 of Regulation (EU) 2021/1232.
[5] See Recital 12 of Regulation (EU) 2021/1232.
[6] See Recital 15 of Regulation (EU) 2021/1232.
[7] See Recital 17 of Regulation (EU) 2021/1232.
[8] See Recital 32 of Regulation (EU) 2021/1232.
[9] See Recital 16 of Regulation (EU) 2021/1232.
[10] See Recital 18 of Regulation (EU) 2021/1232.
[11] See Recital 21 of Regulation (EU) 2021/1232.
[12] See Recital 29 of Regulation (EU) 2021/1232.
[13] See Recital 21 of Regulation (EU) 2021/1232.
[14] See Recital 30 of Regulation (EU) 2021/1232.
[15] See Recital 31 of Regulation (EU) 2021/1232.

Correlation table		
Chapters	**Articles**	**Recitals**
	Article 18a (Delisting orders)	Recitals 33a, 33b
	Article 18aa (Procedure for cross-border delisting orders)	Recital 33b
	Article 18b (Additional rules regarding delisting orders)	Recitals 33a, 33b
	Article 18c (Redress and provision of information)	Recitals 33a, 33b
	Article 19 (Liability of providers)	Recital 34
	Articles 20 (Victims' right to information)	Recital 35
	Article 21 (Victims' right of assistance and support for removal)	Recitals 36-38
	Article 22 (Preservation of information)	Recital 39
	Article 23 (Points of contact)	Recital 40
	Article 24 (Legal representative)	Recitals 41-42
3	Article 2 (Coordinating Authorities and other competent authorities)	Recitals 45, 45a, 50
	Article 26 (Requirements for competent authorities)	Recitals 46a, 46b
	Article 27 (Investigatory and enforcement powers)	Recitals 47-48
	Article 31 (Searches to verify compliance)	Recital 49
	Article 33 (Jurisdiction)	Recital 51
	Article 34 (Right to lodge a complaint)	Recital 52
	Article 34a (Representation)	Recital 52a
	Article 35 (Penalties)	Recital 53
	Article 36 (Identification and submission of online child sexual abuse)	Recitals 54-56, 56a
	Article 37 (Cross-border cooperation among Coordinating Authorities)	Recital 57
	Article 38 (Joint investigations)	Recitals 57, 57a
	Article 38a (Mutual assistance)	-
	Article 39 (Cooperation, coordination and information sharing system)	Recitals 58, 60a
4	Article 40 (Establishment and scope of action of the EU Centre)	Recital 59
	Article 41 (Legal status)	Recital 59
	Article 42 (Seat)	Recital 59
	Article 43 (Tasks of the EU Centre)	Recital 60
	Article 44 (Databases of indicators)	Recital 61
	Article 45 (Database of reports)	Recitals 62-63
	Article 46 (Access, accuracy and security)	Recitals 64, 64a
	Article 47 (Delegated acts related to the databases)	Recital 64
	Articles 48 (Reporting)	Recital 65
	Article 49 (Searches and notifications)	Recital 66
	Article 50 (Technologies, information and expertise)	Recital 67
	Article 51 (Processing activities and data protection)	Recital 68
	Article 52 (Contact officers)	Recitals 69-71a
	Article 53 (Cooperation with Europol)	Recitals 69-71a
	Article 53a (Cooperation with other Union agencies and bodies)	
	Article 54 (Cooperation with partner organisations)	Recitals 69-71a
	Article 54a (Cooperation with third countries and international organisations)	
	Article 55 (Administrative and management structure)	Recitals 73
	Article 56 (Composition of the Management Board)	-

Correlation table		
Chapters	**Articles**	**Recitals**
	Article 57 (Functions of the Management Board)	-
	Article 58 (Chairperson of the Management Board)	-
	Article 59 (Meetings of the Management Board)	-
	Article 60 (Voting rules of the Management Board)	-
	Article 64 (Responsibilities of the Executive Director)	-
	Article 65 (Executive Director)	-
	Article 66 (Establishment and tasks of the Technology Committee)	Recital 74
	Article 66a (Appointment and tasks of the Victims Board)	Recital 74a
	Article 67 (Establishment of the budget)	ANNEX to the Legislative Financial Statement
	Article 68 (Structure of the budget)	ANNEX to the Legislative Financial Statement
	Article 69 (Presentation of accounts and discharge)	ANNEX to the Legislative Financial Statement
	Article 70 (Financial rules)	ANNEX to the Legislative Financial Statement
	Article 71 (General Provisions)	ANNEX to the Legislative Financial Statement
	Article 72 (Seconded national experts and other staff)	-
	Article 73 (Privileges and immunities)	-
	Article 74 (Obligation of professional secrecy)	-
	Article 75 (Security rules on the protection of classified and sensitive non-classified information	-
	Article 76 (Language arrangements)	-
	Article 77 (Transparency and communication)	-
	Article 78 (Anti-fraud measures)	ANNEX to the Legislative Financial Statement
	Article 79 (Liability)	-
	Article 80 (Administrative inquires)	-
	Article 81 (Headquarters Agreement and operating conditions)	-
	Article 82 (Start of the EU Centre's activities)	-
5	Article 83 (Data collection)	-
	Article 84 (Transparency reporting)	-
6	Article 85 (Evaluation)	Recitals 75-77a
	Article 86 (Exercise of the delegation)	-
	Article 87 (Committee procedure)	Recitals 79-82
	Article 88 (Amendment of Regulation (EU) 2021/1232)	Recital 78
	Article 89 (Entry into force and application)	Recital 78a