Council of the European Union

Brussels, 17 May 2021
(OR. en)

8468/1/21
REV 1

LIMITE

TELECOM 183
COMPET 323
MI 312
DATAPROTECT 118
CONSOM 108
JAI 485
DIGIT 53
FREMP 122
CYBER 125
CODEC 644

Interinstitutional File:
2020/0259(COD)

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. Cion doc.:	10682/20
Subject:	Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online - Analysis of the final compromise text with a view to agreement

I. INTRODUCTION

1. The Presidency has **concluded the negotiations** on the ePrivacy derogation (CSAM), following the successful 5th trilogue held on 29 April.

2. Since its inception, the ePrivacy derogation has been centred on **two principles**:
   - Different technologies require different additional safeguards;
   - This Regulation shall not apply to the scanning of audio communications.

3. Throughout the negotiations, the **guiding objective** behind the Presidency's compromise on EP **safeguards** was to ensure their **feasibility**. No flexibility was shown towards requests that would have blocked or inhibited the use of technology for detecting CSAM or children solicitation. Likewise, compromises on safeguards that would have proven impossible to implement by Member States (or electronic communication providers) were refused.

4. In view of the divergent initial positions from both co-legislators at the beginning of negotiations, the Presidency considers that the **final text is fairly balanced**.

5. The agreement reached is a first reading agreement, i.e. the EP adopts its position first. The text uses the marking of the EP for first reading positions, i.e. new text is marked in **bold** and *italic*, and the deleted text in comparison to the Commission proposal is marked by the sign ▌.

6. In order to offer some guidance on the final 4-column document in annex, this note provides, in the following points, an overview of the concessions made and of the political agreement found on outstanding issues.

II. MAIN ELEMENTS OF THE FINAL COMPROMISE PACKAGE

7. The Presidency recalls that, with a view to finding a compromise further to the EP's requests, concessions were made on the following items:
    - Definitions | Lines 33-48;
        - NIICS | Line 35;
        - Material (CSA) | Line 36;
        - Child pornography | Line 37;
        - Solicitation | Lines 38-44, 46;
        - Pornographic performance | Line 45;
        - Online child sexual abuse | Line 47;
    - No audio communications scanning | Line 32-A;

- Supervisory authorities — MS shall ensure sufficient resources | Line 28-C;
- Mandatory prior DPIA for all technologies | Line 53;
- Mandatory prior consultation of the supervisory authority for all technologies | Line 53;
- Providers' internal procedures to prevent abuse, unauthorized access or transfers | Line 57;
- Data retention | Lines 75, 78 – 80-B;
- Providers report annually to the Supervisory authority and to the Commission | Lines 19, 28-A, 81;
- Public list of NGO´s on the Commission website | Lines 28-A, 101, 102;
- Information to data subjects | Line 62;
- Encryption | Line 25;
- Provider's appropriate procedures and redress mechanisms / complaint mechanism | Lines 16-A, 61;
- Effective remedies | Lines 28-E, 95, 96;
- Protection of professional secrecy | Line 27.

8. Notwithstanding the need to find compromise on the items listed above, at the 5th trilogue, and thanks to significant efforts from both co-legislators, a common understanding was found on all major outstanding issues, notably:
   - **"Enhanced prior consultation"** (ex-Prior authorisation) **for anti-grooming technology** | Lines 54, 54-E-54H — Providers will be asked "to demonstrate compliance with written advice [...] issued by the competent supervisory authority", instead of having to request an authorisation before using the anti-grooming technology;
   - **Reporting of reasoned suspicion of CSA** | Line 86 — Providers may report "without delay" to NGOs that are active in the fight against CSA as an alternative to law enforcement authorities (LEAs);

- Nature of the text (**derogation v. restriction**) — Thanks to some extra safeguards, the EP acknowledged the nature of the instrument as a derogation;
- **MS statistics** | Lines 103-111 — In line with our mandate we have achieved a grace period of 12 months;
- **Time of application** | Lines 22, 123 — It was agreed that the time of application would be three years from the entry into application of the Regulation, and the Commission's reporting to EP and Council after two years.
- **Anti-grooming technologies** | Lines 8, 16, 52, 72 — The EP accepted our compromise proposal, which limits the goal of scanning text in communications to the identification of child solicitation, based on "risk factors such as age difference and the likelihood of involvement of a child in the scanned communication".

