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

(TEXT WITH EEA RELEVANCE)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), in conjunction with Article 114(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Directive 2002/58/EC of the European Parliament and of the Council (3) lays down rules ensuring the right to privacy and confidentiality with respect to the processing of personal data in exchanges of data in the electronic communication sector. That Directive particularises and complements Regulation (EU) 2016/679 of the European Parliament and of the Council (4).

(2) **The proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, which the Commission adopted on 11 May 2022 ('the 2022 proposal'), aims to provide the long-term legal framework. However, the interinstitutional negotiations on that proposal have not yet advanced sufficiently to be certain that they will be concluded on time for the long-term legal framework, including any amendments to Regulation (EU) 2021/1232 that it may contain, to be adopted and start to apply before 4 April 2026. The European Parliament adopted its position and the mandate to enter into inter-institutional negotiations on 22 November 2023 while the Council was unable to reach its position before 26 November 2025. This**

requires further extension, even though Regulation (EU) 2021/1232 was designed to be a temporary and unique instrument that allowed for sufficient time for the adoption for the 2022 proposal. ~~Directive 2002/58/EC applies to the processing of personal data in connection with the provision of publicly available electronic communication services. Until 21 December 2020, the definition of 'electronic communication service' set out in Article 2, point (c), of Directive 2002/21/EC of the European Parliament and of the Council (5) applied. On that date, Directive (EU) 2018/1972 of the European Parliament and of the Council (6) repealed Directive 2002/21/EC. The definition of 'electronic communications service' in Article 2, point (4), of Directive (EU) 2018/1972 includes number-independent interpersonal communications services as defined in Article 2, point (7), of that Directive. Number-independent interpersonal communications services, which include, for example, Voice over internet Protocol, messaging and web-based email services, were therefore brought within the scope of Directive 2002/58/EC on 21 December 2020.~~

(3) In accordance with Article 6(1) of the Treaty on European Union (TEU), the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union (the 'Charter'). Article 7 of the Charter protects the fundamental right of everyone to the respect for his or her private and family life, home and communications, which includes the confidentiality of communications. Article 8 of the Charter contains the right to the protection of personal data.

(4) **Given these circumstances, Regulation (EU) 2021/1232 should be amended to extend its period of application for a period of time limited to that which is strictly necessary for the long-term legal framework to be adopted and start to apply. The co-legislators therefore commit to reaching an agreement on the long-term legal framework as soon as possible and with a view to avoiding any further extensions of Regulation (EU) 2021/1232 in the future. Furthermore, taking into consideration that Regulation (EU) 2021/1232 was intended to apply during a limited period of time, it is necessary to clarify some provisions thereof and adapt them to the results from the Implementing Reports from the Commission of 19 December 2023 and of 27 November 2025 ('the 2023 and 2025 implementing reports').** ~~Article 3(1) of the 1989 United Nations Convention on the Rights of the Child (UNCRC) and Article 24(2) of the Charter provide that, in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. Article 3(2) UNCRC and Article 24(1) of the Charter furthermore evoke the right of children to such protection and care as is necessary for their well-being.~~

(5) The protection of children, both offline and online, is one of the Union's priorities. Sexual abuse and sexual exploitation of children constitute serious violations of human and fundamental rights, in particular of the rights of children to be protected from all forms of violence, abuse and neglect, maltreatment or exploitation, including sexual abuse, as provided for by the UNCRC and by the Charter. Digitalisation has brought about many benefits for society and the economy, but it has also brought about challenges, including an increase of online child sexual abuse. On 24 July 2020, the Commission adopted a communication entitled 'EU strategy for a more effective fight against child sexual abuse' (the 'Strategy'). The Strategy aims to provide an effective response, at Union level, to the crime of child sexual abuse.

(5a) The mere fact that certain providers of number-independent interpersonal communications services apply detection technologies on a voluntary basis does not relieve the co-legislators from their

responsibility of establishing a comprehensive legal framework which meets the requirements of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter') and does not undermine the prohibition of general monitoring under Union law.

