EDPB-EDPS

Joint Opinion 4/2022

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

Adopted on 28 July 2022

TABLE OF CONTENTS

Executive Summary

On 11 May 2022, the European Commission published a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.

The Proposal would impose qualified obligations on providers of hosting services, interpersonal communication services and other services concerning the detection, reporting, removing and blocking of known and new online child sexual abuse material, as well as solicitation of children. The Proposal also provides for the establishment of a new, decentralised EU agency (the 'EU Centre') and a network of national Coordinating Authorities for child sexual abuse issues to enable the implementation of the proposed Regulation. As acknowledged in the Explanatory Memorandum to the Proposal, the measures contained in the Proposal would affect the exercise of the fundamental rights of the users of the services at issue.

Sexual abuse of children is a particularly serious and heinous crime and the objective of enabling effective action to combat it amounts to an objective of general interest recognised by the Union and seeks to protect the rights and freedoms of victims. At the same time, the EDPB and EDPS recall that any limitations of fundamental rights, such as the ones that are envisaged by the Proposal, must comply with the requirements set out in Article 52(1) of the Charter of Fundamental Rights of the European Union.

The EDPB and EDPS stress that the Proposal raises serious concerns regarding the proportionality of the envisaged interference and limitations to the protection of the fundamental rights to privacy and the protection of personal data. In that regard, the EDPB and EDPS point out that procedural safeguards can never fully replace substantive safeguards. A complex system of escalation from risk assessment and mitigation measures to a detection order cannot replace the required clarity of the substantive obligations.

The EDPB and EDPS consider that the Proposal lacks clarity on key elements, such as the notions of "significant risk". Furthermore, the entities in charge of applying those safeguards, starting with private operators and ending with administrative and/or judicial authorities, enjoy a very broad margin of appreciation, which leads to legal uncertainty on how to balance the rights at stake in each individual case. The EDPB and EDPS stress that the legislator must, when allowing for particularly serious interferences with fundamental rights provide legal clarity on when and where interferences are allowed. While acknowledging that the legislation cannot be too prescriptive and must leave some flexibility in its practical application, the EDPB and EDPS consider that the Proposal leaves too much room for potential abuse due to the absence of clear substantive norms.

As regards the necessity and proportionality of the envisaged detection measures, the EDPB and EDPS are particularly concerned when it comes to measures envisaged for the detection of unknown child sexual abuse material ('CSAM') and solicitation of children ('grooming') in interpersonal communication services. Due to their intrusiveness, their probabilistic nature and the error rates associated with such technologies, the EDPB and EDPS consider that the interference created by these measures goes beyond what is necessary and proportionate. Moreover, measures permitting the public authorities to have access on a generalised basis to the content of a communication in order to detect solicitation of children are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter. Therefore, the relevant provisions related to grooming should be removed from the Proposal. In addition, the Proposal does not exclude from its scope of application the scanning of audio communications. The EDPB and EDPS believe that the scanning of audio communications is particularly intrusive and as such must remain outside the scope of the detection

obligations set out in the proposed Regulation, both with respect to voice messages and live communications.

The EDPB and EDPS also express doubts regarding the efficiency of blocking measures and consider that requiring providers of internet services to decrypt online communications in order to block those concerning CSAM would be disproportionate.

Furthermore, the EDPB and EDPS point out that encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide. Recital 26 of the Proposal places not only the choice of detection technologies, but also of the technical measures to protect confidentiality of communications, such as encryption, under a caveat that this technological choice must meet the requirements of the proposed Regulation, i.e., it must enable detection. This supports the notion gained from Articles 8(3) and 10(2) of the Proposal that a provider cannot refuse execution of a detection order based on technical impossibility. The EDPB and EDPS consider that there should be a better balance between the societal need to have secure and private communication channels and to fight their abuse. It should be clearly stated in the Proposal that nothing in the proposed Regulation should be interpreted as prohibiting or weakening encryption.

While the EDPB and EDPS welcome the statement in the Proposal stipulating that it does not affect the powers and competences of the data protection authorities under the GDPR, the EDPB and EDPS are of the view that the relationship between the tasks of Coordinating Authorities and those of data protection authorities should nevertheless be better regulated. In this respect, the EDPB and EDPS appreciate the role that the Proposal assigns to the EDPB in requiring its involvement in the practical implementation of the Proposal, in particular the need for the EDPB to issue an opinion on the technologies the EU Centre would make available in order to execute detection orders. It should, however, be clarified what purpose the opinion would serve in the process and how the EU Centre would act after having received an opinion from the EDPB.

Lastly, the EDPB and EDPS note that the Proposal envisages close cooperation between the EU Centre and Europol, which should provide each other with 'the fullest possible access to relevant information systems'. While the EDPB and EDPS, in principle, support the cooperation of the two agencies, given that the EU Centre is not a law enforcement authority, the EDPB and EDPS still make several recommendations for improvement of the relevant provisions, including that the transmission of personal data between the EU Centre and Europol only takes place on a case-by-case basis, following a duly assessed request, via a secure exchange communication tool, such as the SIENA network.

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR'),[1]

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[2]

Having regard to the European Commission's request for a joint opinion of the European Data Protection Board and the European Data Protection Supervisor of 12 May 2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse,[3]

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1. BACKGROUND

1. On 11 May 2022, the European Commission ('Commission') published a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (the 'Proposal' or 'proposed Regulation').[4]

2. The Proposal was issued following the adoption of Regulation (EU) 2021/1232 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 (the 'Interim Regulation')[5]. The Interim Regulation does not require the relevant service providers to put in place measures to detect child sexual abuse material ('CSAM') (e.g., pictures, videos, etc.) or solicitation of children (also known as 'grooming') on their services, but allows these providers to do so on a voluntary basis, in accordance with the conditions set out in that Regulation.[6]

[1] OJ L 295, 21.11.2018, p. 39.
[2] References to 'Member States' made throughout this document should be understood as references to 'EEA Member States'.
[3] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final.
[4] Ibid
[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 OJ [2021] L 274/41.
[6] See also EDPS, Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online (10 November 2020).

3. The Proposal consists of two main building blocks. First, it imposes qualified obligations on providers of hosting services, interpersonal communication services and other services concerning the detection, reporting, removing and blocking of known and new online child sexual abuse material, as well as solicitation of children. Secondly, the Proposal provides for the establishment a new decentralised EU agency ('EU Centre on Child Sexual Abuse' or 'EU Centre') and a network of national Coordinating Authorities for child sexual abuse issues, to enable the implementation of the proposed Regulation. [7]

4. As acknowledged in the Explanatory Memorandum to the Proposal, the measures contained in the Proposal would affect the exercise of the fundamental rights of the users of the services at issue. Those rights include, in particular, the fundamental rights to respect for privacy (including confidentiality of communications, as part of the broader right to respect for private and family life), protection of personal data and freedom of expression and information. [8]

5. Moreover, such proposed measures are intended to build on and to a certain extent complement existing EU data protection and privacy legislation. In this regard, the Explanatory Memorandum notes that:

> 'The proposal builds on the General Data Protection Regulation (GDPR). In practice, providers tend to invoke various grounds for processing provided for in the GDPR to carry out the processing of personal data inherent in voluntary detection and reporting of child sexual abuse online. The proposal sets out a system of targeted detection orders and specifies the conditions for detection, providing greater legal certainty for those activities. As regards the mandatory detection activities involving processing of personal data, the proposal, in particular the detection orders issued on the basis thereof, thus establishes the ground for such processing referred to in Article 6(1)(c) GDPR, which provides for the processing of personal data that is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject.
>
> The proposal covers, inter alia, providers that offer interpersonal electronic communications services and hence are subject to national provisions implementing the ePrivacy Directive and its proposed revision currently in negotiations. The measures set out in the proposal restrict in some respects the scope of the rights and obligations under the relevant provisions of that Directive, namely, in relation to activities that are strictly necessary to execute detection orders. In this regard, the proposal involves the application, by analogy, of Article 15(1) of that Directive.' [9]

6. Given the severity of the envisaged interferences with fundamental rights, the Proposal has particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data. Thus, on 12 May 2022, the Commission decided to consult the European Data Protection Board ('EDPB') and the European Data Protection Supervisor ('EDPS') in accordance with Article 42(2) of the EUDPR.

2. SCOPE OF THE OPINION

[7] COM(2022)209 final, p. 17.
[8] COM(2022)209 final, p. 12.
[9] COM(2022)209 final, pp. 4-5.

7. The present joint opinion sets out the common views of the EDPB and EDPS on the Proposal. It is limited to the aspects of the Proposal relating to the protection of privacy and personal data. In particular, the joint opinion points out the areas where the Proposal fails to ensure sufficient protection of the fundamental rights to privacy and data protection or requires further alignment with the EU legal framework on the protection of privacy and personal data.

8. As further explained in this joint opinion, the Proposal raises serious concerns regarding the necessity and proportionality of the envisaged interferences and limitations to the protection of the fundamental rights to privacy and the protection of personal data. However, the aim of the present joint opinion is neither to provide an exhaustive list of all of the privacy and data protection issues raised by the Proposal nor to provide specific suggestions for improving the wording of the Proposal. Instead, this joint opinion sets out high-level comments on the main issues raised by the Proposal identified by the EDPB and EDPS. Nonetheless, the EDPB and EDPS remain available to provide further comments and recommendations to the co-legislators during the legislative process on the Proposal.

