



EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Opinion X/2019

on the Proposal for a Regulation preventing the dissemination of terrorist content online



xx January 2019

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'. Under Article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'. Under Article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. While the EDPS supports the objective of combatting the dissemination of terrorist content online, thus contributing to a more secure Union overall, he considers that the Proposal ~~sh~~ could be improved ~~in certain key aspects~~ to ensure compliance with data protection principles.

Executive Summary

The EU is working to stop terrorists from using the internet to radicalise, recruit and incite to violence. This Opinion outlines the position of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, currently under negotiations between the European Parliament and the Council.

The EDPS understands the need to combat the dissemination of terrorist propaganda online, in particular with regard to the potential of such material to groom and recruit new terrorists and to prepare and facilitate terrorist attacks. He supports the objectives of the Proposal. At the same time, he stresses that initiatives in this area may have an impact on fundamental rights, including the right to freedom of expression and information, the right to an effective (administrative or judicial) remedy, the right to respect of private and family life and the right to the protection of personal data. In this Opinion, the EDPS has carefully assessed the Proposal and issues several recommendations to assist the legislators to ensure that the proposed Regulation will be compliant with privacy and data protection principles, in particular Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

The EDPS understands the need to combat the dissemination of terrorist propaganda online, in particular with regard to the potential of such material to groom and recruit new terrorists and to prepare and facilitate terrorist attacks. However, the EDPS underlines that the Proposal would likely have an impact on fundamental rights, including the right to freedom of expression and information, the right to an effective (administrative or judicial) remedy, the right to respect of private and family life and the right to the protection of personal data.

While the EDPS welcomes that the Proposal stresses the necessity to take into account the fundamental rights to privacy and data protection, he is of the opinion that the Proposal needs in some aspects further clarification, specification and adjustment by the legislators, in particular:

- The Proposal should **always more clearly describe the relevant actions and measures that should be taken by hosting service providers ('HSPs')** to prevent the dissemination of terrorist content. The Proposal should not leave it to the wide discretion of HSPs to ensure that fundamental rights are protected and that a fair balance between various fundamental rights is struck;
- The proposed obligation for HSPs to take appropriate, reasonable and proportionate actions against the dissemination of terrorist content as laid down in Article 3 and Article 6 of the Proposal **should not result in the establishment of a systematic and general monitoring system**. In this regard, the proposed derogation from Article 15(1) of Directive 2000/31/EC, which would enable the imposition of a general monitoring obligation on HSPs, should be reconsidered;
- When using automated tools, HSPs should take full account of the privacy and data protection principles as provided for in the GDPR. In particular, while **HSPs' decisions based on automated tools should always be subject to human oversight and human verification**, HSPs should always give data subjects a **meaningful explanation** of the functioning of the proactive measures including the used automated tools;

Formatted: Highlight

- With regard to the proposed obligation for HSPs to retain terrorist content and 'related data' for the purpose of prevention, detection, investigation or prosecution of terrorist offences as provided for in Article 7 of the Proposal, the legislators should **strengthen the proposed safeguards and introduce additional procedural provisions for the access and subsequent use of preserved data by competent authorities.**

~~The Opinion provides further recommendations in terms of data protection and privacy that should be taken into consideration in the legislative process.~~

~~Finally, as the Proposal shares certain similarities with the Proposal on e-evidence, in particular regarding context and terminology, the EDPS calls upon the legislator to ensure a consistent and coherent approach to these two Proposals.~~

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND.....	6
1 1 CONTEXT OF THE PROPOSAL	6
1 2 CONTENT OF THE PROPOSAL	7
2. COMMENTS AND RECOMMENDATIONS	8
2 1 PRELIMINARY REMARKS	8
2 2 OBLIGATIONS FOR HSPS	10
2 2 1 On the use of automated tools in the context of proactive measures	10
2 2 2 Article 15(1) of Directive 2000/31/EC	11
2 2 3 Preservation of content and related data	11
3. CONCLUSIONS	1312
Notes	14

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 October 2018 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 data², 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 (Law Enforcement Directive)³,

Commented [BA1]: I don't think we were consulted by the Commission at all, and certainly not since 11/12? Delete?

