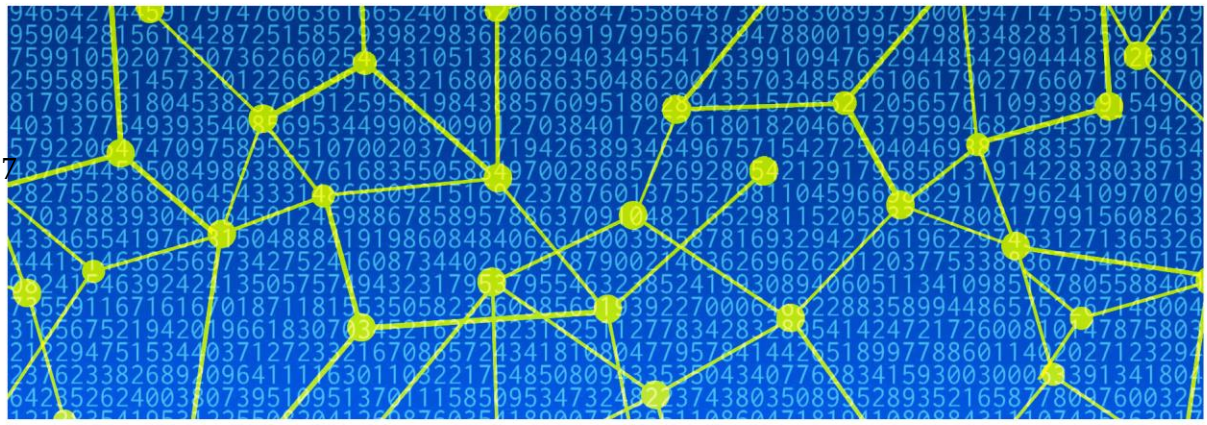

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2020

on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online

EDPS

10 November 2020

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Wiewiorówski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under Article 42(1) of Regulation (EU) 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data' and under Article 57(1)(g), the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.

This Opinion is issued by the EDPS, within the period of eight weeks from the receipt of the request for consultation laid down under Article 42(3) of Regulation (EU) 2018/1725, having regard to the impact on the protection of individuals' rights and freedoms with regard to the processing of personal data of the Commission 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.

Executive Summary

On 10 September 2020, the Commission published a Proposal for a Regulation on a temporary derogation from certain provisions of the ePrivacy Directive 2002/58/EC 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 derogation concerns Articles 5(1) and 6 of the ePrivacy Directive in relation to the processing of personal data in connection with the provision of 'number-independent interpersonal communications services' necessary for the use of technology for the sole purpose of removing child sexual abuse material and detecting or reporting child sexual abuse online to authorities.

In this Opinion the EDPS provides his recommendations related to the Proposal in response to a formal consultation by the Commission pursuant to Article 42 of Regulation (EU) 2018/1725.

In particular, he notes that the measures envisaged by the Proposal would constitute an interference with the fundamental rights to respect for private life and data protection of all users of very popular electronic communications services, such as instant messaging platforms and applications. **Confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life**. **Even voluntary measures by private companies constitute an interference with these rights** when the measures involve the monitoring and analysis of the content of communications and processing of personal data.

The EDPS wishes to underline that the issues at stake are not specific to the fight against child abuse but to any initiative aiming at collaboration of the private sector for law enforcement purposes. If adopted, the Proposal, will inevitably serve as a precedent for future legislation in this field. The EDPS therefore considers it essential that the Proposal is not adopted, even in the form a temporary derogation, until all the necessary safeguards set out in this Opinion are integrated.

In particular, in the interest of legal certainty, the EDPS considers that it is necessary to clarify whether the Proposal itself is intended to provide a legal basis for the processing within the meaning of the GDPR, or not. If not, the EDPS recommends clarifying explicitly in the Proposal which legal basis under the GDPR would be applicable in this particular case. In this regard, the EDPS stresses that **guidance by data protection authorities cannot substitute compliance with the requirement of legality**. It is insufficient to provide that the temporary derogation is "without prejudice" to the GDPR and to mandate prior consultation of data protection authorities. The co-legislature must take its responsibility and ensure that the proposed derogation complies with the requirements of Article 15(1), as interpreted by the CJEU.

In order to satisfy the requirement of proportionality, **the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse**.