(5b) Nothing in this Regulation should be interpreted as prohibiting, weakening or undermining end-to-end encryption. Providers should in particular not be prohibited to offer end-to-end encrypted services.

(6) In line with Directive 2011/93/EU of the European Parliament and of the Council (7), this Regulation does not govern Member States' policies with regard to consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies.

(7) Some providers of certain number-independent interpersonal communications services ('providers'), such as webmail and messaging services, already use specific technologies on a voluntary basis to detect online child sexual abuse on their services and report it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse, by scanning either the content, such as images and text, or the traffic data of communications using, in some instances, historical data. The technology used for those activities could be hashing technology for images and videos and classifiers and artificial intelligence for analysing text or traffic data. When using hashing technology, online child sexual abuse material is reported when a positive hit is returned, which means a match resulting from a comparison between an image or a video and a unique, non-reconvertible digital signature ('hash') from a database maintained by an organisation acting in the public interest against child sexual abuse that contains verified online child sexual abuse material. Those providers refer to national hotlines for reporting online child sexual abuse material and to organisations, located both within the Union and in third countries, whose purpose is to identify children, reduce child sexual exploitation and sexual abuse and prevent child victimisation. Such organisations might not fall within the scope of Regulation (EU) 2016/679. Collectively, such voluntary activities play a valuable role in enabling the identification and rescue of victims, whose fundamental rights to human dignity and to physical and mental integrity are severely violated. Such voluntary activities are also important in reducing the further dissemination of online child sexual abuse material and in contributing to the identification and investigation of offenders and to the prevention, detection, investigation and prosecution of child sexual abuse offences.

(7a) The processing of images and videos under Regulation (EU) 2021/1232 should always be considered to be processing of special categories of personal data under Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council as they are biometric data that that are processed through a specific technical means allowing the unique identification or authentication of a natural person.

(7b) In light of the 2023 and 2025 implementing reports to ensure consistency and clarity, definitions which are no longer relevant due to incomplete, inaccurate data that cannot be independently audited should be deleted from Regulation (EU) 2021/1232. Since the scope of Regulation (EU) 2021/1232

should not include detection of not previously identified online child sexual abuse material, or solicitation of children, their definitions are redundant and therefore should be deleted. The 2023 and 2025 implementing reports also stress that no conclusive data on the proportionality of detecting not previously identified online child sexual abuse material, or solicitation of children can be relied upon to justify the restriction of certain rights as provided by Directive 2002/58/EC and Articles 7 and 8 of the Charter.

(7c) Considering the unproven effectiveness of Regulation (EU) 2021/1232 regarding not previously identified online child sexual abuse material, or solicitation of children, while at the same time the impact on the confidentiality of communications as provided by Directive 2002/58/EC of the European Parliament and of the Council, the detection of not previously identified child sexual abuse material and child solicitation should be taken out of the scope of Regulation (EU) 2021/1232. However, in order to prevent solicitation of children, certain providers of number-independent interpersonal communications services can and are encouraged to take mitigation measures, which do not interfere with Directive 2002/58/EC.

(7d) Since the sole objective of this Regulation is to enable the limited and targeted, modified continuation of certain existing activities aimed at combating child sexual abuse online, the derogation provided for by this Regulation should be limited to well-established technology that is used by certain providers of number-independent interpersonal communications services for the purpose of detecting, reporting and removing child sexual abuse material, which functions by matching images and videos against a database of unique, non-reconvertible digital signatures ((‘hashes’) of identified child sexual abuse material.

(7e) In order to ensure an adequate level of transparency and accountability, as well as to enable comprehensive and comparable reporting, it is necessary to include administrative fines for non-compliance by certain providers of number-independent interpersonal communications services with the reporting and transparency obligations and requirements, notably the use of the standard form for report as established by Regulation (EU) 2024/1307 of the European Parliament and of the Council and subsequent Commission Implementing Regulation (EU) 2024/2916.

(7f) In order to strengthen the enforcement of the rules of Regulation (EU) 2021/1232, administrative fines should be imposed for any infringement of that Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to that Regulation.