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1.1 Context of the Proposal

1. On 12 September 2018, the European Commission published a Proposal for a Regulation on preventing the dissemination of terrorist content online⁴ (hereinafter 'the Proposal').
2. The aim of the Proposal is to establish uniform rules for hosting service providers (hereinafter 'HSPs'), such as social media platforms, video streaming services, video, image and audio sharing services, but also file sharing and other cloud services that make information available to third parties as well as websites where users can make comments or post reviews, who offer their services within the Union - regardless of their place of establishment - to prevent the dissemination of terrorist content through their services and to ensure, where necessary, its swift removal.
3. The Proposal builds on HSPs' obligation pursuant to Directive 2000/31/EC⁵ to remove illegal content that they store and can be seen as part of a series of regulatory and non-regulatory initiatives to combat illegal content online⁶ and also as part of the anti-terrorism package⁷.
4. In this regard, the EDPS takes notice that Member States are already obliged by Article 21 of Directive (EU) 2017/541 to ensure the prompt removal of online content that constitutes public provocation to commit terrorist offences and that the revised Audiovisual Media Services Directive⁸ will also require Member States to ensure that

video-sharing platforms take appropriate measures to protect the public from public provocations to commit a terrorist offence.

5. Moreover, the EDPS observes that the Proposal shares certain similarities with the Proposal on e-evidence⁹ and therefore calls upon the legislator to ensure a consistent and coherent approach¹⁰ to both proposals. In particular, the EDPS - taking into account his Opinion 09/2018 on Proposals to establish European Production and Preservation Orders to gather e-evidence in criminal matters - recommends to have uniform and clear definitions (Point 3.2), to introduce strong security safeguards for transmissions, including authenticity certificates for removal orders and referrals (Point 3.4.1 and 3.4.2) and to clarify that legal representatives are not representatives in the meaning of GDPR and the Law Enforcement Directive (Point 4.3).
6. The EDPS takes notice that the Council reached a general approach on the Proposal on 6 December 2018. He welcomes in particular the introduced clarification to the definitions of terrorist content (cf. Article 2 (5)) and HSPs (cf. Recital 10) as well as the proposed improvement for better cooperation between the relevant competent authorities and Europol (cf. Article 13 (3) and (4)).

Commented [BA2]: is this still valid? I think we should reconsider, also in the interest of timing

Commented [BA3]: I think we have taken it out of the e-evidence, here too?
I personally do not see any reasons why these reps should not be the same person/entity

Commented [BA4]: of the Council GA? or of the proposal?

1.2 Content of the Proposal

7. The Explanatory Memorandum stresses that terrorists misuse the internet for the purposes of grooming and recruiting supporters, preparing and facilitating terrorist activity, glorifying their atrocities and urging others to follow suit.¹¹ Even though Member States and HSPs have established voluntary partnerships and frameworks to reduce the access to terrorist content, it is argued that these measures are not sufficient to adequately address this issue.¹²
8. The Proposal establishes a minimum set of duties of care for HSPs and sets out various obligations for Member States, notably to enforce the Proposal. In particular, the Proposal introduces the following measures:
 - HSPs would have to take appropriate, reasonable and proportionate actions against the dissemination of terrorist content, in particular to protect users from terrorist content (Article 3);
 - HSPs would have to remove or disable access to terrorist content within one hour upon receipt of a removal order issued by a competent authority of a Member State (Article 4);
 - HSPs would have to assess, on the basis of referrals sent by Member States' competent authorities or by Union bodies (such as Europol) whether the content identified in the referral is in breach of the HSPs' respective terms and conditions and decide whether or not to remove that content or disable access to it (Article 5);
 - HSPs would have to implement proactive measures to protect their services against the dissemination of terrorist content, *inter alia* by using automated tools to assess the stored content (Article 6);

Commented [BA5]: move up to "context"

- HSPs would have to preserve the content that has been removed and related data which are necessary for the purposes of subsequent administrative proceedings, judicial review and the prevention, detection, investigation or prosecution of terrorist offences (Article 7);

- HSPs would have to establish a relevant complaint mechanism, by which persons whose content was removed pursuant to a referral or a proactive measure can submit a complaint to the HSP (Article 10);

- HSPs would have to provide information to persons whose content has been removed pursuant to a removal order, a referral or a proactive measure (Article 11);

- Member States would have to designate one or several authorities competent to issue removal orders, detect or identify terrorist content and issue referrals to HSPs, oversee the implementation of proactive measures and enforce the obligations established by the Proposal through penalties (Article 17).