III. CONCLUSION

9. The Permanent Representatives Committee is invited to:
   - Approve the final compromise text set out in the Annex of this note, subject to legal-linguistic revision;
   - Authorise the Presidency to inform the European Parliament that, should the European Parliament adopt its position at first reading, in accordance with Article 294 paragraph 3 of the Treaty, in the form set out in the compromise package contained in the Annex to this note (subject to legal/linguistic revision by both institutions), the Council would, in accordance with Article 294, paragraph 4 of the Treaty, approve the European Parliament's position and the act shall be adopted in the wording which corresponds to the European Parliament's position.

ANNEX

REGULATION (EU) 2021/...
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of ...

on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online

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,

[1] OJ C , , p. .

Whereas:

(1) Directive 2002/58/EC of the European Parliament and of the Council[2] 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[3].

(2) Directive 2002/58/EC applies to the processing of personal data in connection with the provision of publicly available electronic communication services. ***Up 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[4] ***applied***. ***On that date,*** Directive (EU) 2018/1972 of the European Parliament and of the Council[5] ***repealed*** Directive 2002/21/EC ▌. ▌ The definition of electronic communications services ▌ in Article 2(4) of Directive (EU) 2018/1972 ▌ includes number-independent interpersonal communications services as defined in Article 2(7) of that Directive. Those services, which include, for example, voice over IP, messaging and web-based e-mail services, ***have*** therefore ***been*** within the scope of Directive 2002/58/EC, as of 21 December 2020.

---

2 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) (OJ L 201, 31.7.2002, p. 37).

3 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) (OJ L 119, 4.5.2016, p. 1).

4 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

5 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(3) In accordance with Article 6(1) of the Treaty on European Union, the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union. Article 7 of the Charter of Fundamental Rights of the European Union ("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 protection of personal data. ***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. ***Articles 3(3) of the UNCRC and 24(1) of the Charter furthermore evoke the right of children to protection and care as is necessary for their well-being.***

(4) ***The protection of children 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 1989 United Nations Convention on the Rights of the Child and by the Charter. Digitisation has brought about many benefits for society and the economy, but also challenges including an increase of ***online*** child sexual abuse ▌. The protection of children online is one of the Union's priorities. On 24 July 2020, the Commission adopted an EU strategy for a more effective fight against child sexual abuse[6] ("the Strategy"), which aims to provide an effective response, at Union level, to the crime of child sexual abuse.

(4a) In line with Directive (EU) 2011/93/EU, 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.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final.

(5) Certain providers of number-independent interpersonal communications services, such as webmail and messaging services, are already using specific technologies***,*** 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 ▌ on a voluntary basis 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 these activities could be hashing technology for images and videos and classifiers and artificial intelligence for analysing text or traffic data. When using hashing technology, the 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 'hash' from a database containing verified online*** child sexual abuse material ***and maintained by an organisation acting in the public interest against child sexual abuse. The providers*** refer to national hotlines for reporting ***online*** child sexual abuse material, as well as to organisations whose purpose is to ***identify children and*** reduce child sexual exploitation ***and sexual abuse***, and prevent child victimisation, located both within the Union and in third countries. ***Such organisations may 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***, and reducing the further dissemination of ***online*** child sexual abuse material, while also contributing to the identification and investigation of offenders, and the prevention***, detection, investigation and prosecution*** of child sexual abuse offences.

(5a) Notwithstanding their legitimate objective, these activities constitute an interference with the fundamental rights to respect for private and family life and protection of personal data of all users. Any limitation to the fundamental right to respect for private and family life, including the confidentiality of communications, cannot be justified merely on the ground that certain technologies were previously deployed when the services concerned did not, from a legal perspective, constitute electronic communications services. Such interference is only possible under certain conditions. It needs to be provided for by law, respect the essence of the rights to private and family life and to the protection of personal data and, in compliance with the principle of proportionality, be necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others as enshrined in Article 52 (1) of the Charter. Where such measures permanently involve a general and indiscriminate monitoring and analysis of communications of all users, they interfere with the right to confidentiality of communications.