Finally, the EDPS is of the view that the five-year period as proposed does not appear proportional given the absence of (a) a prior demonstration of the proportionality of the envisaged measure and (b) the inclusion of sufficient safeguards within the text of the legislation. He considers that the validity of any transitional measure should not exceed 2 years.

TABLE OF CONTENTS

I. Table of Contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)[1],

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[3],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1 Background

1. On 24 July 2020, the Commission adopted a Communication *EU strategy for a more effective fight against child sexual abuse*.[4] The Communication notes that as from December 2020, Directive 2002/58/EC ('the e-Privacy Directive')[5] will have an extended scope as a result of the already adopted Electronic Communications Code ('ECC')[6]. The ECC extends the scope of the e-Privacy Directive to over the top (OTT) inter-personal communication services such as messaging services and email. According to the Communication, this would prevent certain companies (in the absence of national legislative measures adopted in accordance with Article 15(1) of the e-Privacy Directive) from continuing their own voluntary measures for detection, removal and reporting of child sexual abuse online.[7]

2. On 10 September 2020, the Commission published[8] a Proposal for an Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse, which provides for a temporary derogation from Article 5(1) and Article 6 of the ePrivacy Directive ('the Proposal'). The Commission considers that such a derogation is

necessary in order to allow current voluntary activities to continue after December 2020. The derogation would concern the processing of personal data in connection with the provision of '*number-independent interpersonal communications services*'[9] (e.g., voice over IP, messaging and web-based e-mail services) strictly necessary for the use of technology for the sole purpose of removing child sexual abuse material and detecting or reporting child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse. The Proposal enumerates a number of conditions for the derogation to be applicable, which will be analysed later in this Opinion.

3. The EDPS was formally consulted by the Commission on 16 September 2020. On 30 September, the Commission launched a public consultation inviting feedback in relation to its Proposal.

1.2 Relationship to Directive 2011/93/EU

4. The EU has previously adopted a comprehensive legal instrument to combat the sexual abuse and sexual exploitation of children and child pornography, namely Directive 2011/93/EU ('Child Sexual Abuse Directive').[10]

5. The Child Sexual Abuse Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children and child sexual abuse material. It requires Member States to ensure that inter alia the following intentional conduct, when committed without right[11], shall be punishable:

   - intentionally and knowingly obtaining access, by means of information and communication technology, to child pornography;
   - distribution, dissemination or transmission of child pornography
   - offering, supplying or making available child pornography.[12]

6. The Child Sexual Abuse Directive also obliges Member States to take the necessary measures to ensure that certain conduct amounting to solicitation of children for sexual purposes, including by means of information and communication technology, shall be punishable.

7. The Child Sexual Abuse Directive requires Member States to take the necessary measures to ensure the prompt *removal of web pages* containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory as well as to seize and confiscate instrumentalities and proceeds from such offences.[13] In addition, Member States may take measures to *block access to web pages* containing or disseminating child pornography towards the Internet users within their territory.[14]

8. In 2010, the EDPS issued an own-initiative Opinion on the proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography.[15] This Opinion contains considerations and recommendations that are also relevant to the Proposal for an Interim Regulation. Where appropriate, the EDPS shall reiterate and/or make reference to his 2010 Opinion.

2. MAIN RECOMMENDATIONS

9. Confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life and protection of personal data. Even voluntary measures by private companies **constitute an interference** with these rights when the measures involve the monitoring and analysis of the content of communications and processing of personal data. The measures envisaged by the Proposal will interfere with the rights to respect for private life and data protection of the individuals concerned (users, perceived perpetrators and victims).

10. Interference with confidentiality of communications is possible, but only under certain conditions**.** Limitations may be made only if they are **provided for by law, respect the essence** of the rights to data protection and privacy and, in compliance with the principle of proportionality, are **necessary and genuinely meet objectives of general interest** recognised by the Union or the need to protect the **rights and freedoms of others** (Article 52(1) of the Charter).[16]

11. The Commission maintains that the Proposal **merely seeks to** allow **the continuation of certain existing voluntary practices**, rather than create a new interference with fundamental rights. However, the temporary derogation is proposed precisely because of the extended scope of the ePrivacy Directive resulting from the entry into force of the EECC in December 2020. The EDPS wishes to underline that it was the choice of the European legislator to expand the notion of *"electronic communications service"* to include functionally equivalent online services in order to ensure that end-users and their rights are effectively and equally protected when using those services.[17] Limitations upon the confidentiality of communications cannot be justified merely on the grounds that certain measures were previously deployed when the services concerned did not, from a legal perspective, amount to electronic communications services. The services in question will from 21 December 2020 qualify as electronic communication services, with the attendant legal protection of confidentiality. The proposed derogation must therefore be assessed in accordance with the requirements of Article 52 of the Charter.