3. GENERAL COMMENTS ON THE RIGHTS TO CONFIDENTIALITY OF COMMUNICATIONS AND TO THE PROTECTION OF PERSONAL DATA

9. Confidentiality of communications is an essential element of the fundamental right to respect for private and family life, as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union ('Charter'). [10] In addition, Article 8 of the Charter recognizes a fundamental right to the protection of personal data. The rights to confidentiality of communications and the right to private and family life are also guaranteed in Article 8 of the European Convention on Human Rights ('ECHR'), and form part of the constitutional traditions common to the Member States. [11]

10. The EDPB and EDPS recall that the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society. [12] Child sexual abuse is a particularly serious and heinous crime and the objective of enabling effective action to combat it amounts to an objective of general interest recognised by the Union and seeks to protect the rights and freedoms of victims. As regards effective action to combat criminal offences committed against minors and other vulnerable persons, the Court of Justice of the European Union ('CJEU') has pointed out that positive obligations may result from Article 7 of the Charter, requiring public authorities to adopt legal measures to protect private and family life, home and communications. Such obligations may also arise from Articles 3 and 4 of the Charter, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment. [13]

---

[10] See e.g. Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications (25 May 2018).

[11] Almost all European constitutions include a right protecting the confidentiality of communications. See e.g. Article 15 of the Constitution of the Italian Republic; Article 10 of the Basic Law for the Federal Republic of Germany; Article 22 of the Belgian Constitution; and Article 13 of the Constitution of the Kingdom of the Netherlands.

[12] See, inter alia, judgment of the CJEU, Case C-311/18, *Facebook Ireland and Schrems*, para. 172 and case-law cited therein. See also Recital 4 GDPR.

[13] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, paras. 126-128. See also EDPS Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online (10 November 2020), para. 12.

11. At the same time, any limitations of the rights guaranteed by the Charter, such as the ones that are envisaged by the Proposal,[14] must comply with the requirements set out in Article 52(1) of the Charter. Any measure interfering with the rights to confidentiality of communications and the right to private and family life must first of all respect the essence of the rights at hand.[15] The essence of a right is affected if the right is emptied of its basic content and the individual cannot exercise it[16]. The interference may not constitute, in relation to the aim pursued, such a disproportionate and intolerable interference, impairing the very substance of the right so guaranteed.[17] This means that even a fundamental right that is not absolute in nature, such as the right to confidentiality of communications and the right to the protection of personal data, has some core components that may not be limited.

12. The CJEU has on several occasions applied the 'essence of a right' test in the area of privacy of electronic communications. In *Tele2 Sverige and Watson*, the Court ruled that legislation which does not permit retention of the content of a communication is not such as to adversely affect the essence of the rights to private life and to the protection of personal data.[18] In *Schrems*, the Court found that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[19] In *Digital Rights Ireland and Seitlinger and Others*, the Court found that even though the retention of data required by Directive 2006/24 constituted a particularly serious interference with the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it was not such as to adversely affect the essence of those rights given that the Directive did not permit the acquisition of knowledge of the content of the electronic communications as such.[20] From this case law it may be inferred that measures permitting the public authorities to have access on a generalised basis to the content of a communication are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter. These considerations are equally relevant also with respect to measures for the detection of CSAM and solicitation of children, like the ones envisaged by the Proposal.

13. Furthermore, the CJEU has found that data security measures play a key role to ensure that the essence of the fundamental right to the protection of personal data in Article 8 of the Charter is not adversely affected.[21] In the digital age, technical solutions to secure and protect the confidentiality of electronic communications, including measures for encryption, are key to ensure the enjoyment of all fundamental rights.[22] This should be given due consideration when assessing measures for the

[14] Cf. COM(2022)209 final, pp. 12-13.
[15] Article 52(1) of the Charter.
[16] See EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), p. 8, available at https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.
[17] CJEU, Case C-393/19, *OM*, para. 53.
[18] CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, para. 101.
[19] CJEU, Case C-362/14, *Schrems*, para. 94.
[20] CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, para. 39.
[21] Ibid., para. 40.
[22] See Human Rights Council, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/RES/47/16 (26 July 2021).

mandatory detection of CSAM or solicitation of children, in particular if they would result in the weakening or degrading of encryption.[23]

14. Article 52(1) of the Charter also provides that any limitation on the exercise of a fundamental right guaranteed in the Charter must be provided for by law. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[24] In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that their data will be effectively protected against the risk of abuse.[25] That legislation must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[26] As clarified by the CJEU, the need for such safeguards is all the greater where personal data is subjected to automated processing and where the protection of the particular category of personal data that is sensitive data is at stake.[27]

15. The Proposal would limit the exercise of the rights and obligations provided for in Articles 5(1) and (3) and 6(1) of Directive 2002/58/EC ('e-Privacy Directive')[28] insofar as necessary for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 of the Proposal. The EDPB and EDPS consider that it is therefore necessary to assess the Proposal not only in light of the Charter and the GDPR, but also in the light of Articles 5, 6 and 15(1) of the e-Privacy Directive.

[23] See also Recital 25 of the Interim Regulation.
[24] See "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11 April 2019, available at https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, para. 132.
[26] Ibid.
[27] Ibid.
[28] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2006/24/EC and Directive 2009/136/EC.

4. SPECIFIC COMMENTS

4.1 Relationship with existing legislation

4.1.1 Relationship with the GDPR and ePrivacy Directive

16. The Proposal states that it is without prejudice to the rules resulting from other Union acts, in particular the GDPR[29] and the e-Privacy Directive. Contrary to the Interim Regulation, the Proposal does not provide for an explicit temporary derogation from, but for a limitation of the exercise of the rights and obligations laid down in Articles 5(1), 5(3) and 6(1) of the e-Privacy Directive. Further, it should be noted that the Interim Regulation provides for a derogation exclusively from the provisions in Articles 5(1) and 6(1), and not from Article 5(3) of the e-Privacy Directive.

17. The Proposal further refers to Article 15(1) of the e-Privacy Directive allowing Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5 and 6 of that Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences. According to the Proposal, Article 15(1) of the e-Privacy Directive is applied by analogy where the Proposal limits the exercise of the rights and obligations provided for in Articles 5(1), 5(3) and 6(1) of the e-Privacy Directive.

18. The EDPB and EDPS recall that the CJEU has made it clear that Article 15(1) of the e-Privacy Directive is to be interpreted strictly, meaning that the exception to the principle of confidentiality of communications that Article 15(1) allows must remain an exception and must not become the rule.[30] As outlined further on in the present joint opinion, the EDPB and EDPS consider that the Proposal does not satisfy the requirements of (strict) necessity, effectiveness and proportionality. Moreover, the EDPB and EDPS conclude that the Proposal would entail that the interference with confidentiality of communications may in fact become the rule rather than remain the exception.

4.1.2 Relationship with Regulation (EU) 2021/1232 and impact on voluntary detection of child sexual abuse online

19. Pursuant to Article 88 of the Proposal, the latter would repeal the Interim Regulation, which provides for a temporary derogation from certain provisions of the e-Privacy Directive to enable the voluntary use of technologies for the detection of CSAM and solicitation of children by providers of number-independent interpersonal communications services. Thus, from the date of application of the proposed Regulation, there would be no derogation from the e-Privacy Directive that would allow the voluntary detection of child sexual abuse online by such providers.

20. Given that the detection obligations introduced by the Proposal would apply only to recipients of detection orders, it would be important to make clear in the text of the proposed Regulation that the voluntary use of technologies for the detection of CSAM and solicitation of children remains permitted only inasmuch as it is allowed under the e-Privacy Directive and GDPR. This would entail, for instance,

---

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119, 4.5.2016, p. 1–88).

[30] Judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson*, para. 89.

that providers of number-independent interpersonal communications services would be prevented from using such technologies on a voluntary basis, unless this would be permitted under the national laws transposing the e-Privacy Directive, in accordance with Article 15(1) of the e-Privacy Directive and the Charter.

21. More generally, the proposed Regulation would benefit from further clarity regarding the status of the voluntary detection of child sexual abuse online after the date of application of the proposed Regulation, and on the transition from the voluntary detection regime set out in the Interim Regulation to the detection obligations set out in the proposed Regulation. For instance, the EDPB and EDPS recommend making clear that the proposed Regulation would not provide for a lawful basis for the processing of personal data for the sole purpose of detecting online child sexual abuse on a voluntary basis.

4.2 Lawful basis under the GDPR

22. The Proposal aims to establish a lawful basis, within the meaning of the GDPR, for the processing of personal data for CSAM and grooming detection. Accordingly, the Explanatory Memorandum notes: 'As regards the mandatory detection activities involving processing of personal data, the proposal, in particular the detection orders issued on the basis thereof, thus establishes the ground for such processing referred to in Article 6(1)(c) GDPR, which provides for the processing of personal data that is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject'.[31]

23. The EDPB and EDPS welcome the decision of the Commission to eliminate legal uncertainty as to the legal basis of the processing of personal data, which has arisen under the Interim Regulation. The EDPB and EDPS also agree with the Commission's conclusion that the consequences of the deployment of detection measures are too far-reaching and serious to leave the decision on whether to implement such measures to the service providers.[32] At the same time, the EDPB and EDPS note that any legal basis obliging service providers to interfere with the fundamental rights to data protection and privacy will only be valid insofar as it respects the conditions set out in Article 52(1) of the Charter, as analysed in the following sections.

4.3 Risk assessment and mitigation obligations

24. Under Chapter II, Section 1 of the Proposal, providers of hosting services and providers of interpersonal communications services are required to identify, analyse and assess, for each such service that they offer, the risk of use of the service for the purpose of online child sexual abuse, and then try to minimise the identified risk by applying 'reasonable mitigation measures, tailored to the risk identified'.

25. The EDPB and EDPS note that when carrying out a risk assessment, the provider should take into account in particular the elements listed in Article 3(2)(a) to (e) of the Proposal, including: prohibitions and restrictions laid down in the terms and conditions of the provider; the manner in which users use the service and the impact thereof on that risk; the manner in which the provider designed and operates the service, including the business model, governance and relevant systems and processes, and the impact thereof on that risk. With respect to the risk of solicitation of children, the proposed elements to be considered are: the extent to which the service is used or is likely to be used by

[31] Ibid, p. 4.
[32] Cf. Proposal, COM(2022)209 final, p. 14.

children; the age groups and the risk of solicitation by age group; the availability of functionalities enabling a user search, functionalities enabling users to establish contact with other users directly, in particular through private communications and functionalities enabling users to share images or videos with other users.