(6) Until 20 December 2020, the processing of personal data by providers of number-independent interpersonal communications services by means of voluntary measures for the purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material ***was*** governed ***solely*** by Regulation (EU) 2016/679. ***Directive (EU) 2018/1972, which had to be transposed by that date, brought providers of number-independent interpersonal communications services within the scope of Directive 2002/58/EC. In order to continue using such voluntary measures after 20 December 2020, providers of number-independent interpersonal communications services 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.***

(7) Directive 2002/58/EC does not contain any specific provisions concerning the processing of personal ▌ data in connection with the provision of electronic communication services for the purpose of detecting and reporting ***online*** child sexual abuse ▌ and removing child sexual abuse material. However, pursuant to Article 15(1) of Directive 2002/58/EC, Member States may 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 purpose of prevention, investigation, detection 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***, those voluntary measures of*** providers of number-independent interpersonal communications services ***can no longer rely on Regulation (EU) 2016/679*** to continue to detect and report ***online*** child sexual abuse ▌ and 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 number-independent interpersonal communications services for the sole purpose of detecting and reporting online child sexual abuse and removing online child sexual abuse material from their services, but it provides for a derogation from certain provisions of Directive 2002/58/EC. It also lays down additional safeguards to be respected by the providers of number-independent interpersonal communication services if they wish to rely on this Regulation.***

(7a) The processing for the purposes of this Regulation could entail the processing of special categories of personal data under Article 9 of Regulation (EU) 2016/679. Where the processing of images and videos through specific technical means allows for the unique identification or authentication of a natural person, it is considered as processing of special categories of personal data.

(8) This Regulation therefore 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 number-independent interpersonal communications services of technologies for the processing of personal and other data to the extent necessary to detect and report*** *online* ***child sexual abuse and remove online child sexual abuse material falls within the scope of the derogation provided that it 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.*** Since Directive 2002/58/EC was adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union, it is appropriate to adopt this Regulation on the same legal basis. Moreover, not all Member States have adopted legislative measures at national level to restrict the scope of the rights and obligations provided for in those provisions in accordance with Article 15 (1) of Directive 2002/58/EC, and the adoption of such measures involves a significant risk of fragmentation likely to negatively affect the internal market.

(9) Given that ***data related to*** electronic communications involving natural persons will normally qualify as personal data, this Regulation should also be based on Article 16 of the Treaty ***on the Functioning of the European Union***, 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 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.

(10) To the extent that processing of personal data in connection with the provision of electronic communications services by number-independent interpersonal communications services for the sole purpose of detecting and reporting ***online*** child sexual abuse ▌ and removing ***online*** child sexual abuse material falls within the scope of the derogation provided for by this Regulation, Regulation (EU) 2016/679 applies to such processing ▌ .

(11) ▌ The types of technologies deployed should be the least privacy-intrusive in accordance with the state of the art in the industry***. They*** should not ***be used for*** systematic filtering and scanning of ▌ text ***in*** communications ***other than solely to detect patterns which point to possible*** concrete elements of suspicion of online child sexual abuse ***without being able to deduce the substance of the content. In the case of technology used for identifying solicitation, such concrete elements of suspicion should be based on objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication.***

(11a) Appropriate procedures and redress mechanisms should be in place to ensure that individuals can lodge complaints with the provider of a number-independent interpersonal communications service. This is 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 online child sexual abuse.

(12) In order to ensure accuracy and reliability as much as possible, the technology used should, in accordance with the state of the art in the industry, be such as to limit the error rate of false positives to the maximum extent possible and, where necessary, to rectify without delay any such errors that may nonetheless occur.

(13) ***The content and traffic data processed, and personal data generated*** when carrying out the activities covered by ▌ this Regulation, as well as the period during which the data is subsequently ***stored*** in case of ***identification of suspected child sexual abuse,*** should ***remain*** limited to what is strictly necessary ***to carry out those activities. When no longer strictly necessary for one of the purposes specified in this Regulation, including where no suspected online child sexual abuse is identified, any data should be immediately and irrevocably deleted, and in any event after expiration of the time period of twelve months for specific purposes as specified. This should be without prejudice to the possibility to store relevant content and traffic data in accordance with Directive 2002/58/EC. This Regulation does not affect the application of any legal obligation under EU or Member State law to preserve data that may apply to the provider concerned.***

(13a) This Regulation does not prevent providers from requesting a proof of receipt by law enforcement authorities after reporting child sexual abuse online to them.