12. The EDPS wishes to underline that the issues at stake are **not specific to the fight against child abuse** but to any initiative aiming at collaboration of the private sector for law enforcement purposes.[18] Child abuse is a particularly abhorrent crime and the objective of enabling effective action to combating child sexual abuse online clearly amounts to both an objective of general interest recognised by the Union and seeks to protect the rights and freedoms of others.[19] As regards effective action to combat criminal offences committed against minors and other vulnerable persons, the CJEU has pointed out that **positive obligations** may result from Article 7 of the Charter, requiring public authorities to **adopt legal measures** to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment.[20]

13. The EDPS already previously **questioned purely voluntary mechanisms** to combat the dissemination of child abuse material, given the nature of the interference and the need for legal certainty for all actors involved.[21] Indeed, there is a need to ensure **harmonised, clear**

and detailed procedures when fighting illegal content, under the supervision of independent public authorities.

14. Even if the Proposal does not *oblige* private parties to interfere with the confidentiality of communications, it nevertheless provides for a restriction of the confidentiality of communications. Given the nature of the interference at hand, the EDPS considers that the measures to detect, remove and report child sexual abuse online must be accompanied by **a comprehensive legal framework** which meets the requirements of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. In order to satisfy the requirement of proportionality, the legislation must lay down **clear and precise rules governing the scope and application of the measures** in question and imposing **minimum safeguards**, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse.[22] That legislation must be legally binding and, in particular, must indicate **in what circumstances and under which conditions** a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is **limited to what is strictly necessary**.[23] As clarified by the CJEU, the need for such safeguards is all the greater where personal data is subjected to automated processing and where the protection of the particular category of personal data that is sensitive data is at stake.[24]

15. The introduction of **appropriate safeguards** in the Proposal itself is all the more necessary as it concerns a Regulation rather than a Directive. The choice for a legal instrument that is directly applicable in all Member States entails the responsibility of EU legislator for ensuring that the appropriate safeguards are introduced already at EU level.

3. SPECIFIC RECOMMENDATIONS

3.1. Legal basis

16. Recital (10) of the Proposal indicates that the Regulation (EU) 2016/679 ('GDPR')[25] remains applicable to the processing of personal data falling within the scope of the derogation. In accordance with Article 6 GDPR, the processing of personal data shall be lawful only on the basis of one of six specified grounds set out in Article 6(1)(a) to (f).

17. The Proposal does not clearly indicate whether or not it seeks to provide a legal basis within the meaning of article 6 GDPR. The Explanatory Memorandum merely notes that the ePrivacy Directive "*does not contain an explicit legal basis*" for voluntary processing of content or traffic data for the purpose of detecting child sexual abuse online. It also notes that, in the absence of legislative measures providing for a derogation, providers of number-independent interpersonal communications services "*would lack a legal basis*" for continuing to detect child sexual abuse on their services.[26]

18. For the sake of legal certainty, the EDPS considers that it is necessary to **clarify** whether the Proposal itself is intended to provide a **legal basis** for the processing within the meaning of the GDPR, or not. If not, the EDPS recommends clarifying explicitly in the Proposal which legal basis of the GDPR would be applicable in this particular case.

19. In this regard, the EDPS notes that the derogation provided by the Proposal concerns the *voluntary* processing of content or traffic data for the purpose of detecting child sexual abuse online. In other words, it would not oblige providers of number-independent interpersonal communications services to carry out any processing. As a result, the legal basis for the processing cannot be found in Article 6(1)c GDPR (processing necessary for compliance with a legal obligation to which the controller is subject).

20. In its 2014 Opinion on the notion of legitimate interests of the data controller, the Article 29 Working Party considered that the legitimate interests pursued by the controller *"may include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as child grooming. In these situations, however, it is particularly important to ensure that the limits of Article 7(f) are fully respected"*.[27]

21. The EDPS observes that the aforementioned statement does not entail that *any* processing carried out to combat illegal activities may automatically be considered as lawful under Article 6(1)f GDPR. First, the processing in question must satisfy three cumulative conditions, namely (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.[28] Second, the statement by the Article 29 Working Party was made in general terms, without any suggestion that controllers might be allowed to rely on the lawful basis of legitimate interest in cases which interfere with the confidentiality of communications.