26. While the EDPB and EDPS acknowledge that these criteria seem relevant, the EDPB and EDPS are nevertheless concerned that such criteria leave a rather broad margin for interpretation and appreciation. Several criteria are described in highly generic terms (e.g. 'the manner in which users use the service and the impact thereof on that risk') or relate to basic functionalities that are common to many online services (e.g. 'enabling users to share images or videos with other users'). As such, the criteria appear prone to a subjective (rather than objective) assessment.

27. In the view of the EDPB and EDPS, the same holds true for the risk mitigation measures to be taken pursuant to Article 4 of the Proposal. Measures like adapting, through appropriate technical and operational measures and staffing, the provider's content moderation or recommender systems seem relevant to reduce the identified risk. However, if applied within a complex risk assessment process and combined with abstract and vague terms to describe the acceptable amount of risk (e.g. 'appreciable extent'), these criteria do not meet the legal certainty and foreseeability criteria needed to justify an interference with the confidentiality of communications between private individuals which constitutes a clear interference with the fundamental rights to privacy and freedom of expression.

28. While providers are not authorised to interfere with the confidentiality of communications as part of their risk assessment and mitigation strategies prior to receiving a detection order, a direct connection exists between the risk assessment and mitigation obligations and the ensuing detection obligations. Article 7(4) of the Proposal makes the issuance of a detection order dependent on the existence of evidence of a significant risk that the relevant service could be used for the purpose of online child sexual abuse. Before a detection order is issued, a complex process involving providers, the Coordinating Authority and the judicial or other independent administrative authority responsible for issuing the order must be followed. First, providers must assess the risk of use of their services for the purpose of online child sexual abuse (Article 3 of the Proposal) and evaluate possible risk mitigation measures (Article 4 of the Proposal) to reduce that risk. The results of this exercise are then to be reported to the competent Coordinating Authority (Article 5 of the Proposal). If the risk assessment shows that a significant risk remains despite the efforts to mitigate it, the Coordinating Authority shall hear the provider on a draft request for the issuance of a detection order and shall give the provider the possibility to provide comments. The provider is further obliged to present an implementation plan, including an opinion from the competent data protection authority in the case of grooming detection. If the Coordinating Authority pursues the case, a detection order is sought and eventually issued by a court or other independent administrative authority. Therefore, the initial risk assessment and the measures chosen to reduce the risk identified are a decisive basis for the assessment by the Coordinating Authority, as well as by the competent judicial or administrative authority, of whether a detection order is necessary.

29. The EDPB and EDPS take note of the complex steps leading to the issuance of a detection order, which include an initial risk assessment by the provider and the provider's proposal of risk mitigation measures, as well as the further interaction of the provider with the competent Coordinating Authority. The EDPB and EDPS consider that there is a substantial possibility for the provider to influence the outcome of the process. In this regard, the EDPB and EDPS note that Recital 17 of the Proposal stipulates that providers should be able to indicate, as part the risk reporting, 'their willingness and preparedness' to eventually being issued a detection order. Therefore, it cannot be

assumed that each and every provider will seek to avoid the issuance of a detection order in order to preserve the confidentiality of communications of its users by applying the most effective, but least intrusive mitigation measures, especially where such mitigation measures interfere with the provider's freedom to conduct a business according to Article 16 of the Charter.

30. The EDPS and EDPB would like to stress that procedural safeguards can never fully replace substantive safeguards. Thus, the complex process leading to the possible issuance of a detection order described above should be accompanied by clear substantive obligations. The EDPB and EDPS consider that the Proposal lacks clarity on several key elements (e.g. the notions of 'significant risk', 'appreciable extent', etc.), which cannot be remedied by the presence of multiple layers of procedural safeguards. This is all the more relevant in light of the fact that the entities in charge of applying those safeguards (e.g., providers, judicial authorities, etc.) enjoy a wide margin of appreciation on how to balance the rights at stake in each individual case. In view of the extensive interferences with fundamental rights that would stem from the adoption of the Proposal, the legislator should make sure that the Proposal provides more clarity as to when and where such interferences are allowed. While acknowledging that legislative measures cannot be too prescriptive and must leave some flexibility in their practical application, the EDPB and EDPS consider that the current text of the Proposal leaves too much room for potential abuses due to the absence of clear substantive norms.

31. Given the potential significant impact on a very large number of data subjects (i.e., potentially all users of interpersonal communications services), the EDPB and EDPS stress the need of a high level of legal certainty, clarity and foreseeability of the legislation in order to ensure that the proposed measures are genuinely effective in achieving the objective they pursue and at the same time are the least detrimental to the fundamental rights at stake.

4.4 Conditions for the issuance of detection orders

32. Article 7 of the Proposal provides that the Coordinating Authority of establishment will have the power to request the competent judicial authority 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 to take the measures specified in Article 10 to detect online child sexual abuse on a specific service.

33. The EDPB and EDPS take due account of the following elements to be fulfilled prior to the issuance of a detection order:

    a. there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of Article 7, paragraphs 5, 6 or 7, as applicable;

    b. the reasons for issuing the detection order outweigh the 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.

34. The meaning of significant risk is specified at paragraph 5 and following of Article 7, depending on the type of detection order under consideration. Significant risk shall be assumed in the case of detection orders regarding the detection of known CSAM if:

    a. it is likely, despite any mitigation measures that the provider may have taken or will take, that the service is used, to an appreciable extent for the dissemination of known child sexual abuse material; and

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.

35. To issue a detection order for unknown CSAM, the likelihood and the factual evidence need to refer to unknown CSAM, and a prior detection order for known CSAM must have been issued and have led to a significant number of CSAM reports by the provider (Article 7(6) of the Proposal). For a grooming detection order, the significant risk will be deemed to exist where the provider qualifies as a provider of interpersonal communication services, it is likely that the service is used to an appreciable extent for the solicitation of children, and there is evidence of the service having been used to an appreciable extent for the solicitation of children (Article 7(7) of the Proposal).

36. The EDPB and EDPS observe that even with the specifications in Article 7(5)-(7) of the Proposal, the conditions for the issuance of a detection order are dominated by vague legal terms, such as 'appreciable extent', 'significant number', and are in part repetitive, as evidence of former abuse will often contribute to establishing the likelihood of future abuse.

37. The Proposal envisages a system whereby, when deciding whether a detection order is necessary, a predicting decision regarding the future use of a service for the purpose of online child sexual abuse needs to be made. It is therefore understandable that the elements set out in Article 7 have a prognostic character. However, the Proposal's recourse to vague notions make it difficult for providers, as well as for the competent judicial or other independent administrative authority empowered, to apply the legal requirements introduced by the Proposal in a predictable and non-arbitrary manner. The EDPB and EDPS are concerned that these broad and vague notions will result in a lack of legal certainty and will also lead to considerable divergences in the concrete implementation of the Proposal across the Union, depending on the interpretations that will be given to notions such as 'likelihood' and 'appreciable extent' by judicial or other independent administrative authorities in the Member States. Such an outcome would not be acceptable in the light of the fact that the provisions on detection orders for providers of interpersonal communication services will constitute 'limitations' to the principle of confidentiality of communications laid down in Article 5 of the e-Privacy Directive and their clarity and foreseeability is thus of utmost importance to ensure that these limitations are uniformly applied across the Union.

4.5 Analysis of the necessity and proportionality of the envisaged measures[33]

38. As indicated above, there are three types of detection orders that may be issued: detection orders concerning the dissemination of known child sexual abuse material (Article 7(5) of the Proposal), detection orders concerning the dissemination of new child sexual abuse material (Article 7(6) of the Proposal) and detection orders concerning the solicitation of children (Article 7(7) of the Proposal). Each detection order would normally require a different technology for its practical implementation. Consequently, they have different level of intrusiveness and thus different impact on the rights to privacy and personal data protection.

39. Technologies to detect known child sexual abuse material are usually matching technologies in the sense that they rely on an existing database of known CSAM against which they can compare images

[33] See also "The EDPS quick guide to necessity and proportionality", available at: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

(including stills from videos). To enable the matching, the images that the provider is processing as well as the images in the database must have been made digital, typically by converting them into hash values. This kind of hashing technology has an estimated false positives rate of no more than 1 in 50 billion (i.e., 0,000000002% false positive rate). [34]

40. For the detection of new CSAM, a different type of technology is typically used, including classifiers and artificial intelligence (AI). [35] However, their error rates are generally significantly higher. For instance, the Impact Assessment Report indicates that there are technologies for the detection of new CSAM whose precision rate can be set at 99.9% (i.e., 0,1% false positive rate), but with that precision rate they are only able to identify 80% of the total CSAM in the relevant data set. [36]

41. As for the detection of solicitation of children in text-based communications, the Impact Assessment Report explains that this is typically based on pattern detection. The Impact Assessment Report notes that some of the existing technologies for grooming detection have an "accuracy rate" of 88%[37]. According to the Commission, this means that 'out of 100 conversations flagged as possible criminal solicitation of children, 12 can be excluded upon review [according to the Proposal, by the EU Centre] and will not be reported to law enforcement'. [38] However, even though – contrary to the Interim Regulation – the Proposal would apply to audio communications too, the Impact Assessment Report does not elaborate on the technological solutions that could be used to detect grooming in such a setting.