(8) Notwithstanding their legitimate objective, voluntary activities by providers to detect online child sexual abuse on their services and report it constitute an interference with the fundamental rights to respect for private and family life and to the protection of personal data of all users of number-independent interpersonal communications services (‘users’). Any limitation to the exercise of the fundamental right to respect for private and family life, including the confidentiality of communications, cannot be justified merely on the grounds that providers were using certain technologies at a time when number-independent interpersonal communications services did not fall within the definition of ‘electronic communications services’. Such limitations are only possible under certain conditions. Pursuant to Article 52(1) of the Charter, such limitations are to be provided for by law and are to respect the essence of the rights to private

and family life and to the protection of personal data and, subject to the principle of proportionality, they are to be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Where such limitations permanently involve a general and indiscriminate monitoring and analysis of the communications of all users, they interfere with the right to confidentiality of communications.

(9) Until 20 December 2020, the processing of personal data by providers by means of voluntary measures for the purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services was governed solely by Regulation (EU) 2016/679. Directive (EU) 2018/1972, which was to be transposed by 20 December 2020, brought providers within the scope of Directive 2002/58/EC. In order to continue using such voluntary measures after 20 December 2020, providers should comply with the conditions set out in this Regulation. Regulation (EU) 2016/679 will continue to apply to the processing of personal data carried out by means of such voluntary measures.

(10) Directive 2002/58/EC does not contain any specific provisions concerning the processing of personal data by providers in connection with the provision of electronic communication services for the purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services. However, pursuant to Article 15(1) of Directive 2002/58/EC, Member States can adopt legislative measures to restrict the scope of the rights and obligations provided for in, inter alia, Articles 5 and 6 of that Directive, which concern the confidentiality of communications and traffic data, for the purposes of the prevention, detection, investigation and prosecution of criminal offences linked to child sexual abuse. In the absence of such national legislative measures and pending the adoption of a longer-term legal framework to tackle child sexual abuse at Union level, providers can no longer rely on Regulation (EU) 2016/679 to continue to use voluntary measures to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services beyond 21 December 2020. This Regulation does not provide for a legal ground for the processing of personal data by providers for the sole purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services, but it provides for a derogation from certain provisions of Directive 2002/58/EC. This Regulation lays down additional safeguards which are to be respected by providers if they wish to rely on it.

(11) Processing of data for the purposes of this Regulation could entail the processing of special categories of personal data as set out in Regulation (EU) 2016/679. Processing of images and videos by specific technical means which allow for the unique identification or authentication of a natural person is considered processing of special categories of personal data.

(12) This Regulation provides for a temporary derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC, which protect the confidentiality of communications and traffic data. The voluntary use by providers of technologies for the processing of personal and other data to the extent necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services falls within the scope of the derogation provided for by this Regulation provided that such use complies with the conditions set out in this Regulation and is therefore subject to the safeguards and conditions set out in Regulation (EU) 2016/679.

(13) Directive 2002/58/EC was adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU). Moreover, not all Member States have adopted legislative measures in accordance with Directive 2002/58/EC to restrict the scope of the rights and obligations related to the confidentiality of communications and traffic data as set out in that Directive, and the adoption of such measures involves a significant risk of fragmentation likely to negatively affect the internal market. Consequently, this Regulation should be based on Article 114 TFEU.

(14) Given that data related to electronic communications involving natural persons usually qualify as personal data, this Regulation should also be based on Article 16 TFEU, which provides a specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and rules relating to the free movement of such data.

(15) Regulation (EU) 2016/679 applies to the processing of personal data in connection with the provision of electronic communications services by providers for the sole purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services to the extent that that processing falls within the scope of the derogation provided for by this Regulation.

(16) **The types of technologies used for the purposes of this Regulation should be the least privacy-intrusive in accordance with the state of the art in the industry. Those technologies should not be used to systematically filter and scan text in communications unless it is solely to detect patterns which point to possible concrete reasons for suspecting online child sexual abuse, and they should not be able to deduce the substance of the content of the communications.** ~~In the case of technology used for identifying solicitation of children, such concrete reasons for suspicion should be based on objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication.~~

(17) Appropriate procedures and redress mechanisms should be put in place to ensure that individuals can lodge complaints with providers. Such procedures and mechanisms are, in particular, relevant where content that does not constitute online child sexual abuse has been removed or reported to law enforcement authorities or to an organisation acting in the public interest against child sexual abuse.