3.2. Necessity and proportionality

22. Due to the absence of an impact assessment accompanying the Proposal, the Commission has **yet to demonstrate** that the measures envisaged by the Proposal are **strictly necessary, effective and proportionate** for achieving their intended objective. The EDPS in first instance calls upon the Commission to provide additional information to enable the co-legislator to consider whether the envisaged measures in fact satisfy the requirements of necessity, effectiveness and proportionality.[29]

23. In order to be able to assess the impact of a measure on the fundamental rights to privacy and to the protection of personal data, it is particularly important to precisely identify[30]:

- the **scope** of the measure, including the number of people affected and whether it raises *'collateral intrusions'* (i.e. interference with the privacy of persons other than the subjects of the measure);
- the **extent** of the measure, including amount of information collected; for how long; whether the measure under scrutiny requires the collection and processing of special categories of data;
- the **level of intrusiveness**, taking into account: the **nature of the activity** subjected to the measure (whether it affects activities covered by duty of confidentiality or not, lawyer-client relationship; medical activity); the **context**; whether it amounts to

profiling of the individuals concerned or not; whether the processing entails the use of (partially or fully) **automated** decision making system with a 'margin of error';

- whether it concerns **vulnerable** persons or not;
- whether it **also affects other fundamental rights** (for instance the right to protection of privacy and the right to freedom of expression, as in the *Digital Rights* and *Tele2* cases).

In this context, it is also important to note that the impact can be minor with regard to the individual concerned, but nonetheless significant or highly significant collectively/for society as a whole.[31]

24. The EDPS observes that different measures to combat child sexual abuse online may involve **different levels of intrusiveness**. As a preliminary matter, the EDPS observes that automated analysis of speech or text with a view of identifying potential instances of child solicitation is likely to constitute a more significant interference than the matching of images or video on the basis of previously confirmed instances of child pornography.

25. Recital (11) of the Proposal stipulates that *"[t]he types of technologies deployed should be the least privacy-intrusive in accordance with the state of the art in the industry and should not include systematic filtering and scanning of communications containing text but only look into specific communications in case of concrete elements of suspicion of child sexual abuse*." While the EDPS welcomes the underlying intention to delineate the scope of the interference, a number of observations need to be made. First, any delineation affecting the **scope of the interference should be reflected clearly in the text** of the Proposal itself and not only in a recital. Second, it should be made explicit whether **communications containing data other than text** (e.g. image or audio communications) would be allowed to be subject to systematic filtering and monitoring. Third, there needs to be clarity as to **how "*concrete elements of suspicion*" will be established in practice,** and in particular whether such a determination involves a competent authority or not.

26. As regards technology to detect child solicitation, Article 3(c) of the Proposal states that the technology used must be "*limited to the use of relevant key indicators, such as keywords and objectively identified risk factors such as age difference, without prejudice to the right to human review*". In this regard, the EDPS considers that the **general, indiscriminate and automated analysis of all text-based communications transmitted through number-independent interpersonal communications services with a view of identifying new potential infringements does not respect the principle of necessity and proportionality**. Even if the technology used is limited to the use of *"relevant key indicators"*, the EDPS considers the deployment of such general and and indiscriminate analysis is excessive.

27. As regards the **"*right to human review*"** mentioned in Article 3(c) of the Proposal, the EDPS urges the co-legislator to provide further clarity as when such a right would become applicable and which entity would be in charge of carrying out this review. This is particularly important in terms of ensuring appropriate **redress mechanisms** (see also section 6.5 [reporting to public authorities] and 6.6 [transparency and data subject rights]). Finally, the use of the term *"right"* suggests that human review would not be implemented by default. The EDPS urges the legislature to specify in which circumstances human review will be ensured and by whom. This is all the more necessary to clarify in which

circumstance the use of the technology **could amount to automated decision-making** within the meaning of Article 22 GDPR (in particular given the possible consequences of both reporting and user blocking envisaged by the Proposal).