4.5.1 Effectiveness of the detection

42. Necessity implies the need for a fact-based assessment of the effectiveness of the envisaged measures for achieving the objective pursued and of whether it is less intrusive than other options for achieving the same goal. [39] Another factor to be considered in the assessment of proportionality of a proposed measure is the effectiveness of existing measures over and above the proposed one. [40] If measures for the same or a similar purpose already exist, their effectiveness should be assessed as part of the proportionality assessment. Without such an assessment of the effectiveness of existing measures pursuing the same or a similar purpose, the proportionality test for a new measure cannot be considered as having been duly performed.

43. The detection of CSAM or grooming by providers of hosting services and providers of interpersonal communications services is capable of contributing to the overall objective of preventing and combating child sexual abuse and the online dissemination of child sexual abuse material. At the same

[34] See European Commission, Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final (hereinafter 'Impact Assessment Report' or 'SWD(2022) 209 final'), p. 281, fn. 511.
[35] Impact Assessment Report, p. 281.
[36] Ibid, p. 282.
[37] Ibid, p. 283.
[38] Proposal, COM(2022)209 final, p. 14, fn. 32.
[39] EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 5; EDPS, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), p. 8.
[40] EDPS, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), p. 11.

time, the need to assess the effectiveness of the measures provided for in the Proposal triggers three key questions:

- Can the measures to detect child sexual abuse online be easily circumvented?
- What is the effect that the detection activities will have on action taken by law enforcement authorities?[41]
- How would the Proposal reduce legal uncertainty?

44. It is not for the EDPB and EDPS to answer these questions in detail. However, the EDPB and EDPS note that neither the Impact Assessment Report nor the Proposal fully address these questions.

45. As regards the possibility of circumventing CSAM detection, it should be noted that at present there seems to be no technological solution to detect CSAM that is shared in an encrypted form. Therefore, any detection activity – even client-side scanning intended to circumvent end-to-end encryption offered by the provider[42] – can be easily circumvented by encrypting the content with the help of a separate application prior to sending it or uploading it. Thus, the detection measures envisaged by the Proposal might have a smaller impact on the dissemination of CSAM on the Internet than one might hope for.

46. Further, the Commission expects an increase in the numbers of child sexual abuse reports to law enforcement authorities with the adoption of the detection obligations introduced by the Proposal.[43] However, neither the Proposal nor the Impact Assessment Report explain how this will tackle the shortcomings of the current state of play. Given the limited resources of law enforcement authorities, it seems necessary to better understand whether increasing the amount of reports would have a meaningful impact on law enforcement activities against child sexual abuse. In any event, the EDPB and EDPS wish to stress that such reports should be assessed in a timely manner to ensure that a decision on the criminal relevance of the reported material is made as early as possible and to limit the retention of irrelevant data as far as possible.

4.5.2 No less intrusive measure

47. Assuming that the positive effects of CSAM and grooming detection envisaged by the Commission could be realized, the detection needs to be the least intrusive measure of equally effective measures. Article 4 of the Proposal provides that, as a first step, providers should consider the adoption of mitigation measures to reduce the risk of use of their service for the purpose of online child sexual abuse below the threshold that warrants the issuance of a detection order. If there are mitigation measures that could lead to a substantial reduction of the amount of grooming or CSAM exchanged within the relevant service, these measures would often constitute less intrusive measures compared to a detection order[44]. Therefore, should the relevant provider fail to adopt such measures on a voluntary basis, it should be possible for the competent independent administrative authority or judicial authority to make the implementation of mitigation measures mandatory and enforceable

[41] According to the Impact Assessment Report, Annex II, p. 132, 85.71 % of law enforcement survey respondents raised their concerns with regards to the increased number of child sexual abuse material in the last decade and the lack of resources (i.e. human, technical).
[42] See further section 4.10 below.
[43] See, *inter alia,* Impact Assessment Report, Annex 3, SWD(2022) 209 final, p. 176.
[44] For instance, measures like client-side blocking of the transmission of CSAM by preventing uploading and sending of content of the electronic communications could be considered, as they might help in certain contexts to prevent the circulation of known CSAM.

instead of issuing a detection order. In the view of the EDPB and EDPS, the fact that Article 5(4) of the Proposal enables the Coordinating Authority to 'require' the provider to introduce, review, discontinue or expand mitigation measures is not sufficient as such a requirement would not be independently enforceable; failure to comply would only be 'sanctioned' by ordering a detection order.

48. Therefore, the EDPB and EDPS consider that the Coordinating Authority or the competent independent administrative or judicial authority should be explicitly empowered to impose less intrusive mitigation measures prior to or instead of issuing a detection order.

4.5.3 Proportionality in the strict sense

49. For a measure to respect the principle of proportionality enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental rights. Therefore, the principle of proportionality 'restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)'.[45]

50. In order to be able to assess the impact of a measure on the fundamental rights to privacy and to the protection of personal data, it is particularly important to precisely identify: [46]

- the **scope of the measure**, including the number of people affected and whether it raises 'collateral intrusions' (i.e. interference with the privacy of persons other than the subjects of the measure);
- the **extent of the measure**, including the amount of information collected; for how long; whether the measure under scrutiny requires the collection and processing of special categories of data;
- the **level of intrusiveness**, taking into account: the nature of the activity subjected to the measure (whether it affects activities covered by duty of confidentiality or not, lawyer-client relationship; medical activity); the context; whether it amounts to profiling of the individuals concerned or not; whether the processing entails the use of (partially or fully) automated decision-making system with a 'margin of error';
- whether it concerns **vulnerable persons** or not;
- whether it also affects **other fundamental rights** (for instance the right to freedom of expression, as in the *Digital Rights Ireland and Seitlinger and Others* and *Tele2 Sverige and Watson* cases).[47]

---

[45] See Case C-343/09, *Afton Chemical*, para. 45; joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Hartmut Eifert*, para. 74; Cases C-581/10 and C-629/10, *Nelson and Others*, para. 71; Case C-283/11, *Sky Österreich*, para. 50; and Case C-101/12, *Schaible*, para. 29. See further EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (11 April 2017).

[46] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), p. 23.

[47] See also EDPS, Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online (10 November 2020), p. 9 and following.

51. In this context, it is also important to note that the impact can be minor with regard to the individual concerned, but nonetheless significant or highly significant collectively/for society as a whole.[48]

52. In all three types of detection orders (detection of known CSAM, new CSAM, and grooming), the technologies currently available rely on the automated processing of content data of all affected users. The technologies used to analyse the content are often complex, typically involving the use of AI. As a result, the behavior of this technology may not be fully comprehensible for the user of the service. Moreover, the technologies currently available, especially those for detecting new CSAM or grooming, are known to have relatively high error rates.[49] In addition, there is the risk of being reported to the EU Centre in accordance with Articles 12(1) and 48(1) of the Proposal, based on a detection of 'potential' CSAM.

53. Moreover, the general conditions for the issuance of a detection order under the Proposal, i.e. applied to an entire service and not just to selected communications[50], the duration up to 24 months for known or new CSAM and up to 12 months for grooming[51], etc. may lead to a very broad scope of the order in practice. As a result, the monitoring would actually be general and indiscriminate in nature, and not targeted in practice.

54. In light of the above, the EDPB and EDPS are also concerned about the possible chilling effects for the exercise of the freedom of expression. The EDPB and EDPS recall that such chilling effect is deemed more probable the lesser the clarity of the law is.

55. In the absence of the specificity, precision and clarity required in order to satisfy the requirement of legal certainty,[52] and given its wide scope, i.e. all providers of relevant information society services offering such services in the Union,[53] the Proposal does not ensure that only a targeted approach to CSAM and grooming detection will effectively take place. Therefore, the EDPB and EDPS consider that, in practice, the Proposal could become the basis for *de facto* generalized and indiscriminate scanning of the content of virtually all types of electronic communications of all users in the EU/EEA. As a result, the legislation may lead people to refrain from sharing legal content out of fear that they could be targeted based on their action.

56. That being said, the EDPB and EDPS recognise that different measures to combat child sexual abuse online may involve different levels of intrusiveness. As a preliminary matter, the EDPB and EDPS observe that the automated analysis of speech or text with a view of identifying potential instances of solicitation of children is likely to constitute a more significant interference than the matching of images or videos on the basis of previously confirmed instances of CSAM in view of detecting dissemination of CSAM. Furthermore, a distinction should be made between the detection of 'known CSAM' and of 'new CSAM'. In addition, the impact should be further differentiated between the measures addressed to providers of hosting services and those imposed on providers of inter-personal communications services.

---

[48] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), p. 20.
[49] See details above, section 4.5, and below, subsection 4.8.2.
[50] See Article 7(1) of the Proposal.
[51] See Article 7(9), third subparagraph of the Proposal.
[52] Cf. CJEU, Case C-197/96, *Commission of the European Communities v French Republic*, para. 15.
[53] See Article 1(2) of the Proposal.

4.5.4 Detection of known child sexual abuse material

57. While according to Recital 4, the Proposal would be 'technology-neutral', both the effectiveness of the proposed detection measures and their impact on individuals will depend very much on the choice of the applied technology and on the selected indicators. This fact is acknowledged by the Commission in the Impact Assessment Report, Annex 8,[54] and confirmed by other studies, such as the European Parliamentary Research Service's targeted substitute impact assessment on the Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse from February 2021.[55]

58. Article 10 of the Proposal lays down a number of requirements for the technologies to be used for detection purposes, in particular concerning their effectiveness, reliability and least intrusive nature in terms of impact on the users' rights to private and family life, including the confidentiality of communications, and to protection of personal data.

59. In this context, the EDPB and EDPS note that, currently, the only technologies which appear to be able to meet generally these standards, are those used to detect known CSAM, i.e. matching technologies relying on a database of hashes as a reference.

4.5.5 Detection of previously unknown child sexual abuse material

60. The assessment of the measures aimed at detection of previously unknown (new) CSAM leads to different conclusions regarding their effectiveness, reliability and limitation of the impact on the fundamental rights to privacy and data protection.