9. The EDPS ~~acknowledges the objectives of the Proposal and also~~ understands the need to combat the dissemination of terrorist propaganda online and supports the objectives of the Proposal. As the Proposal would likely effect several fundamental rights, including the right to freedom of expression and information and the right to an effective remedy as well as the right to respect of private and family life and the right to the protection of personal data, he has decided to issue this Opinion. Nevertheless, he wishes to suggest a number of areas for possible improvements, in order to strengthen the compliance with the relevant fundamental rights, including privacy and data protection.

2. COMMENTS AND RECOMMENDATIONS

2.1 Preliminary remarks

10. The EDPS observes that the Proposal is based on Article 114 TFEU which provides for the establishment of measures to ensure the functioning of the Internal Market. As the objective of the Proposal appears to be linked to the prevention, detection and investigation of criminal offences, in particular the prevention and combatting of terrorism, the Proposal would probably fall rather within the scope of **Title V of the TFEU**. Therefore, the EDPS suggests to the legislators to evaluate whether Article 114 TFEU could serve as a more appropriate legal basis for the Proposal.

11. The term ‘**terrorist content**’ is defined in Article 2(5) of the Proposal and encompasses inciting, advocating or glorifying the commission of terrorist offences, thereby causing a danger that such acts be committed (a), encouraging the contribution to terrorist offences (b) and promoting the activities of a terrorist group (c). The EDPS welcomes that the definition is consistent and closely aligned with Directive (EU) 2017/541 on Combatting Terrorism. As Article 3 of Directive (EU) 2017/541 refers with regard to ‘terrorist offences’ to ‘intentional acts’, the EDPS suggests to include the term ‘intentional’ also in the Proposal’s definition. This clarification would help to avoid inconsistencies between the two legal texts. However, the EDPS welcomes that Recital 9 of the Proposal clearly sets out that competent authorities and HSPs should take into account the context in which such

Commented [BA6]: Apologies, I did not notice this before. As a rule, we do not comment on the legal basis, unless there is a data protection dimension i.e. would like to suggest Art 16 as an alternative/additional legal basis. This was long discussed in the evidence context as well. Also, the beginning of the paragraph and the last sentence together don't make sense :)

content appears and that content, which was disseminated for educational, journalistic or research purposes should be adequately protected. Recital 9 of the Proposal also clarifies that the expression of radical, polemic or controversial views in a public debate on sensitive political questions should not be considered as terrorist content.

12. Nevertheless, with regard to the definition of ‘hosting service provider’ as provided for in Article 2(1) of the Proposal, the EDPS notes that the definition could be interpreted broader than it seems to have been intended. In particular, the wording “making the information stored available to third parties” could also be interpreted as including the sharing of content within a closed group of a social media platform or a one-to-one communication such as e-mail. In this regard, the EDPS is of the view that Recital 10 of the Proposal would not provide sufficient clarification to exclude such a broad interpretation. Therefore, the EDPS suggests to clarify the definition by replacing the term ‘third parties’ with ‘the public’.

Commented [BA7]: what if the “closed group” has hundreds of thousands of users (e.g. “gilets jaunes” on facebook)? messenger apps might be different, although even here I don’t think there are limits on how many people you can reach within a “closed group”

Commented [BA8]: please reconsider: with this, a twitter account with 10 followers would be “public” while a massive “closed” facebook group would not. This is not something we should be asking for!

13. The EDPS takes positive note that the Proposal stresses in several provisions that it will ensure the protection of the fundamental rights at stake and that HSPs should always take into account the fundamental rights of the users and also the importance of these rights.¹³ In this respect, the EDPS ~~observes and~~ welcomes that Recital 7 of the Proposal explicitly stresses that the Regulation will ensure the rights to respect for private life and to the protection of personal data. ~~However, the EDPS notes that the Proposal contains no~~ In order to strengthen this commitment, he suggest adding an explicit reference to the applicable data protection legislation, i.e. the General Data Protection Regulation (EU) 2016/679 (the GDPR)¹⁴ and the Directive (EU) 2016/680 (the Law Enforcement Directive)¹⁵ in Recital 7. Therefore, and for the sake of clarity and legal certainty, the EDPS suggests to insert in the Proposal a specific provision confirming the applicability of the aforementioned legal acts.