3.3. Scope and extent of the derogation

28. The Proposal extends to *'number-independent interpersonal communications services'*. Such services include a wide variety of services, such voice over IP, messaging and web-based e-mail services. Further clarity should be provided regarding the **types of services** that would affected by the derogation. For example, it should be unambiguously stated whether the derogation concerns measures to detect child sexual abuse materials consisting of video and images or also to text messages and voice calls. This is necessary to satisfy the requirement that the legislation must lay down *clear and precise* rules governing the scope and application of the measure.

29. In the same vein, more clarity is needed as to the **types of detection measures** that would fall within the scope of the derogation. Article 3 of the Proposal sets out a number of conditions for the derogation to be applicable, yet does not offer a clear description of the types of the measures envisaged.[32] Article 3(c) indicates that "*key indicators, such as keywords and objectively identified risk factors such as age difference*" would be used to detect solicitation of children, whereas Article 3(e) *in fine* implies that the detection of child pornography may involve the "*use of a non-reconvertible digital signature ('hash')*". A clear understanding of the precise nature of the measures limiting the confidentiality of communications is necessary not only with a view to ensuring clarity and legal certainty, but also with a view to assessing whether the measures are indeed limited to that which is strictly necessary.

30. Third, more clarity is need as to the **extent** of communications to which the "*well-established technologies"* would be applied. In particular, it should be clarified what exactly is to be understood as *"well-established technologies"* and whether those technologies would be applied to all communications exchanged by all users or to a subset of them. In the latter case, it would be necessary to clarify the criteria by which the technologies would be applied to a specific subset of communications.

31. The EDPS questions whether the **extent of the proposed derogation** is strictly necessary to achieve the objectives set out by the Proposal. Specifically, the EDPS questions whether the derogation from the entirety of Article 6 of ePrivacy Directive is justified, given that Article 6 mainly concerns processing activities that have no relationship with the processing envisaged by the Proposal. Moreover, Article 6(1) explicitly provides that it is without prejudice to Article 15(1) of the ePrivacy Directive. Finally, Article 5(1) also makes reference to the *"related traffic data"* which appears to be more directly linked to the underlying objectives of the Proposal.

3.4. Purpose limitation and storage limitation

32. The Proposal stipulates as one of the conditions for the derogation that the processing shall be "*limited to what is strictly necessary for the purpose of detection and reporting of child sexual abuse online and removal of child sexual abuse material and, unless child sexual abuse online has been detected and confirmed as such, is erased immediately*". The EDPS

understands the obligation to erase the data refers to all *"**personal and other data**"* covered by the scope of the derogation. The EDPS urges the co-legislature to be **more explicit** in this respect, clarifying also the specific categories of data that may be retained.

33. The Proposal also provides that where child sexual abuse online has been detected and confirmed as such, the *"relevant data"* may be retained solely for the following purposes and only for the time period necessary: (i) for its reporting and to respond to proportionate requests by law enforcement and other relevant public authorities; (ii) for the blocking of the concerned user's account; and (iii) in relation to data reliably identified as child pornography, for the creation of a unique, non-reconvertible digital signature ('hash'). Here too the EDPS would encourage the co-legislature to spell out, in the text of the Proposal **which categories of data would amount to "*relevant data*"** in relation to each of these purposes and **which recipients in fact constitute "*other relevant public authorities*".**

34. The EDPS questions whether the reporting of individuals and blocking of the concerned user's account will be strictly necessary and proportionate in all instances, given also the absence of further information as to **what amounts to a "*detected and confirmed*" case** of child sexual abuse online. Would the unsolicited receipt of child sexual abuse material justify reporting and/or blocking? Does the confirmation process by definition entail human review?[33] Who makes the confirmation and who determines whether the account holder is in fact culpable of the acts described in Article 2(2) of the Proposal? While the EDPS supports the objective of swiftly disabling the means used to commit child sexual abuse online, the legal framework should be sufficiently clear and precise as regards the **circumstances in which the described measures may be taken**.