61. First, as explained in the Impact Assessment Report to the Proposal, the technologies currently used for the detection of previously unknown CSAM include classifiers and AI. A classifier is any algorithm that sorts data into labelled classes, or categories of information, through pattern recognition.[56] Thus, these technologies have different results and impact in terms of accuracy, effectiveness, and level of intrusiveness. At the same time, they are also more prone to errors.

62. The techniques used in order to detect previously unknown CSAM are similar to the ones used to detect solicitation of children, as both are based not on simple matching technologies, but on predictive models, employing AI technologies. The EDPB and EDPS consider that a high level of caution should be taken when detecting previously unknown CSAM, as an error of the system would have severe consequences for data subjects, who would be automatically flagged as having possibly committed a very serious crime and have their personal data and details of their communications reported.

63. Secondly, the performance indicators found in the literature, some of which are highlighted in the Impact Assessment Report that accompanied the Proposal,[57] provide very little information on the conditions that were used for their computation and their adequacy with real life conditions, meaning

[54] Cf. information on the false positives rates in the Impact Assessment Report, Annex 8, p. 279 and following.
[55] Cf. Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment (European Parliamentary Research Service, February 2021), p. 14 and following.
[56] Impact Assessment Report, Annex 8, p. 281.
[57] Impact Assessment Report, Annex 8, pp. 281-283.

that their real-world performance could be significantly lower than what is expected, leading to less accuracy and a higher percentage of 'false positives'.

64. Thirdly, performance indicators should be considered in the specific context of use of the relevant detection tools and provide an exhaustive insight into the behavior of the detection tools. When using artificial intelligence algorithms on images or text, it is well documented that bias and discrimination can occur due to the lack of representativeness of certain population groups in the data used to train the algorithm. These biases should be identified, measured and reduced to an acceptable level in order for the detection systems to be truly beneficial to society as a whole.

65. Although a study of the technologies used for detection has been carried out,[58] the EDPB and EDPS consider that further analysis is necessary in order to assess the reliability of the existing tools. This analysis should rely on exhaustive performance indicators and assess the impact of potential errors in real life conditions for all data subjects concerned by the Proposal.

66. As noted above, the EDPB and EDPS have serious doubts as to what extent the procedural safeguards provided for in Article 7(6) of the Proposal are sufficient to compensate these risks. Moreover, as indicated earlier, they note that the Proposal uses rather abstract and vague terms to describe the acceptable amount of risk (e.g. 'appreciable extent').

67. The EDPB and EDPS are concerned that these broad and vague notions will result in a lack of legal certainty and will also provoke strong divergences in the concrete implementation of the Proposal across the Union, depending on the interpretations that will be given to notions such as 'likelihood' and 'appreciable extent' by judicial or other independent administrative authorities in the Member States. This is worrying also in light of the fact that the provisions on detection orders will constitute 'limitations' to the principle of confidentiality laid down in Article 5 of the e-Privacy Directive. Thus, their clarity and foreseeability need to be improved in the proposed Regulation.

4.5.6 Detection of solicitation of children ('grooming')

68. The EDPB and EDPS observe that the proposed measures concerning detection of solicitation of children ('grooming'), entailing automated analysis of speech or text, are likely to constitute the most significant interference on the users' rights to private and family life, including the confidentiality of communications, and to protection of personal data.

69. While the detection of known and even new CSAM can be limited in scope to the analysis of images and videos, grooming detection would extend by definition to all text-based (and possibly audio) communications that fall within the scope of a detection order. As a result, the intensity of the interference with the confidentiality of communications concerned is much greater.

70. The EDPB and EDPS consider that *de facto* general and indiscriminate automated analysis of text-based communications transmitted through interpersonal communications services with a view of identifying potential solicitation of children does not respect the requirements of necessity and proportionality. Even if the technology used is limited to the use of indicators, the EDPB and EDPS consider that the deployment of such general and indiscriminate analysis is excessive and may even affect the very core of the fundamental right to privacy enshrined in Article 7 of the Charter.

71. As already stated, the lack of substantive safeguards in the context of the measures for detection of solicitation of children cannot be compensated solely by procedural safeguards. Moreover, the

[58] Impact Assessment Report, pp. 279 et seq.

problem of the lack of sufficient legal clarity and certainty (e.g. the use of vague legal language like 'appreciable extent') is even more serious in the case of automated analysis of text-based personal communications, as compared to photo comparison based on hashing technology.

72. Furthermore, the EDPB and EDPS consider that the 'chilling effect' on freedom of expression is particularly significant when individuals' text (or audio) communications are being scanned and analysed on a large scale. The EDPB and EDPS recall that such chilling effect is the more severe the lesser the clarity of the law is.

73. In addition, as indicated in the Impact Assessment Report[59] and in the European Parliamentary Research Service's study[60] the accuracy rate of technologies for detection of text-based grooming is much lower than the accuracy rate of technologies for the detection of known CSAM[61]. Grooming-detection techniques are designed to analyse and assign probability ratings to each aspect of the conversation, therefore the EDPB and EDPS also consider them prone to errors and vulnerable to abuse.

4.5.7 Conclusion on the necessity and proportionality of the envisaged measures

74. As regards the necessity and proportionality of the envisaged detection measures, the EDPB and EDPS are particularly concerned as regards measures envisaged for the detection of unknown CSAM and solicitation of children (grooming), due to their intrusiveness because of potential granting of access to content of communications on a generalised basis, their probabilistic nature and the error rates associated with such technologies.

75. Moreover, from the case law of the CJEU it may be inferred that measures permitting the public authorities to have access on a generalised basis to the content of a communication are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter. These considerations are specifically relevant with respect to measures for the detection of solicitation of children envisaged by the Proposal.

76. In any event, the EDPB and EDPS consider that the interference created in particular by the measures for the detection of solicitation of children goes beyond what is strictly necessary and proportionate. These measures should therefore be removed from the Proposal.

4.6 Reporting obligations

77. The EDPB and EDPS recommend to complement the list of specific reporting requirements in Article 13 of the Proposal with a requirement to include in the report information on the specific technology that enabled the provider to become aware of the relevant abusive content, in case the provider became aware of the potential child sexual abuse following measures taken to execute a detection order issued in accordance with Article 7 of the Proposal.

[59] Impact Assessment Report, Annex 8, p. 281-283.
[60] p. 15-18.
[61] See above, para. 40.

4.7 Removal and blocking obligations

78. One of the measures envisaged by the Proposal for mitigating the risks of dissemination of CSAM is the issuance of removal and blocking orders which would oblige providers to remove or disable access to, or to block online child sexual abuse material.[62]

79. While the impact of removal orders on data protection and the privacy of communications is relatively limited, as a general remark, the EDPB and EDPS recall the overarching principle to be complied with, that any such measure should be as targeted as possible.

80. At the same time, the EDPB and EDPS draw the attention on the fact that internet access service providers have only access to the precise URL of content if this content is made available in clear text. Every time content is made accessible via HTTPS, the internet access service provider will not have access to the precise URL, unless it breaks the encryption of the communication. Therefore, the EDPB and EDPS have doubts regarding the efficiency of blocking measures, and consider that requiring providers of internet access services to decrypt online communications to block those concerning CSAM would be disproportionate.

81. Moreover and more generally, it should be noted that blocking (or disabling) access to a digital item is an operation that takes place at network level and its implementation may prove ineffective, in case of multiple (possibly similar and not identical) copies of the same item. Further, such operation may prove disproportionate, if the blocking affects other, not illegal, digital items when they are stored in the same server made inaccessible using network commands (e.g. IP address or DNS blacklisting). In addition, not all network-level approaches to blocking are equally effective, and some may be easily circumvented with rather basic technical skills.

82. Finally, the powers of Coordinating Authorities with respect to the issuance of blocking orders should be clarified in the proposed Regulation. For instance, from the current wording of Articles 16(1) and 17(1), it is unclear whether Coordinating Authorities are empowered to issue or only to request the issuance of blocking orders.[63]

4.8 Relevant technologies and safeguards

4.8.1 Data protection by design and by default

83. The Proposal's requirements that apply to the technologies to be deployed for the detection of CSAM and solicitation of children do not appear to be sufficiently stringent. In particular, the EDPB and EDPS have noted that – contrary to the analogous provisions in the Interim Regulation[64] – the Proposal does not make any express reference to the principle of data protection by design and by default, and does not provide that technologies that are used to scan text in communications must not be able to deduce the substance of the content of the communications. The Proposal simply provides in Article 10(3)(b) that the technologies must not be able to 'extract' any other information from the relevant

[62] Proposal, Arts. 14 and 16.
[63] Article 16(1) of the Proposal reads 'The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State to issue a blocking order […]', whereas Article 17(1) reads 'The Coordinating Authority of establishment shall issue the blocking orders referred to in Article 16 […]' (emphasis added).
[64] Interim Regulation, Art. 3(1)(b).

communications than the information strictly necessary to detect. However, this standard does not appear to be sufficiently stringent, as it might be possible to *deduce* other information from the substance of the content of a communication without *extracting* information from it as such.

84. Consequently, the EDPS and the EDPB recommend to introduce in the Proposal a Recital that stipulates that the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 applies to the technologies regulated by Article 10 of the Proposal by virtue of law and therefore had not to be repeated in the legal text. In addition, Article 10(3)(b) should be amended to ensure that not only no other information is extracted, but also not deduced, as it is currently provided for by Article 3(1)(b) of the interim Regulation.

4.8.2 Reliability of the technologies

85. The Proposal assumes that several kinds of technological solutions may be used by service providers to execute detection orders. In particular, the Proposal assumes that artificial intelligence systems are available and working for the detection of unknown CSAM and for the detection of solicitation of children, [65] and could be considered as state-of-the-art by some Coordinating Authorities. While the effectiveness of the Proposal hinges on the reliability of these technological solutions, very little information is available on the generalized and systematic use of these techniques, which warrants careful consideration.