(18) In order to ensure accuracy and reliability as much as possible, technology used for the purposes of this Regulation should, in accordance with the state of the art in the industry, limit the numbers and ratios of errors (false positives) to the maximum extent possible and should, where necessary, rectify without delay any such errors that might nonetheless occur.

(19) The content data and traffic data processed and the personal data generated when carrying out the activities covered by this Regulation, and the period during which the data are subsequently stored in the event of the identification of suspected online child sexual abuse, should remain limited to what is strictly necessary to carry out those activities. Any data should be immediately and permanently deleted as soon as they are no longer strictly necessary for one of the purposes specified in this Regulation, including where no suspected online child sexual abuse is identified, and in any event no later than 12 months from the date of the detection of suspected online child sexual abuse. This should be without prejudice to the possibility to store relevant content data and traffic data in accordance with Directive 2002/58/EC. This Regulation does

not affect the application of any legal obligation under Union or national law to preserve data that applies to providers.

(20) This Regulation does not prevent a provider that has reported online child sexual abuse to law enforcement authorities from requesting those authorities to acknowledge receipt of the report.

(21) **In order to ensure transparency and accountability in respect of the activities undertaken pursuant to the derogation provided for by this Regulation, providers should, by 3 February 2022, and by 31 January every year thereafter, publish and submit reports to the competent supervisory authority designated pursuant to Regulation (EU) 2016/679 ('supervisory authority') and to the Commission. Such reports should cover processing falling within the scope of this Regulation, including the type and volumes of data processed, the specific grounds relied on for the processing of personal data pursuant to Regulation (EU) 2016/679, the grounds relied on for transfers of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable, the number of cases of online child sexual abuse identified, the number of cases in which a user has lodged a complaint with the internal redress mechanism or sought a judicial remedy and the outcome of such complaints and judicial proceedings, the numbers and ratios of errors (false positives) of the different technologies used, the measures applied to limit the error rate and the error rate achieved, the retention policy and the data protection safeguards applied pursuant to Regulation (EU) 2016/679, and the names of the organisations acting in the public interest against child sexual abuse with which data have been shared pursuant to this Regulation.** ~~In order to ensure transparency and accountability in respect of the activities undertaken pursuant to the derogation provided for by this Regulation, providers should, by 3 February 2022, and by 31 January every year thereafter, publish and submit reports to the competent supervisory authority designated pursuant to Regulation (EU) 2016/679 ('supervisory authority') and to the Commission. Such reports should cover processing falling within the scope of this Regulation, including the type and volumes of data processed, the specific grounds relied on for the processing of personal data pursuant to Regulation (EU) 2016/679, the grounds relied on for transfers of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679, where applicable, the number of cases of online child sexual abuse identified, differentiating between online child sexual abuse material and solicitation of children, the number of cases in which a user has lodged a complaint with the internal redress mechanism or sought a judicial remedy and the outcome of such complaints and judicial proceedings, the numbers and ratios of errors (false positives) of the different technologies used, the measures applied to limit the error rate and the error rate achieved, the retention policy and the data protection safeguards applied pursuant to Regulation (EU) 2016/679, and the names of the organisations acting in the public interest against child sexual abuse with which data have been shared pursuant to this Regulation.~~

(22) In order to support the supervisory authorities with their tasks, the Commission should request the European Data Protection Board to issue guidelines on the compliance of processing falling within the scope of the derogation laid down in this Regulation with Regulation (EU) 2016/679. When the supervisory authorities assess whether an established or new technology to be used is in accordance with the state of the art in the industry, the least privacy-intrusive and operating on an adequate legal basis under Regulation (EU) 2016/679, those guidelines should, in particular, assist the supervisory authorities in providing advice in the framework of the prior consultation procedure set out in that Regulation.