Commented [BA9]: In line with a long standing practice of the Legal Service and a recent comment by Giovanni

14. The EDPS observes that pursuant to Article 4(2) of the Proposal, HSPs should **remove terrorist content within one hour from receipt of the removal order**. In this regard, the Impact Assessment explains that terrorist content is most harmful in the first hours of its appearance because of the speed at which it is disseminated and therefore multiplied. The EDPS shares this sentiment and stresses that terrorist content should be taken down as fast as possible. However, fast removal requires a good cooperation and also a good interaction between HSPs and the competent authorities. Therefore, the EDPS suggests to explore the application of digital signatures for electronically transmitted removal orders and to establish an official and easily accessible list of the competent authorities of the Member States. Thereby, HSPs could quickly verify the authenticity of a removal order and would have quickly available the contact details of the competent authorities in case of doubt.

Commented [BA10]: To me, this is not related to the *timing*, but a general issue of security and authenticity. Could we present it as such?

15. The EDPS takes positive notice that pursuant to Article 10 of the Proposal, HSPs would have to establish effective and accessible mechanism allowing content providers, whose content were removed or access to it was disabled, to appeal against the decision of the HSP. In accordance with Article 10(2) of the Proposal, the responsible HSP shall promptly examine the complaint and inform the content provider about the outcome of the examination. The EDPS welcomes the introduction of a **complaint mechanism** as it constitutes an ~~adequate~~ important safeguard against erroneous removals. However, the EDPS considers that the responsibility for as public authorities are the protection and the necessary balancing of relevant fundamental rights belongs ultimately ~~responsible for the protection of fundamental rights to~~ Member States through their courts or other public

authorities; He would therefore welcome the EDPS considers that if a specific provision could be added, to identify the (independent) public authority responsible for reviewing stating that the final decision of a responsible HSP is subject to review by an independent authority. Procedures should also be envisaged Furthermore, the EDPS suggests to include in Article 10 of the Proposal a provision for cases in which the responsible HSP does not react to the complaint of a content provider.

2.2 Obligations for HSPs

16. The EDPS observes that Article 3 of the Proposal would oblige HSPs to take “*appropriate, reasonable and proportionate actions*” against the dissemination of terrorist content, whereas they should “*act in a diligent, proportionate and non-discriminatory manner*” and take “*due regard to the fundamental rights of their users*”. While Article 3(2) of the Proposal sets out that HSPs should include in their terms and conditions provisions to prevent the dissemination of terrorist content, Article 6 of the Proposal elaborates that HSPs should also implement proactive measures to protect their services against the dissemination of terrorist content. Along the lines of Recital 18 of the Proposal, such **proactive measures** could consist of measures to prevent the re-upload of terrorist content which has previously been removed, checking the content against publicly or privately held tools containing known terrorist content as well as using reliable technical tools to identify new terrorist content.
17. While the implementation of these obligations would be overseen by competent authorities in the Member States, the EDPS observes that the Proposal leaves it widely to the discretion and the responsibility of HSPs to design, establish and implement effective and proportionate measures to prevent the dissemination of terrorist content on their services. As the Proposal would likely affect several fundamental rights, the EDPS considers that the proposed obligations could put HSPs’ in a difficult situation as they would have to weigh all relevant fundamental rights against each other. For this reason, the EPDS suggests that the legislators could explore the possibility to either further describe the relevant actions that HSPs should take - considering also their impact on the different fundamental rights - or provide HSPs with more guidance in the Proposals’ recitals, so they are able to strike a fair balance between the various fundamental rights.

2.2.1 On the use of automated tools in the context of proactive measures

- ~~18.~~The EDPS observes that Recital 16 and 18 of the Proposal specifically provide that proactive measures may include the use of **automated tools**. The EDPS is aware that due to the vast volume of data, the use of automated tools could be necessary to enable HSPs to successfully search for terrorist content. Nevertheless, the EDPS stresses that the use of such automated tools could require a systematic analysis of all content and also the ~~collection and~~ identification of users which have disseminated terrorist content¹⁶, which in turn would imply processing of their personal data. In this respect, the EDPS draws attention to the fact that compliance with the GDPR will be essential at ~~As the implementation of such automated tools would also have consequences for the right of data protection, especially if stage. Moreover, to the extent the use of such tools would lead to the amount to profiling of the uploaders or automated decision making in the meaning of Art xxx GDPR, the EDPS stresses the need to comply with the relevant~~

Commented [BA11]: I would suggest to redraft:
- repeat again that it is the responsibility of Member States to protect/balance fund rights
- safeguards/balancing should ideally be written in the legislation
- alternative, provision should be made for further guidance to be provided (at EU level? national? Commission - DA or IA?)
- try to avoid using language that would position us as industry defenders

provisions, including Article 25 and in particular explanation and human intervention recommends that HSPs should take full account of the privacy and data protection principles as provided for in the GDPR. In particular, HSPs should address the following issues:

~~automated tools should only process those personal data which are necessary and proportionate for the specific purpose;~~

- 18. HSPs should always give their users a **meaningful explanation** of the functioning of the implemented tools;
- the results of automated tools should always be subject to **human verification**, and
 - HSPs should provide competent authorities with **all necessary information on the implemented tools** to verify their functioning and impact.