86. In addition, even though the EDPB and EDPS had to use them in their proportionality assessment, due to a lack of alternatives, it must be noted that the performance indicators of detection technologies mentioned in the Impact Assessment Report that accompanied the Proposal provide very little information on how they have been assessed and whether they reflect the real-world performance of the relevant technologies. There is no information on the tests or benchmarks used by the technology vendors to measure those performances. Without such information, it is not possible to replicate the tests or evaluate the validity of the performance statements. In this regard, it should be noted that although the performance indicators could be interpreted as suggesting that some detection tools have a high level of accuracy (for instance, the accuracy of certain grooming detection tools is 88%),[66] these indicators should be considered in light of the envisaged practical use of the detection tools and the severity of the risks that an incorrect assessment of a given material would entail for the relevant data subjects. Moreover, the EDPB and EDPS consider that, with such a high risk processing, 12% failure rate presents a high risk to data subjects who have been subject to false positives, even when there are safeguards in place to prevent false reports to law enforcement. It is highly unlikely that service providers could commit enough resources to review such a percentage of false positives.

87. As previously mentioned, [67] performance indicators should provide an exhaustive insight in the behavior of the detection tools. When using artificial intelligence algorithms on images or text, it is well documented that bias and discrimination can occur due to the lack of representativeness of certain population groups in the data used to train the algorithm. These biases should be identified, measured and reduced to an acceptable level in order for the detection systems to be truly profitable to society as a whole.

---

[65] See Impact Assessment Report, pp. 281-282.
[66] Ibid, p. 283.
[67] See paragraphs 63-64 above.

88. Although a study of the technologies used for detection has been done,[68] the EDPB and EDPS consider that further analysis is necessary in order to assess independently the reliability in real world use cases of the existing tools. This analysis should rely on exhaustive performance indicators and assess the impact of potential errors in real life conditions for all data subjects concerned by the Proposal. As these technologies are the basis on which the Proposal relies, the EDPB and EDPS consider this analysis to be of paramount importance for assessing the adequacy of the Proposal.

89. The EDPB and EDPS also note that the Proposal does not define technology-specific requirements, be it with regard to the error rates, to the use of classifiers and their validation, or other restrictions. This leaves it to the practice to develop such criteria when assessing the proportionality of the use of a specific technology, contributing further to the lack of preciseness and clarity.

90. Given the importance of the consequences for the data subjects in cases of false positive, the EDPB and EDPS consider that the false positive rates must be reduced to a minimum, and that those systems must be designed while keeping in mind that the vast majority of the electronic communications do not include any CSAM nor solicitations of children, and also that even a very low false positive rate will imply a very high number of false positives given the volume of data that will be subject to detection. More generally, the EDPB and EDPS are also concerned by the fact that the performance of the available tools indicated in the Impact Assessment Report does not reflect precise and comparable indicators regarding false positive and false negative rates, and consider that comparable and meaningful performance indicators for those technologies should be issued, before considering them as available and efficient.

4.8.3 Scanning of audio communications

91. Contrary to the Interim Regulation,[69] the Proposal does not exclude from its scope of application the scanning of audio communications in the context of grooming detection.[70] The EDPB and EDPS believe that the scanning of audio communications is particularly intrusive, as it would normally require active, ongoing and 'live' interception. Moreover, in some Member States, the privacy of the spoken word enjoys special protection.[71] Furthermore, due to the fact that, in principle, all content of the audio communication would need to be analysed this measure is likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter. Thus, this detection method should remain outside the scope of the detection obligations set out in the proposed Regulation, both with respect to voice messages and live communications, all the more in light of the fact that the Impact Assessment Report that accompanied the Proposal did not identify any specific risks or changes in the threat landscape that would warrant its use.[72]

4.8.4 Age verification

92. The Proposal encourages providers to use age verification and age assessment measures to identify child users on their services.[73] In this respect, the EDPB and EDPS note that there is currently no technological solution that is capable of assessing with certainty the age of a user in an online context,

[68] See Impact Assessment Report, pp. 279 et seq.
[69] Cf. Interim Regulation, Art. 1(2).
[70] Cf. Proposal, Art. 1.
[71] See e.g. German Criminal Code, Section 201.
[72] See Impact Assessment Report.
[73] See Proposal, Arts. 4(3), 6(1)(c) and Rec. 16.

without relying on an official digital identity, which is not available to every European citizen at this stage.[74] Therefore, the Proposal's envisaged use of age verification measures could possibly lead to the exclusion of, e.g., young-looking adults from accessing online services, or to the deployment of very intrusive age verification tools, which might inhibit or discourage the legitimate use of the affected services.

93. In this regard, and even though Recital 16 of the Proposal refers to parental control tools as possible mitigation measures, the EDPB and EDPS recommend that the proposed Regulation be amended to expressly allow providers to rely on parental control mechanisms in addition or as an alternative to age verification.

4.9 Preservation of information

94. Article 22 of the Proposal limits the purposes for which the providers subject to the Proposal may keep the content data and other data processed in connection to the measures taken to comply with the obligations set out in the Proposal. However, the Proposal indicates that providers may also preserve this information for the purpose of improving the effectiveness and accuracy of the technologies to detect online child sexual abuse for the execution of a detection order, but they shall not store any personal data for that purpose.[75]

95. The EDPB and EDPS consider that only those providers that use their own detection technologies should be allowed to retain data for improving the effectiveness and accuracy of the technologies, whereas those who use technologies provided by the EU Centre should not benefit from this possibility. Moreover, the EDPB and EDPS note it might be difficult to ensure in practice that no personal data are stored for that purpose, as most content data and other data processed for detection purposes is likely to qualify as personal data.

4.10 Impact on encryption

96. European data protection authorities have consistently advocated for the widespread availability of strong encryption tools and against any type of backdoors.[76] This is because encryption is important to ensure the enjoyment of all human rights offline and online.[77] Moreover, encryption technologies contribute in a fundamental way both to the respect for private life and confidentiality of communications, as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide.

97. In the context of interpersonal communications, end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider. Preventing or discouraging in any way the use of E2EE, imposing on service providers an obligation to process electronic communication data for purposes other than providing their services, or imposing on them an obligation to proactively forward electronic communications to third parties would entail the risk that providers offer less encrypted services in

[74] See e.g. CNIL, Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy (9 August 2021).
[75] Proposal, Art. 22(1).
[76] See e.g. Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11 April 2018).
[77] See Human Rights Council, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/RES/47/16 (26 July 2021).

order to better comply with the obligations, thus weakening the role of encryption in general and undermining the respect for the fundamental rights of European citizens. It should be noted that while E2EE is one of the most commonly used security measures in the context of electronic communications, other technical solutions (e.g., the use of other cryptographic schemes) might be or become equally important to secure and protect the confidentiality of digital communications. Thus, their use should not be prevented or discouraged too.

98. The deployment of tools for the interception and analysis of interpersonal electronic communications is fundamentally at odds with E2EE, as the latter aims to technically guarantee that a communication remains confidential between the sender of the receiver.

99. Therefore, even though the Proposal does not establish a systematic interception obligation for providers, the mere possibility that a detection order might be issued is likely to weigh heavily on the technical choices made by providers, especially given the limited timeframe they will have to comply with such an order and the heavy penalties they would face for failing to do so.[78] In practice, this might lead certain providers to stop using E2EE.

100. The impact of degrading or discouraging the use of E2EE, which may result from the Proposal needs to be assessed properly. Each of the techniques for circumventing the privacy preserving nature of E2EE presented in the Impact Assessment Report that accompanied the Proposal would introduce security loopholes.[79] For example, client-side scanning[80] would likely lead to substantial, untargeted access and processing of unencrypted content on end user's devices. Such a substantial degradation of confidentiality would especially affect children since the services they use are more likely to be targeted by detection orders, making them vulnerable to monitoring or eavesdropping. At the same time, *server-side* scanning, is also fundamentally incompatible with the E2EE paradigm, since the communication channel, encrypted peer-to-peer, would need to be broken, thus leading to the bulk processing of personal data on the servers of the providers.

101. While the Proposal states that it 'leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as encouraging or discouraging the use of any given technology',[81] the structural incompatibility of some detection order with E2EE becomes in effect a strong disincentive to use E2EE. The inability to access and use services using E2EE (which constitute the current state of the art in terms of technical guarantee of confidentiality) could have a chilling effect on freedom of expression and the legitimate private use of electronic communication services. The adverse relationship between CSAM or grooming detection and E2EE is also acknowledged by the Commission when noting in the Impact Assessment Report[82] the likelihood that the implementation of E2EE by Facebook in 2023 would bring Facebook's voluntary scanning to an end.

---

[78] Cf. Proposal, Art. 35.

[79] See section 4.2 in Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso, 'Bugs in our Pockets: The Risks of Client-Side Scanning', ArXiv abs/2110.07450 (2021).

[80] Client side scanning broadly refers to systems that scan message contents for matches against a database of objectionable content before the message is sent to the intended recipient.

[81] Proposal, Rec. 26.

[82] Impact Assessment Report, p. 27.

102. To ensure that the proposed Regulation does not undermine the security or confidentiality of electronic communications of European citizens, the EDPB and EDPS consider that the enacting terms of the Proposal should clearly state that nothing in the proposed Regulation should be interpreted as prohibiting or weakening encryption, in line with what is stated in Recital 25 of the Interim Regulation.

4.11 Supervision, enforcement and cooperation

4.11.1 Role of national supervisory authorities under the GDPR

103. The Proposal provides for the establishment of a network of national Coordinating Authorities, which shall be responsible for the application and enforcement of the proposed Regulation.[83] While Recital 54 of the Proposal states that 'the rules of this Regulation on supervision and enforcement should not be understood as affecting the powers and competences of the data protection authorities under Regulation (EU) 2016/679', the EDPB and EDPS are of the view that relationship between the tasks of Coordinating Authorities and those of data protection authorities should be better regulated, and that data protection authorities should be given a more prominent role within the proposed Regulation.