(23) This Regulation restricts the right to protection of the confidentiality of communications and derogates from the decision taken under Directive (EU) 2018/1972 to subject number-independent interpersonal communications services to the same rules that apply to all other electronic communications services as regards privacy for the sole purpose of detecting online child sexual abuse on those services and reporting it to law enforcement authorities or to organisations acting in the public interest against child sexual abuse and removing online child sexual abuse material from those services. The period of application of this Regulation should, therefore, be limited to three years from its date of application to allow for the necessary time to adopt a new long-term legal framework. Where the long-term legal framework is adopted and enters into force before that date, that long-term legal framework should repeal this Regulation.

(24) With regard to all other activities that fall within the scope of Directive 2002/58/EC, providers should be subject to the specific obligations set out in that Directive and, consequently, to the monitoring and investigative powers of the competent authorities designated pursuant to that Directive.

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

(26) The right to respect for private and family life, including the confidentiality of communications, is a fundamental right guaranteed under Article 7 of the Charter. It is thus also a prerequisite for secure communications between victims of child sexual abuse and a trusted adult or organisations active in the fight against child sexual abuse and for communications between victims and their lawyers.

(27) This Regulation should be without prejudice to the rules on professional secrecy under national law, such as rules on the protection of professional communications, between doctors and their patients, between journalists and their sources, or between lawyers and their clients, in particular since the confidentiality of communications between lawyers and their clients is key to ensuring the effective exercise of the rights of the defence as an essential part of the right to a fair trial. This Regulation should also be without prejudice to national rules on registers of public authorities or organisations which offer counselling to individuals in distress.

(28) Providers should communicate to the Commission the names of the organisations acting in the public interest against child sexual abuse to which they report potential online child sexual abuse under this Regulation. While it is the sole responsibility of the providers acting as controllers to assess with which third party they can share personal data under Regulation (EU) 2016/679, the Commission should ensure transparency regarding the transfer of potential cases of online child sexual abuse by making public on its website a list of the organisations acting in the public interest against child sexual abuse communicated to it. That public list should be easily accessible. It should also be possible for providers to use that list in order to identify relevant organisations in the global fight against online child sexual abuse. That list should be without prejudice to the obligations of the providers acting as controllers under Regulation (EU) 2016/679, including with regard to their obligation to conduct any transfer of personal data outside the Union pursuant to Chapter V of that Regulation and their obligation to fulfil all of the obligations under Chapter IV of that Regulation.

(29) The statistics to be provided by Member States under this Regulation are important indicators for the evaluation of policy, including legislative measures. In addition, it is important to recognise the impact of secondary victimisation inherent in the sharing of images and videos of victims of child sexual abuse that might have been circulating for years and which is not fully reflected in such statistics.

(30) In line with the requirements laid down in Regulation (EU) 2016/679, in particular the requirement that Member States ensure that supervisory authorities are provided with the human, technical and financial resources necessary for the effective performance of their tasks and exercise of their powers, Member States should ensure that supervisory authorities have such sufficient resources for the effective performance of their tasks and exercise of their powers under this Regulation.

(31) Where a provider has conducted a data protection impact assessment and consulted the supervisory authorities with regard to a technology in accordance with Regulation (EU) 2016/679 prior to the entry into force of this Regulation, that provider should not be obliged under this Regulation to carry out an additional data protection impact assessment or consultation provided that the supervisory authorities have indicated that the processing of data by that technology would not result in a high risk to the rights and freedoms of natural persons or that measures have been taken by the controller to mitigate such a risk.

(32) Users should have the right to an effective judicial remedy where their rights have been infringed as a result of the processing of personal and other data for the purpose of detecting online child sexual abuse on number-independent interpersonal communications services and reporting it and removing online child sexual abuse material from those services, for instance where a user's content or identity have been reported to an organisation acting in the public interest against child sexual abuse or to law enforcement authorities or where a user's content has been removed or a user's account has been blocked or a service offered to a user has been suspended.

(33) In line with Directive 2002/58/EC and the principle of data minimisation, the processing of personal and other data should be limited to content data and related traffic data, in as far as strictly necessary to achieve the purpose of this Regulation.