35. Finally, while the Proposal envisages that the *"relevant data"* should only be retained as necessary to achieve the enumerated purposes, there is no clarity as to **how long data should be retained** with a view of "*responding to proportionate requests by law enforcement and other relevant public authorities*".[34] The Proposal fails to provide a clear indication of any actual time period in this respect. The Proposal also fails to clearly set out which entities would be allowed to continue to process the relevant data in a manner which would continue to permit identification of the individuals concerned (perceived perpetrators and victims).[35]

3.5. Reporting to relevant authorities

36. When it comes to reporting, the EDPS has already previously indicated that there is a need for a **precise description** in the text of the legislation of **who is enabled to collect and keep which information** and under what specific safeguards.[36] This is particularly important considering the consequences of reporting: in addition to the information related to children, personal data of any individual connected in some way with the information circulating on the network could be at stake, including for instance information on a person suspected of misbehaviour, be it an internet user or a content provider, but also information on a person reporting a suspicious content or the victim of the abuse.[37]

37. In this regard, the EDPS is particularly concerned that the Proposal does not explain the governance model of electronic service providers using this derogation. It is unclear how the electronic service providers will report or to whom. It is also not specified who will be

in charge of maintaining and updating the relevant databases for identifying future instances of child sexual abuse online.

38. In terms of **quality and integrity** requirements, additional safeguards should be implemented in order to guarantee that this information considered as digital evidence has been properly collected and preserved and would therefore be admissible before a court. Guarantees related to the supervision of the system and its use, in principle by law enforcement authorities, are decisive elements to comply with. Transparency and independent redress possibilities available to individuals are other essential elements to be integrated in such a scheme.[38]

3.6. Transparency and data subject rights

39. The Proposal does not contain any provision concerning **transparency and the exercise of data subject rights**. Insofar as the proposal is intended to be *"without prejudice"* to the GDPR, the duties of the provider to inform individuals and to accommodate data subject rights in principle remain unaffected. Nevertheless, the EDPS recommends the co-legislature to introduce additional measures place to ensure transparency and exercise of data subject rights, subject, where strictly necessary, to narrowly defined restrictions (e.g., where necessary to protect the confidentiality of an ongoing investigation). Such restrictions must, in any case, comply with the requirements set out in Article 23(1) and (2) GDPR.

40. As far as users are concerned, an example of possible measures to ensure transparency and complaint mechanisms can be found in the Proposal for a Regulation on preventing the dissemination of terrorist content online.[39] In addition to general transparency obligations (Article 8) and complaint mechanisms (Article 9), it also provides for information to content providers (subject to derogation where competent authorities decide that for reasons of public security including in the context of an investigation, it is considered inappropriate or counter-productive to directly notify the content provider of the removal or disabling of content) (Article 11). While further adaptation is likely to be necessary, these examples be useful to consider as the EU co-legislator seeks to incorporate additional safeguards into the text of the Regulation.

3.7. Keeping up with the state of the art

41. Article 3 (a) of the Proposal limits the scope of the derogation to *"...well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose before the entry into force of this Regulation...*". The EDPS stresses that these *"well established technologies"* are not described in the Proposal. This lack of precise identification of the measures subject to the derogation is likely to undermine legal certainty.

42. Limiting the measures to those regularly used before the future entry into force of the Proposal would prevent future developments towards less intrusive technical and organisational measures. Recital (11) of the Proposal states that the Regulation would not preclude "*the further evolution of the technology in a privacy-friendly manner*", it is not supported by the text of the Proposal itself.

43. The EDPS therefore recommends clarifying in the text of the Proposal that the **reference to technologies regularly used** before the future entry into force of the Proposal **does not prevent deployment of technologies with a similar purpose** which are less privacy-intrusive, in accordance with the requirements of data minimisation and data protection by design and by default.

3.8. DPIA and prior consultation

44. Recital (10) of the Proposal clarifies that the requirement to carry out, prior to the deployment of the technologies concerned, an assessment of the impact of the envisaged processing operations pursuant to Article 35 GDPR ('DPIA') shall apply "*where appropriate*".

45. The EDPS notes in accordance with Article 35(1) GDPR, carrying out a DPIA shall be required when the processing is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing. Taking into account the relevant guidance, the processing envisaged by the Proposal is very likely to satisfy this threshold (as the processing is likely to be large scale in nature, involve processing sensitive data or data of highly personal nature, etc.).[40]

46. The EDPS recommends the introduction, also with a view of providing legal certainty, of an explicit requirement of carrying out a DPIA within the meaning of Article 35 GDPR in relation to any processing that falls within the scope of the proposed derogation. While the carrying out of DPIA may not always be necessary in relation to processing operations which were already being carried out on 25 May 2018[41], controllers are obliged to conduct such a DPIA, at the appropriate time, as part of its general accountability obligations.[42] Adding an explicit requirement in this respect would provide additional clarity as well assurances that the processing will be carried out in compliance with the GDPR.