104. In particular, providers should be required to consult data protection authorities through a prior consultation procedure as referred to in Article 36 of the GDPR prior to deploying any CSAM or grooming detection measures, and not exclusively in connection with the use of measures for detecting solicitation of children, as currently envisaged by the Proposal.[84] All detection measures should be considered to result in 'high risk' by default, and should thus undergo a prior consultation procedure regardless of whether they concern grooming or CSAM, as it is already the case under the Interim Regulation.[85] In addition, the competent data protection authorities designated under the GDPR should always be empowered to provide their views on the envisaged detection measures, and not only in specific circumstances.[86]

105. Moreover, the proposed Regulation should establish a system for addressing and resolving disagreements between competent authorities and data protection authorities regarding detection orders. In particular, data protection authorities should be given the right to challenge a detection order before the courts of the Member State of the competent judicial authority or independent administrative authority that issued the detection order. In this regard, the EDPB and EDPS note how, under the current version of the Proposal, the opinion of the competent data protection authorities may be dismissed by the competent authority when issuing a detection order. This may potentially lead to conflicting decisions, as data protection authorities would, as confirmed by Article 36(2) GDPR, retain the full range of their corrective powers under Article 58 of the GDPR, including the power to order a ban on processing.

4.11.2 Role of the EDPB

106. The EDPB and EDPS note that the Proposal provides in Article 50(1), third sentence, that 'the EU Centre shall request the opinion of its Technology Committee and of the European Data Protection Board' before it adds a specific technology to the lists of technologies that providers of hosting services and providers of interpersonal communications services may consider using for executing detection orders. It further provides that the EDPB shall deliver its opinions within eight weeks, which may be

[83] Proposal, Art. 25.
[84] Proposal, Art. 7(3) second indent (b).
[85] Interim Regulation, Art. 3(1)(c).
[86] Cf. Proposal, Art. 7(3) second indent (c).

extended by a further six weeks where necessary, taking into account the complexity of the subject matter. It finally requires the EDPB to 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.

107. The existing tasks of the EDPB are laid down in Article 70 GDPR and Article 51 of Directive (EU) 2016/680 (hereinafter 'LED')[87]. In these tasks, it is set forth that the EDPB shall provide advice to the Commission and issue opinions on request of the Commission, a national supervisory authority or its Chair. While Article 1(3)(d) of the Proposal states that the rules laid down in the GDPR and the LED shall be unaffected by the Proposal, empowering the EU Centre to requests opinions from the EDPB goes beyond the tasks attributed to EDPB under the GDPR and LED. Thus, it should be made clear in the proposed Regulation – at least in a Recital – that the Proposal expands the tasks of the EDPB. In this respect, the EDPB and EDPS appreciate the important role that the Proposal assigns to the EDPB in requiring its involvement in the practical implementation of the proposed Regulation. In practice, the EDPB Secretariat plays an essential role in providing the analytical, administrative and logistical support necessary for the adoption of the opinions of the EDPB. Therefore, to ensure that the EDPB and its members can fulfil their tasks, it is essential to allocate sufficient budget and staff to the EDPB. Unfortunately, though, the Proposal's legislative financial statement does not indicate that any additional resources will be made available for the performance of the additional tasks that the Proposal assigns to the EDPB.[88]

108. Further, the EDPB and EDPS note that Article 50 of the Proposal does not indicate how the EU Centre will proceed after receiving an opinion by the EDPB.[89] Recital 27 of the Proposal merely states that advice given by the EDPB should be taken into account by the EU Centre and the European Commission. It should therefore be clarified what purpose the requested opinion will serve in the process provided in Article 50 of the Proposal and how the EU Centre is to act after having received an opinion by the EDPB.

109. In addition, the EDPB and EDPS consider that while any EDPB guidelines or possible opinion on the use of detection technologies will assess the use of such technologies on a general level, for a prior consultation under Article 36 GDPR the national supervisory authority will need to take account of the specific circumstances and perform a case by case assessment of the intended processing by the relevant controller. The EDPB and EDPS note that supervisory authorities will and should apply the criteria set out in Article 36 GDPR to decide whether it is necessary to extend the time period set out in the GDPR for providing their opinions in response to a prior consultation, and there is no need for applying different standards when a prior consultation concerns the use of a detection technology.[90]

110. Finally, in the application of Article 11 ('Guidelines regarding detection obligations'), the Proposal stipulates that the Commission may issue guidelines on the application of Articles 7 to 10 of the Proposal. Article 11 of the Proposal should be amended to make clear that, in addition to the Coordinating Authorities and the EU Centre, the EDPB should be consulted by the Commission on the

[87] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89–131).
[88] Cf. Proposal, pp. 105 et seq.
[89] See in contrast Art. 51(4) LED.
[90] Cf. Proposal, Recital 24.

draft guidelines outside of the envisaged public consultation process prior to issuing guidelines regarding detection obligations.

111. Therefore, this task of the EDPB, as well as its role within the legal framework that would be introduced by the Proposal, warrants further assessment by the legislature.

4.11.3 Role of the EU Centre on Child Sexual Abuse

112. Chapter IV of the Proposal would establish the EU Centre, as a new decentralised agency to enable the implementation of the Proposal. Among other tasks, the EU Centre should facilitate access to reliable detection technologies to providers; make available indicators created based on online child sexual abuse as verified by courts or independent administrative authorities of Member States for the purpose of detection; provide certain assistance, upon request, in connection to the performance of risk assessments; and provide support in communicating with relevant national authorities. [91]

113. In that regard, the EDPB and EDPS welcome Article 77(1) of the Proposal confirming that processing of personal data by the EU Centre shall be subject to the EUDPR as well as providing that the measures for the application of that Regulation by the EU Centre, including those concerning the appointment of a Data Protection Officer of the EU Centre, shall be established after consultation of the EDPS. However, the EDPB and EDPS are of the opinion that several provisions of this Chapter deserve closer scrutiny.

114. In the first place, the EDPB and EDPS note that Article 48 of the Proposal prescribes forwarding all reports which are 'not manifestly unfounded' [92] to national law enforcement authorities and the EU Agency for Law Enforcement Cooperation ('Europol'). This threshold for the EU Centre to forward reports to national law enforcement authorities and Europol ('not manifestly unfounded') appears too low, especially having in mind that the purpose of establishing the EU Centre, as set out in the Commission's Impact Assessment Report, [93] is to alleviate the burden on law enforcement authorities and Europol of filtering content mistakenly flagged as CSAM. In that regard, it is unclear why the EU Centre, as a hub of expertise, could not conduct a more thorough legal and factual assessment to limit the risks of innocent persons' data being transmitted to law enforcement.

115. Secondly, the provision concerning duration of storage of personal data by the EU Centre appears relatively open given the sensitivity of the data concerned. Even if it would not be possible to set a maximum retention period for the storage of those data, the EDPB and EDPS recommend to set in the Proposal, at least a maximum time limit for reviewing the necessity of continued storage of data and requiring justification for prolonged retention after that period.

116. In addition, given the very high sensitivity of the personal data to be processed by the EU Centre, the EDPB and EDPS are of the opinion that processing should be subject to additional safeguards, in particular to ensure effective oversight. This could include the obligation on the EU Centre to keep logs for processing operations in automated processing systems concerning the data (i.e. mirroring the requirement for operational personal data under Chapter IX of the EUDPR), including logging the entry, alteration, access, consultation, disclosure, combination and erasure of personal data. The logs

[91] See COM(2022) 209 final, p. 7.
[92] The term "manifestly unfounded" is described in Recital 65 of the Proposal as "where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online sexual abuse."
[93] See, for instance, page 349 of the Impact Assessment Report.

of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients. These logs would be used for verification of the lawfulness of processing, self-monitoring, and for ensuring its integrity and security and would be made available to the EU Centre's data protection officer and to the EDPS on request.

117. Furthermore, the Proposal makes reference to the obligation on providers to inform users about the detection of CSAM via detection orders, as well as the right to submit a complaint to a coordinating authority.[94] However, the Proposal does not lay down procedures for the exercise of data subjects' rights, also taking into account the multiple locations where personal data may be transmitted and stored under the Proposal (EU Centre, Europol, national law enforcement agencies). The requirement to inform users should include the obligation to inform individuals that their data has been forwarded and is being processed by different entities where applicable (e.g. by national law enforcement agencies and to Europol). In addition, there should be a centralised procedure for receiving and coordinating requests for the right of access, rectification and deletion or alternatively an obligation that the entity that receives a data subject request coordinates with the other entities concerned.

118. The EDPB and EDPS note that under Article 50 of the Proposal, the EU Centre is tasked to specify the list of the technologies that may be used for executing detection orders. However, according to Article 12(1) of the Proposal, providers are obliged to report all information indicating potential online child sexual abuse on its services, not only the ones coming from the execution of a detection order. It is highly probable that a significant amount of such information would come from the operation of providers' mitigating measures, in accordance with Article 4 of the Proposal. It thus seems critical to determine what these measures might be, their effectiveness, their error rate in reporting potential child sexual abuse, and what is their impact on the rights and freedoms of individuals. Despite the fact that Article 4(5) of the Proposal states that the Commission, in cooperation with Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue relevant guidelines, the EDPB and EDPS find it important that the legislator includes in Article 50 a task for the EU Centre to provide also a list of recommended mitigating measures and relevant best practices that are in particular effective in identifying potential online child sexual abuse. As such measures may interfere with the fundamental rights to data protection and privacy it is also recommended that the EU Centre ask for the opinion of the EDPB before issuing such a list.