2.2.2 Article 15(1) of Directive 2000/31/EC

19. The EDPS recalls that Article 15(1) of Directive 2000/31/EC prohibits the imposition of a general monitoring obligation on service providers and hence welcomes that Recital 16 of the Proposal explicitly stresses that the proposed obligation for HSPs to implement proactive measures **should not imply a general monitoring obligation**. However, the EDPS takes notice that Recital 19 of the Proposal elaborates that a competent authority that oversees the implementation of proactive measures “*could derogate from the approach established in Article 15(1) of Directive 2000/31/EC*” (emphasis added) and issue in accordance with Article 6(4) of the Proposal specific additional measures.
20. The EDPS understands that Recital 19 of the Proposal would constitute a derogation from Article 15(1) of Directive 2000/31/EC and would enable competent authorities to impose a general monitoring obligation on HSPs. While, the EDPS is doubtful as to whether a derogation to a directive can effectively be introduced in a recital of another legal act, he is of the opinion that the proposed derogation requires a proper debate, involving all stakeholders concerned, where all advantages and possible disadvantages are carefully weighed against each other. The EDPS is of the view that the imposition of a general monitoring obligation on HSPs, which would indeed affect a large and undefined number of individuals, irrespective of whether they are under suspicion to disseminate terrorist content or not, could probably constitute a disproportionate measure exceeding the limits posed by the principles of necessity and proportionality.¹⁷
21. In light of the above, the EDPS has reservations about the envisaged derogation from Article 15(1) of Directive 2000/31/EC in Recital 19 of the Proposal and recommends the legislators to reassess this measure.

2.2.3 Preservation of content and related data

22. The EDPS observes that pursuant to Article 7 of the Proposal, HSPs would be required to preserve removed content and ‘related data’ for the purpose of subsequent administrative proceedings and judicial review (as a safeguard in cases of erroneous removal) and for the purpose of prevention, detection, investigation or prosecution of terrorist offences (‘double purpose’)¹⁸.

Commented [BA12]: please double check the language and references

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0,25 cm + Indent at: 0,89 cm

Commented [BA13]: please provide GDPR references

Commented [BA14]: was okay with this? not really our core business, so for me this could go

23. While the EDPS takes notice that Article 7 of the Proposal does not clearly define the term ‘related data’, he observes that Recital 20 of the Proposal only broadly explains that such data “can include ‘subscriber data’, including in particular data pertaining to the identity of the content provider as well as ‘access data’, including for instance data about the date and time of use by the content provider, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider”. The EDPS considers that a clear definition of ‘related data’ could help HSPs to avoid uncertainties and also help them to comply with their imposed preservation obligation. For these reasons, he suggests to bring more clarification to the term ‘related data’, which could be done, for instance, by providing an exhaustive list of data categories that HSPs should preserve¹⁹.

24. In particular, the lack of a definition of the data to be preserved and the broad formulation of Recital 20 might bring about a risk of HSPs preserving data that could [paint a detailed picture of the individual’s life ...] This, in turn, would require the various obligations and safeguards required by the Court of Justice under its DRI case law to be set out in the Proposal itself. For example... With regard to the proposed safeguards, the EDPS observes that Article 7(3) of the Proposal provides that HSPs should “ensure that the terrorist content and related data [...] are subject to appropriate technical and organisational safeguards” and that these “technical and organisational safeguards shall ensure that the preserved terrorist content and related data is only accessed and processed for the [relevant] purposes [...] and ensure a high level of security of the personal data concerned.” The EDPS wants to remind the legislators that Article 7 of the later repealed Directive 2006/24²⁰ similarly provided that “the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure”; and that “the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only”. However, the CJEU concluded in *Digital Rights Ireland Ltd*, that the provided safeguards are not sufficient to ensure effective protection of the retained data against the risk of abuse, unlawful access and subsequent use of that data.²¹

25. Moreover, the EDPS observes that the Proposal does not provide substantive and procedural conditions relating to the access and the subsequent use of the preserved data by ‘competent authorities’, as it was required by the CJEU in the aforementioned judgment. The mere reference in Recital 23 of the Proposal, according to which the Regulation “does not affect the procedural guarantees and procedural investigation measures related to the access to content and related data preserved for the purposes of the investigation and prosecution of terrorist offences, as regulated under the national law of the member States, and under Union legislation” could be interpreted in this regard as being insufficient.