47. As regards the requirement of prior consultation in accordance with Article 36 GDPR, the EDPS notes the requirement proposed by the Council[43] that the prior consultation procedure set out in Article 36 GDPR shall apply to any technology which has not been used before the entry into force of the Proposal. The EDPS wishes to stress, however, that such an obligation continues to be applicable in any situation where a DPIA reveals high residual risks.[44]

48. Finally, the EDPS would like to emphasize that **guidance provided by data protection authorities cannot substitute compliance with the requirement of legality**. As the Proposal provides for a derogation upon the confidentiality of communications, it is **insufficient** to provide that the temporary derogation is ***"without prejudice"* to the GDPR** and to mandate prior consultation of data protection authorities and/or to call upon the EDPB to issue guidance. The co-legislature must take its responsibility and ensure that the proposed derogation complies with the requirements of Article 15(1), as interpreted by the CJEU.

3.9. Duration of the temporary derogation

49. Article 4 of the Proposal specifies that the Regulation shall apply from 21 December 2020 until 31 December 2025, i.e. for a period of five years. Recital (16) clarifies that the period

of application of this Regulation was chosen as "*a time period reasonably required for the adoption of a new long-term legal framework*". In case the announced long-term legislation were to be adopted and enter into force prior to this date, that legislation should repeal the present Regulation.

50. The EDPS is of the view that a five-year period is too longdoes not seem proportional given the absence of (a) a prior demonstration of the proportionality of the envisaged measure and (b) the inclusion of sufficient safeguards within the text of the legislation. **He recommends that the validity of any transitional measure should not exceed 2 years.**

51. If adopted, the Proposal, will inevitably serve as a precedent for future legislation tackling the dissemination of illegal content online, in particular in relation to confidential communications. **The EDPS therefore considers it essential that the Regulation is not adopted, even in the form a temporary derogation, until the necessary safeguards and all the outstanding missing elements as identified in these specific recommendations are integrated.**

4. CONCLUSIONS

52. The measures envisaged by the Proposal would constitute an interference with the fundamental rights to respect for private life and data protection of all users of very popular electronic communications services, such as instant messaging platforms and applications. Even voluntary measures by private companies constitute an interference with these rights when the measures involve the monitoring and analysis of the content of communications and processing of personal data.

53. The issues at stake are not specific to the fight against child abuse but to any initiative aiming at collaboration of the private sector for law enforcement purposes. If adopted, the Proposal will inevitably serve as a precedent for future legislation in this field. The EDPS therefore considers it essential that the Proposal is not adopted, even in the form a temporary derogation, until all the necessary safeguards set out in this Opinion are integrated.

54. In the interest of legal certainty, the EDPS considers that it is necessary to clarify whether the Proposal itself is intended to provide a legal basis for the processing within the meaning of the GDPR, or not. If not, the EDPS recommends clarifying explicitly in the Proposal which legal basis under the GDPR would be applicable in this particular case. In this regard, the EDPS stresses that guidance by data protection authorities cannot substitute compliance with the requirement of legality. It is insufficient to provide that the temporary derogation is *"without prejudice"* to the GDPR and to mandate prior consultation of data protection authorities. The co-legislature must take its responsibility and ensure that the proposed derogation complies with the requirements of Article 15(1), as interpreted by the CJEU.

55. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and

imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse.

56. The lack of precise identification of the measures subject to the derogation is likely to undermine legal certainty.

57. Finally, the EDPS is of the view that the five-year period as proposed does not appear proportional given the absence of (a) a prior demonstration of the proportionality of the envisaged measure and (b) the inclusion of sufficient safeguards within the text of the legislation. He considers that the validity of any transitional measure should not exceed 2 years.