119. Lastly, the security requirements set out in Article 51(4) of the Proposal should be more specific. In this regard, inspiration may be drawn from the security requirements laid down in other Regulations regarding large-scale systems involving high risk processing, such as Regulation 767/2008[95] (see

[94] See Article 10(6), and, following the submission of a report to the EU Centre, Article 12(2) of the Proposal.
[95] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) OJ L 218, 13.8.2008, p. 60–81.

Article 32), Regulation 1987/2006[96] (see Article 16), Regulation 2018/1862[97] (see Article 16), and Regulation 603/2013[98] (see Article 34).

4.11.4 Role of Europol

120. The Proposal provides for close cooperation between the EU Centre and Europol. Under Chapter IV of the Proposal, upon receiving reports from providers on suspected CSAM, the EU Centre shall check them to assess which reports are actionable (not manifestly unfounded) and shall forward them to Europol as well as to national law enforcement authorities.[99] The EU Centre shall grant Europol access to its databases of indicators and databases of reports to assist Europol's investigations of suspected child sexual abuse offences.[100] Moreover, the EU Centre would be granted the 'fullest possible' access to Europol's information systems.[101] The two agencies will also share premises and certain (non-operational) infrastructure.[102]

121. The EDPB and EDPS note that several aspects related to cooperation between the proposed EU Centre and Europol raise concern or require further specification.

On the forwarding of reports by the EU Centre to Europol (Article 48)

122. Article 48 of the proposed Regulation requires the EU Centre to forward reports that are not considered manifestly unfounded, together with any additional relevant information, to Europol and to the competent law enforcement authority or authorities of the Member State(s) likely to have jurisdiction to investigate or prosecute the potential child sexual abuse. Although this Article accords Europol the role of identifying the relevant law enforcement authority where the Member State concerned is unclear, the provision in fact provides that all reports shall be transmitted to Europol regardless of whether the national authority has been identified and already transmitted the report by the EU Centre.

---

[96] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4–23).
[97] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56–106).
[98] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1–30).
[99] See Article 48 of the Proposal.
[100] See Article 46(4)-(5) of the Proposal.
[101] See Article 53(2) of the Proposal.
[102] Notably those regarding human resources management, information technology (IT), including cybersecurity, the building and communications.

123. However, the Proposal does not clarify what would be the added value of Europol's involvement or its expected role upon receiving the reports, particularly in those cases where the national law enforcement authority has been identified and notified in parallel.[103]

124. The EDPB and EDPS recall that Europol's mandate is limited to supporting action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States.[104] Article 19 of Regulation (EU) 2016/794[105] as amended by Regulation (EU) 2022/991[106] ('amended Europol Regulation') stipulates that a Union body providing information to Europol is obliged to determine the purpose or purposes for which it is to be processed by Europol as well as the conditions for processing. It is also responsible for ensuring the accuracy of the personal data transferred.[107]

125. A blanket forwarding of reports to Europol would therefore be in contravention with the amended Europol Regulation and would carry a number of data protection risks. The duplication of personal data processing could lead to multiple copies of the same highly sensitive personal data being stored in parallel (e.g. at the EU Centre, Europol, national law enforcement authority), with risks for data accuracy as a result of the potential desynchronisation of databases, as well as for the exercise of data subjects' rights. Furthermore, the low threshold established in the Proposal for sharing reports with law enforcement authorities (those 'not manifestly unfounded') implies a high likelihood that false positives (i.e. content mistakenly flagged as child sexual abuse) will be stored in Europol's information systems, potentially for prolonged periods.[108]

126. The EDPB and EDPS therefore recommend that the Proposal specify and limit the circumstances and purposes under which the EU Centre could forward reports to Europol, in accordance with the amended Europol Regulation. This should explicitly exclude those circumstances where reports have been transmitted to the relevant Member State law enforcement authority, which imply no cross-border dimension. In addition, the Proposal should include the requirement that the EU Centre only transfer personal data to Europol that is adequate, relevant and limited to what is strictly necessary. Specific safeguards for ensuring data quality and reliability must also be provided for.

[103] Recital 71 of the Proposal only makes a general reference to Europol's experience in identifying competent national authorities in unclear situations and its database of criminal intelligence, which can contribute to identifying links to investigations in other Member States.
[104] See Article 3 of the amended Europol Regulation.
[105] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53–114).
[106] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (OJ L 169, 27.6.2022, p. 1–42).
[107] Article 38(2)(a) of the amended Europol Regulation.
[108] According to the Commission Impact Assessment report, Europol has only been able to examine 20% of the 50 million unique CSAM images and videos in its database, implying a lack of resources to action the contributions of CSAM that it currently receives. See Impact Assessment Report accompanying the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022)209, pp.47-48.

Article 53(2) on cooperation between the EU Centre and Europol

127. Article 53(2) of the Proposal requires that Europol and the EU Centre shall provide each other with 'the fullest possible access to relevant information systems, where necessary for the performance of their respective tasks and in accordance with the acts of Union law regulating such access.'

128. Articles 46(4) and 46(5) of the Proposal further specify that Europol shall have access to the EU Centre's database of indicators and database of reports, and Article 46(6) lays down the procedure for granting this access: Europol shall submit a request, specifying the purpose and degree of access required to fulfil that purpose, which shall be duly assessed by the EU Centre.

129. The criteria and safeguards conditioning Europol's access and subsequent use of data obtained from the EU Centre's information systems are not specified. Moreover, it is not explained why it is necessary to grant Europol direct access to the information systems of a non-law enforcement agency, containing highly sensitive personal data, whose link to criminal activity and crime prevention may not have been established. In order to ensure a high level of data protection, and compliance with the principle of purpose limitation, the EDPB and EDPS recommend that transmission of personal data from the EU Centre to Europol only takes place on a case-by-case basis, following a duly assessed request, via a secure exchange communication tool, such as SIENA.[109]

130. Article 53(2) offers the only reference in the Proposal to access by the EU Centre to Europol's information systems. It is therefore unclear for which purposes, and according to which specific safeguards, such access would take place.

131. The EDPB and EDPS recall that Europol is a law enforcement agency, established under the EU Treaties with a core mandate of preventing and combating serious crime. The operational personal data processed by Europol is consequently subject to strict data processing rules and safeguards. The proposed EU Centre is not a law enforcement body, and under no circumstances should be granted direct access to Europol's information systems.

132. The EDPB and EDPS further note that a large proportion of the information of shared interest to the EU Centre and Europol will concern personal data relating to victims of alleged crimes, personal data of minors and personal data concerning sex life, which qualify as special categories of personal data under the amended Europol Regulation. The amended Europol Regulation imposes strict conditions regarding access to special categories of personal data. Article 30(3) of the amended Europol Regulation stipulates that only Europol shall have direct access to such personal data, more specifically only a limited number of Europol officials duly authorised by the Executive Director.[110]

133. The EDPB and EDPS therefore recommend to clarify the wording of Article 53(2) of the Proposal in order to properly reflect the restrictions in place under the amended Europol Regulation and specify the modalities for access by the EU Centre. In particular, any access to personal data processed in Europol's information systems, where deemed strictly necessary for the performance of the EU Centre's tasks, should be granted only on a case-by-case basis, upon submission of an explicit request, which documents the specific purpose, and justification. Europol should be required to diligently

[109] Secure Information Exchange Network Application (SIENA).

[110] Under the amended Europol Regulation exceptions to this prohibition are made for Union agencies established under Title V TFEU. However, given the legal basis for the Proposal (114 TFEU, relating to internal market harmonisation), this exception would not include the proposed EU Centre.

assess those requests and only transmit personal data to the EU Centre where strictly necessary and proportionate to the required purpose.

Article 10(6) on Europol's role in informing users following implementation of a detection order

134. The EDPB and EDPS welcome the requirement, as laid down in Article 10(6) of the Proposal, for providers to inform users whose personal data may be concerned by the execution of a detection order. This information is to be provided to users only after obtaining confirmation from Europol or the national law enforcement authority of a Member State that received the report pusuant to Article 48 of the Proposal that providing information to users would not interfere with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

135. There is a lack of specificity, however, regarding the practical implementation of this provision. Where reports are forwarded to both Europol and a Member State law enforcement authority, the Proposal does not stipulate whether confirmation is required from one or both recipients, nor are the procedures/modalities for obtaining this confirmation spelled out in the Proposal (e.g. whether confirmations are to be channelled through the EU Centre). Taking into account the high volume of CSAM that Europol and national law enforcement authorities could be required to process, and the lack of a precise time limit for providing confirmation ('without undue delay'), the EDPB and EDPS recommend clarifying the applicable procedures in order to ensure the realisation of this safeguard in practice. Furthermore, the obligation to inform users should also include information regarding the recipients of the personal data concerned.

On data collection and transparency reporting (Article 83)

136. Article 83(3) of the Proposal provides for the EU Centre to collect data and generate statistics relating to a number of its tasks under the proposed Regulation. For monitoring purposes, the EDPB and EDPS recommend adding to this list statistics on the number of reports forwarded to Europol in accordance with Article 48, as well as the number of access requests received by Europol under Article 46(4) and 46(5), including the number of those requests granted and refused by the EU Centre.

5. CONCLUSION

137. While the EDPB and EDPS welcome the Commission's efforts to ensure effective action against child sexual abuse online, they consider that the Proposal raises serious data protection and privacy concerns. Therefore, the EDPB and EDPS would invite the co-legislators to amend the proposed Regulation, in particular to ensure that the envisaged detection obligations meet the applicable necessity and proportionality standards and do not result in the weakening or degrading of encryption on a general level. The EDPB and EDPS remain available to offer their support during the legislative process, should their input be deemed necessary to address the concerns highlighted in the present joint opinion.

For the European Data Protection Supervisor	For the European Data Protection Board
The European Data Protection Supervisor	The Chair
(Wojciech Wiewiorowski)	(Andrea Jelinek)