(14) In order to ensure transparency and accountability in respect of the activities undertaken pursuant to the derogation***, provided for by this Regulation, interpersonal communications service*** providers should publish ***and submit*** reports ***to the supervisory authority as determined in accordance with Regulation (EU) 2016/679 and to the Commission by ... [six months after the entry into force of this Regulation], and thereafter by 31 January every year,*** on the processing falling within the scope of this Regulation, including on the type and volumes of data processed, ***the specific ground relied on for the processing of personal data pursuant to Regulation (EU) 2016/679, the ground 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 identified**,** ***differentiating between child sexual abuse material and solicitation, 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 those proceedings***, the numbers and ratios of errors (false positives) of the different technologies deployed, 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 as well as the names of the organisations acting in the public interest against child sexual abuse with whom data has been shared pursuant to this Regulation.***

(14a) In order to support the responsible supervisory authorities in their task, the Commission should request the European Data Protection Board to issue guidelines on compliance with Regulation (EU) 2016/679 of processing falling within the scope of the derogation laid down in this Regulation. Those guidelines should in particular assist the supervisory authorities in providing advice in the framework of the prior consultation procedure set out in Article 36 of Regulation (EU) 2016/679, which is to be carried out when assessing whether an established or new technology to be used is state of the art, the least privacy-intrusive and operating on an adequate legal basis under Regulation (EU) 2016/679.

(16) This Regulation restricts the right to protection of the confidentiality of communications and derogates from the decision taken in Directive (EU) 2018/1972 to subject number-independent interpersonal communications services to the same rules as all other electronic communications services as regards privacy ***for the sole purpose of detecting and removing online child sexual abuse material and reporting it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to law enforcement authorities or organisations acting in the public interest against child sexual abuse***. 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. In case the long-term legislation is adopted and will enter into force before that date, that legislation should repeal this Regulation.

(17) ***With regard to all other activities that fall within the scope of Directive 2002/58/EC,*** providers of number-independent interpersonal communications services 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***.

(17b) End-to-end encryption is an important tool to guarantee secure and confidential 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.

(17c) 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 as well as in communications between victims and their lawyers.

(17ca) This Regulation is 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, journalists and their sources, or lawyers and their clients - in particular since confidentiality of communication 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 - including national rules on registers on public authorities or organisations which offer counselling to individuals in distress.

(18) 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, national legislation would most probably not be adopted in time in all Member States. As this objective 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 of the Treaty on European Union. 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 those objectives. 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 objectives.

(18a) The providers of number-independent interpersonal communications services 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 of number-independent interpersonal communication services 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 and may also be used by the providers of number-independent interpersonal communications services to identify ~~trusted~~ relevant organisations in the global fight against online child sexual abuse. That list is without prejudice to the obligations of the providers of number-independent interpersonal communications services acting as controllers under Regulation (EU) 2016/679, including with regards to their obligation to conduct any transfer of personal data outside the Union pursuant to Chapter V of Regulation (EU) 2016/679 and their obligation to fulfil all of the obligations under chapter IV of that Regulation.

(18b) Statistics as set out in Article 3g are important indicators for the evaluation of policy, including legislation. 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 may have been circulating for years and which is not fully reflected in such statistics.

(18c) 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 also ensure that supervisory authorities have such sufficient resources for the effective performance of their tasks and exercise of their powers under this Regulation.

(18ca) 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.

(18d) Users should have a right to effective judicial remedy where their rights have been infringed as a result of the processing of personal and other data for the purposes of detecting and reporting child sexual abuse online and removing child sexual abuse material on those services, for instances where the users' 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 the users' content has been removed or their account has been blocked or a service offered to them has been suspended.

(18e) It is appropriate to specify that, in line with Directive 2002/58/EC and the principle of data minimisation, the processing of personal data should remain limited to the categories of content data and related traffic data, in as far as strictly necessary to achieve the purpose of this Regulation.

(18f) The present derogation extends to the categories of data referred to in Article 5(1) and 6(1) 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.

(19) 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[7] and delivered its opinion on ***10 November 2020,***

HAVE ADOPTED THIS REGULATION:

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 (OJ C 20, 21.1.2019, p. 1).