(34) The derogation provided for by this Regulation should extend to the categories of data referred to in Articles 5(1) and 6(1) of Directive 2002/58/EC, which are applicable to the processing of both personal and non-personal data processed in the context of the provision of a number-independent interpersonal communications service.

(35) The objective of this Regulation is to create a temporary derogation from certain provisions of Directive 2002/58/EC without creating fragmentation in the internal market. In addition, it is unlikely that all Member States could adopt national legislative measures in time. Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective. It introduces a temporary and strictly limited derogation from the applicability of Articles 5(1) and 6(1) of Directive 2002/58/EC, with a series of safeguards to ensure that it does not go beyond what is necessary for the achievement of the set objective.

(36) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (8) and delivered its opinion on 10 November 2020,

HAVE ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

1. This Regulation lays down temporary and strictly limited rules derogating from certain obligations laid down in Directive 2002/58/EC, with the sole objective of enabling providers of certain number-independent interpersonal communications services ('providers') to use, without prejudice to Regulation (EU) 2016/679, specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services.

2. This Regulation does not apply to the scanning of audio communications.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'number-independent interpersonal communications service' means a number-independent interpersonal communications service as defined in Article 2, point (7), of Directive (EU) 2018/1972;

(2) 'online child sexual abuse material' means:

(a) child pornography as defined in Article 2, point (c), of Directive 2011/93/EU;

(b) pornographic performance as defined in Article 2, point (e), of Directive 2011/93/EU;

(3) ~~'solicitation of children' means any intentional conduct constituting a criminal offence under Article 6 of Directive 2011/93/EU;~~

(4) ~~'online child sexual abuse' means online child sexual abuse material and solicitation of children.~~

Article 3

Scope of the derogation

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

(a) the processing is:

(i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing **known** online child sexual abuse material and reporting it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse ~~and of detecting solicitation of children and reporting it to law enforcement authorities or organisations acting in the public interest~~

~~against child sexual abuse~~;

(ii) proportionate and limited to technologies used by providers for the purpose set out in point (i);

(iii) limited to content data ~~and related traffic data~~ that are strictly necessary for the purpose set out in point (i);

(iv) limited to what is strictly necessary for the purpose set out in point (i);

(b) the technologies used for the purpose set out in point (a)(i) of this paragraph are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 and, to the extent that they are used to **detect possible known online child sexual abuse material** ~~scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse~~;

(c) in respect of any specific technology used for the purpose set out in point (a)(i) of this paragraph, a prior data protection impact assessment as referred to in Article 35 of Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation have been conducted;

(d) with regard to new technology, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services ('users') in the Union before 2 August 2021, ~~and with regard to technology used for the purpose of identifying possible solicitation of children,~~ the provider reports back to the competent authority on the measures taken to demonstrate compliance with written advice issued in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation ('supervisory authority') in the course of the prior consultation procedure;

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

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

(f) ~~(g)~~ the providers:

(i) have established internal procedures to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal ~~and other~~ data;

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

(iii) ensure that material not previously identified **through other means than voluntary detection** as online child sexual abuse material, ~~or solicitation of children,~~ is not reported to law enforcement authorities or organisations acting in the public interest against child sexual abuse without prior human confirmation;

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

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

(vi) inform users of the following, where their content has been removed or their account has been blocked or a service offered to them has been suspended:

(1) the avenues for seeking redress from them;

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

(3) the right to a judicial remedy;

(vii) by 3 February 2022, and by 31 January every year thereafter, publish and submit to the competent supervisory authority and to the Commission a report on the processing of personal data under this Regulation, including on:

(1) the type and volumes of data processed;

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

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

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

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

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

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

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

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

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

(i) reporting, without delay, the suspected online child sexual abuse to the competent law enforcement

and judicial authorities or organisations acting in the public interest against child sexual abuse;

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

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

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

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

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

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

2. Until 3 April 2022, the condition set out in paragraph 1, point (c), shall not apply to providers that:

(a) were using a specific technology before 2 August 2021 for the purpose set out in paragraph 1, point (a)(i), without having completed a prior consultation procedure in respect of that technology;

(b) start a prior consultation procedure before 3 September 2021; and

(c) duly cooperate with the competent supervisory authority in connection with the prior consultation procedure referred to in point (b).