Brussels, 10 November 2020

Wojciech Wiewiorowski

(e-signed)

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89.
[4] COM(2020) 607 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf
[5] 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. 37–47
[6] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ L 321, 17.12.2018, p. 36
[7] COM(2020) 607 final, p. 4. The Communication notes that because the ePrivacy Directive does not contain a legal basis for *voluntary* processing of content and traffic data for the purpose of detecting child sexual abuse, providers can only apply such measures if based on a national legislative measure, that meets the requirements of Article 15 of the ePrivacy Directive for restricting the right to confidentiality. In the absence of such legislative measures, measures to detect child sexual abuse undertaken by these providers, which process content or traffic data, would lack a legal basis.
[8] COM(2020) 568 final, 2020/0259 (COD), 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 numberindependent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, https://ec.europa.eu/digital-single-market/en/news/interim-regulation-processing-personal-and-other-data-purpose-combatting-child-sexual-abuse
[9] Article 2 (5) EECC defines an *'interpersonal communications service'* as *"a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service"*. A *'number-independent interpersonal communications service'* means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans (Article 2(7) ECC).
[10] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1.
[11] The term 'without right' allows Member States to provide a defence in respect of conduct relating to pornographic material having for example, a medical, scientific or similar purpose. It also allows activities carried out under domestic legal powers, such as the legitimate possession of child pornography by the authorities in order to conduct criminal proceedings or to prevent, detect or investigate crime. Furthermore, it does not exclude legal defences or similar relevant principles that relieve a person of responsibility under specific circumstances, for example where telephone or Internet hotlines carry out activities to report those cases. Recital (25) of Directive 2011/93/EU.
[12] Article 5(3), 5(4) and 5(5) of Directive 2011/93/EU.
[13] Articles 11 and 25(1) of Directive 2011/93/EU.
[14] Article 25(2) of Directive 2011/93/EU.
[15] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, 10 May 2010, https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_en.pdf.
[16] Court of Justice of the European Union, *La Quadrature du Net a.o*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, atparagraph 121.
[17] Recital (15) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), O.J. 17.12.2018, L 321/36.
[18] EDPS, Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 5.

[19] Court of Justice of the European Union, *La Quadrature du Net a.o*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, at paragraph 128 .
[20] Judgment of the Court of Justice of the European Union, *La Quadrature du Net a.o*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, at paragraph 126.
[21] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, 10 May 2010, available at https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_en.pdf, paragraph 7.
[22] Judgment of the Court of Justice of the European Union, *La Quadrature du Net a.o*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, at paragraph 132.
[23] Idem.
[24] Idem.
[25] 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. 1–88
[26] Explanatory Memorandum of the Proposed Interim Regulation, p. 2.
[27] Article 29 Data Protection Working Party, *'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'*, WP 217, 9 April 2014, p. 29.
[28] Judgment of the Court of Justice of the European Union in Fashion ID, 29 July 2019, C-40/17, ECLI:EU:C:2019:629, at paragrap 95.
[29] See also: the European Data Protection Supervisor, *Necessity toolkit on assessing the necessity of measures that limit the fundamental right to the protection of personal data*, 11 April 2017, p.9 The first step pf the checklist for assessing necessity of new legislative measure requires *"**a detailed factual description** of the measure proposed and its purpose, prior to any further assessment."*
[30] European Data Protection Supervisor Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, p. 23 available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf
[31]European Data Protection Supervisor Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, p.20 available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf
[32] While Article 3 the Proposal limits the proposed measures to *"...well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose before the entry into force of this Regulation...*", the Proposal does not further describe what those *"well established technologies"* are, which could create legal certainty to the identification of the allowed measures.
[33] Recital (11) of the Proposal specifies that « *The reference to the technology includes <u>where necessary</u> any human review directly relating to the use of the technology and overseeing it*." This does not clarify in which circumstances human review will be present, only that it is not always present.
[34] Compare for example with Article 7 (Preservation of content and related data) of the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, COM(2018) 640 final.
[35] While the Proposal indicates that in relation to data reliably identified as child pornography, data may only be kept for the creation of a unique, non-reconvertible digital signature ('hash'), it does not explicitly state which entities would be authorised to retain a copy of the orginal data identified as child pornography, nor at which moment in time the provider would be required to delete erase the data reliably identifed as child pornography.
[36] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, 10 May 2010, paragraph 12, available at https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_en.pdf
[37] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 13.
[38] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 15.
[39] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, COM(2018) 640 final.
[40] See Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is *"likely to result in a high risk"* for the purposes of Regulation 2016/679, WP 248 rev.01, 4 October 2017
[41] Processing that received a positive advice from a DPA upon consultation.

[42] Ibid, p. 14.
[43] Council of the European Union 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 Mandate for negotiations with the European Parliament, 23 October 2020, 2020/0259(COD)
[44] Ibid, p. 18-19.