Article 1

Subject matter ***and scope***

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 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 and report child sexual abuse online and remove child sexual abuse material on their services.

1a. This Regulation shall not apply to the scanning of audio communications.

Article 2

Definitions

For the purpose 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(7) of Directive (EU) 2018/1972;

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

(a) material constituting child pornography as defined in Article 2, point (c), of Directive 2011/93/EU of the European Parliament and of the Council;

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

(2a) 'solicitation of children' means any intentional conduct constituting a criminal offense under Article 6 of Directive 2011/93/EC;

(2b) 'online child sexual abuse' means 'online child sexual abuse material' and 'solicitation of children'.

Article 3

Scope of the derogation

▌ Article 5(1) and Article 6***(1)*** of Directive 2002/58/EC shall not apply to the ***confidentiality of communications involving*** the processing of personal and other data in connection with the provision of number-independent interpersonal communications services ***where the processing is*** strictly necessary for the use of ***specific*** technology for the sole purpose of ***detecting and*** removing ***online*** child sexual abuse material and ▌ reporting ***it*** to law enforcement authorities and to organisations acting in the public interest against child sexual abuse ***and for detecting online solicitation of children and reporting it to law enforcement authorities or organisations acting in the public interest against child sexual abuse*** provided that:

(a) the processing is proportionate and limited to ▌ technologies ▌ used by providers of number-independent interpersonal communications services for that ***sole*** purpose and ***provided*** that:

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

(ii) ***in respect of any specific technology used for that purpose, a prior data protection impact assessment and a prior consultation procedure have been conducted pursuant to Articles 35 and 36 of Regulation (EU) 2016/679;***

(iii) ***in respect of new technology, that is, technology used for the purpose of the detection of child sexual abuse material that has not been used by any provider in relation to services provided to users in the Union before the date of entry into force of this Regulation and of technology used for the purpose of identifying possible solicitation of children, the provider reports back to the competent authority about 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 in the course of the prior consultation procedure.***

1a. The condition relating to the prior consultation procedure set out in point (ii) of paragraph 1(a) shall, until [date of entry into force of this Regulation + 8 months], not apply to providers that:

(a) were using a specific technology referred to in that point before [date of entry into force of this Regulation] without previously completed a consultation procedure in respect of that technology;

(b) start such a consultation procedure before [date of entry into force + 1 month]; and

(c) duly cooperate with the competent supervisory authority in connection to that consultation procedure.

1b. The condition set out in point (iii) of paragraph 1(a) shall, until [date of entry into force of this Regulation + 8 months], not apply to providers that:

(a) were using a technology referred to in that point before [date of into force of this Regulation] without having previously completed a consultation procedure in respect of that technology;

(b) start a procedure under point (iii) before [date of entry into force + 1 month]; and]

(c) duly cooperate with the competent supervisory authority in connection to the procedure under point (iii);

(aa) the processing of personal data is limited to content data and related traffic data that is strictly necessary for the purpose set out in paragraph 1;

(ab) the provider of the number-independent interpersonal communications service has established internal procedures to prevent abuse, unauthorised access and transfers;

(ac) the provider of the number-independent interpersonal communications services ensures human oversight of, and, where necessary, intervention in the processing of personal data using technologies falling under this Regulation, and ensures that no report of material not previously identified as child sexual abuse or of solicitation is sent to law enforcement authorities or organisations acting in the public interest against child sexual abuse without prior human confirmation;

(ad) the provider of a number-independent interpersonal communications service has established appropriate procedures and redress mechanisms to ensure that individuals can lodge complaints with it within a reasonable timeframe for the purpose of presenting their views;

(ae) the end-users are informed in a clear, prominent and comprehensible way that the provider invokes the legal derogation, in accordance with this Regulation, from Articles 5(1) and 6(1) of Directive 2002/58/EC concerning the confidentiality of their communications, for the sole purpose of detecting, removing or reporting child sexual abuse online, the logic behind such measures and the impact on users' communications confidentiality, including the possibility that personal data is shared with law enforcement authorities and organisations acting in the public interest against child sexual abuse;

(af) where the end-user's content has been removed or their account has been blocked or a service offered to them has been suspended, the provider of a number-independent interpersonal communications service shall inform the end-user of:

(b) the avenues for redress with the provider of number-independent interpersonal communications services; and

(c) the possibility of lodging a complaint with a supervisory authority and of the right to a judicial remedy;

(b) the technology used is in itself sufficiently reliable in that it limits to the maximum extent possible the rate of errors regarding the detection of content representing child sexual abuse, and where such occasional errors occur, their consequences are rectified without delay;

(c) the technology used to detect ***patterns of possible*** solicitation of children is 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;

(d) the processing ***allowed by the derogation provided for in this Regulation*** is limited to what is strictly necessary for the ***sole*** purpose of detection and reporting of ***online*** child sexual abuse ***and removal of online child sexual abuse material***;

(db) where suspected online child sexual abuse has been identified, the strictly necessary content data, related traffic data, as well as personal data generated through such processing, are stored in a secure manner, solely for the following purposes:

(i) in order to report, 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) in order to block the account of, or suspend or terminate the provision of the service to, the user concerned;

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

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

(v) in order to respond 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, investigation, detection or prosecution of criminal offences set out in Directive 2011/93/EU; and

(dc) the data are stored no longer than strictly necessary for the relevant purpose specified in point (db) and in any event no longer than 12 months from the date of the identification of the suspected online child sexual abuse;

(e) the provider ▌ publishes ***and submits*** a report ***to the supervisory authority as determined by Regulation (EU) 2016/679 and to the Commission, by ... [six months after the date of entry into force of this Regulation], and thereafter by 31 January every year, of the*** processing ***of personal data under this Regulation,*** including ▌ the type and volumes of data processed, ***the specific ground relied on for the processing pursuant to Regulation (EU) 2016/679, the legal ground 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 child sexual abuse online differentiating between child sexual abuse material and solicitation*** identified***, 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 those proceedings,*** numbers and ratios of errors (false positives) of the different technologies deployed, 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, as well as the names of the organisations acting in the public interest against child sexual abuse with whom data has been shared pursuant to this Regulation;***

(ea) 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.

Article 3a

European Data Protection Board guidelines

By ... [one month after the date of entry into force of this Regulation], 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 responsible in accordance with Regulation (EU) 2016/679 to assess whether the processing falling within the scope of this Regulation, for existing as well as future technologies, used for the sole purpose of combatting online child sexual abuse complies with Regulation (EU) 2016/679.

Article 3d

Effective remedies

In accordance with Article 79 of Regulation 2016/679 and Article 15, paragraph 2, of Directive 2002/58, users of number-independent interpersonal communications services 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 purposes of detecting and reporting child sexual abuse online and removing child sexual abuse material on those services.

Article 3e

Supervisory authorities

The supervisory authorities designated pursuant to Chapter VI 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 3f

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

By ... [two months of the date of entry into force of this Regulation], the Commission shall make public the names of organisations acting in the public interest against child sexual abuse to which the providers of public independent interpersonal communications services have indicated that they report child sexual abuse online under this Regulation. The providers shall communicate the names of these organisation to the Commission by .... [one month after the entry into force of this Regulation] and any modifications thereto regularly. The Commission shall keep that public list up to date.

Article 3g

Statistics

1. By .... [12 months after entry into force of Regulation], and on annual basis thereafter, the Member States shall make publicly available and submit reports to the Commission with statistics on the following elements:

(a) the total number of reports of detected online child sexual abuse that have been provided by number-independent interpersonal communications services and organisations acting in the public interest against child sexual abuse to the competent national law enforcement authorities, differentiating, where this information is available, between the absolute number of cases and those cases reported several times and the type of provider of number-independent interpersonal communications services where the online child sexual abuse was detected;

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

(d) 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 3h.

Article 3h

Implementation report

1. On the basis of the reports provided pursuant to Article 3(1), point(e), and the statistics provided pursuant to Article 3g, the Commission shall, by …[two years after entry into force of Regulation], prepare a report on the implementation of this Regulation and submit and present it to the European Parliament and to Council.

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

(a) all conditions for the processing of personal data and other data enumerated under Article 3, point (a);

(b) the proportionality of the derogation provided for by this Regulation, including an assessment of the statistics submitted by the Member States under Article 3g;

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

Article 4

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 ***... [three years from the date of entry into force]***.

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*