3. Until 3 April 2022, the condition set out in paragraph 1, point (d), shall not apply to providers that:

(a) were using a technology as referred to in paragraph 1, point (d), before 2 August 2021 without having completed a prior consultation procedure in respect of that technology;

(b) start a procedure as referred to in paragraph 1, point (d), before 3 September 2021; and

(c) duly cooperate with the competent supervisory authority in connection with the procedure referred to in paragraph 1, point (d).

4. The data included in the report referred to in paragraph 1, point (g)(vii), shall be provided in writing by means of a standard form. By 3 December 2024 at the latest, the Commission shall determine the content and presentation of that form by means of implementing acts. In doing so, the Commission may divide the data categories listed in paragraph 1, point (g)(vii), into subcategories.

Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 9a(2).

Article 4

European Data Protection Board guidelines

By 3 September 2021, and pursuant to Article 70 of Regulation (EU) 2016/679, the Commission shall request the European Data Protection Board to issue guidelines for the purpose of assisting the supervisory authorities in assessing whether processing falling within the scope of this Regulation, for existing and new technologies used for the purpose set out in Article 3(1), point (a)(i), of this Regulation, complies with Regulation (EU) 2016/679.

Article 5

Effective judicial remedies

In accordance with Article 79 of Regulation (EU) 2016/679 and Article 15(2) of Directive 2002/58/EC, users shall have the right to an effective judicial remedy where they consider that their rights have been infringed as a result of the processing of personal and other data for the purpose set out in Article 3(1), point (a)(i), of this Regulation.

Article 6

Supervisory authorities

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

Article 7

Public list of organisations acting in the public interest against child sexual abuse

1. By 3 September 2021, providers shall communicate to the Commission a list of the names of organisations acting in the public interest against child sexual abuse to which they report online child sexual abuse under this Regulation. Providers shall communicate any changes to that list to the Commission on a regular basis.

2. By 3 October 2021, the Commission shall make public a list of the names of organisations acting in the public interest against child sexual abuse communicated to it under the paragraph 1. The Commission shall keep that public list up to date.

Article 7a

General conditions for imposing administrative fines

The Commission shall impose fines for the infringement or failure to comply with this Regulation which shall in each individual case be effective, proportionate and dissuasive.

Infringements of this Regulation shall be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The exercise by the Commission of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial

remedy and due process.

Article 8

Statistics

1. By 3 August 2022, and on an annual basis thereafter, the Member States shall make publicly available and submit to the Commission reports with statistics on the following:

(a) the total number of reports of detected online child sexual abuse that have been submitted by providers and organisations acting in the public interest against child sexual abuse to the competent national law enforcement authorities, differentiating, where such information is available, between the absolute number of cases and those cases reported several times and the type of provider on whose service the online child sexual abuse was detected;

(b) the number of children identified through actions pursuant to Article 3, differentiated by gender;

(c) the number of perpetrators convicted.

2. The Commission shall aggregate the statistics referred to in paragraph 1 of this Article and shall take them into account when preparing the implementation report pursuant to Article 9.

Article 9

Implementation report

1. On the basis of the reports submitted pursuant to Article 3(1), point (g)(vii), and the statistics provided pursuant to Article 8, the Commission shall, by 4 September **2026** ~~2025~~, prepare a report on the implementation of this Regulation and submit and present it to the European Parliament and to the Council.

2. In the implementation report, the Commission shall consider, in particular:

(a) the conditions for the processing of personal data and other data set out in Article 3(1), point (a)(ii), and points (b), (c) and (d);

(b) the proportionality of the derogation provided for by this Regulation, including an assessment of the statistics submitted by the Member States pursuant to Article 8;

(c) developments in technological progress regarding the activities covered by this Regulation, and the extent to which such developments improve accuracy and reduce the numbers and ratios of errors (false positives).

Article 9a

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a Committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Article 10

Entry into force and application

This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.

It shall apply until 3 April **2027** ~~2026~~.

This Regulation shall be binding in its entirety and directly applicable in all Member States.