26. Against this background, the EDPS recommends to reassess the proposed safeguards as well as the lack of procedural provisions concerning the access and subsequent use of preserved data by competent authorities and to align the Proposal with the aforementioned case-law of the CJEU.

Commented [BA15]: quote from DRI recently also cited in Ministerio Fiscal. If we are in this category (and in this category only), then full extent of DRI requirements apply

Commented [BA16]: As commented above, I believe that DRI would only apply fully *if* the situation here could be compared to data retention directive
- are we saying that the proposal is comparable to DRD (I hope not)
- if not, we should ask for the categories of data to be defined/limited (to *avoid* full applicability of DRI)

3. CONCLUSIONS

Commented [BA17]: to be revisited once text stable

27. After carefully analysing the Proposal, the EDPS makes the following main recommendations to ensure compliance with data protection principles:

- The Proposal should **always clearly describe the relevant actions and measures that should be taken by HSPs** to prevent the dissemination of terrorist content. In addition, the Proposal should not leave it to the wide discretion of HSPs to ensure that fundamental rights are protected and that a fair balance between various fundamental rights is struck;
- The proposed obligation for HSPs to take appropriate, reasonable and proportionate actions against the dissemination of terrorist content as laid down in Article 3 and Article 6 of the Proposal should **not result in the establishment of a systematic and general monitoring system**. In this regard, the proposed derogation from Article 15(1) of Directive 2000/31/EC, which would enable the imposition of a general monitoring obligation on HSPs, should be reconsidered;
- When using **automated tools**, HSPs should take full account of the privacy and data protection principles as provided for in the GDPR. In particular, while HSPs' decisions based on automated tools should always be subject to **human oversight and human verification**, HSPs should **always give data subjects a meaningful explanation of the functioning of the proactive measures including the used automated tools**;
- With regard to the proposed obligation for HSPs to retain terrorist content and 'related data' for the purpose of prevention, detection, investigation or prosecution of terrorist offences as provided for in Article 7 of the Proposal, the legislators should **strengthen the proposed safeguards and introduce additional procedural provisions for the access and subsequent use of preserved data** by competent authorities.

28. The EDPS remains available to provide further advice on the Proposal.

Brussels, xx January 2019

Giovanni BUTTARELLI

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 (2018) 640 final, Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.

⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

⁶ These initiatives include inter alia Directive 2011/92/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. 1–14; Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21; COM (2016) 593 final, Proposal for Directive of the European Parliament and of the Council on copyright in the Digital Single Market and most recent COM (2018) 1177 final, Commission Recommendation of 1.3 2018 on measures to effectively tackle illegal content online .

⁷ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21.

⁸ COM(2016) 287 final Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities.

⁹ COM(2018) 225 final, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

¹⁰ The EDPS observes in particular that Recital 32 of the Proposal already refers to the e-evidence Proposal.

¹¹ In the Impact Assessment it is stated that the terrorist group Daesh produced in the years 2015-2017 an average of 1200 new propaganda items every month (cf. Impact Assessment, p. 7).

¹² Explanatory Memorandum, p. 1.

¹³ For instance Recital 7 and 17 or Article 3 and 6 of the Proposal.

¹⁴ 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.

¹⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

¹⁶ Cf. Article 7, 10 and 11 of the Proposal.

¹⁷ See Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, para. 104-107.

On general monitoring in the context of IPR infringements (general monitoring mandates for platforms conflicting not only with Article 15 of the eCommerce Directive, but also with fundamental rights of internet users, including the right to the protection of personal data), see Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs (SABAM)*, para. 53.

¹⁸ See Recital 21 of the Proposal.

¹⁹ As long as HSPs obligations are unclear, there is a risk that HSPs would be 'incentivized' by the threat of penalties laid down in the Regulation (cf. Article 18(1)(e) referring to Article 7) to collect an excessive amount of data, which will be obviously detrimental to the protection of personal data (as well as to other fundamental rights such as freedom of expression).

²⁰ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54-63, repealed by Judgment of the Court (Grand Chamber), 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

²¹ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, para. 54-55 and 65-67.