Formal comments 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

1. Introduction and background

- These formal comments on the proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (hereinafter, 'the Proposal')[1], adopted by the European Commission on 12 September 2018, are issued by the EDPS in accordance with Article 57(1)(g) and 58(3)(c) of Regulation (EU) 2018/1725[2].

- The aim of the Proposal is to establish harmonized rules for hosting service providers (hereinafter, 'HSPs') 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 its swift removal.

- The Proposal establishes a set of duties of care for HSPs and sets out various obligations for competent authorities of the Member States relating to the enforcement of 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);
  - 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);

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

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, L295, 21.11.2018.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

- 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).

- The EDPS understands the need to combat the dissemination of terrorist content online also defining duties of care for HSPs in this regard and supports the objectives of the Proposal. He recommends **possible improvements**, in order to significantly **reduce any possible 'conflict' with the fundamental rights to privacy and to the protection of personal data**, and to ultimately ensure legal compliance with the latters, as applied in particular by the Court of Justice of the European Union (hereinafter, 'the CJEU').

- The EDPS **takes note** that the Council reached a general approach on the Proposal on 6 December 2018[3], and of the adoption of the draft Opinion by the IMCO Committee on 13 December 2018, of the draft Opinion by the CULT Committee on 16 January 2019, and of the draft Report issued by the LIBE Committee on 21 January 2019[4].

- These formal comments **focus on the possible impact of the Proposal on the rights to privacy and to the protection of personal data**, having regard to Article 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter') and Article 16 of the Treaty on the Functioning of the European Union (hereinafter, 'the TFEU'). However, **especially in relation to this Proposal, we note that the right to the protection of personal data is inextricably linked to other fundamental rights, such as the right to freedom of expression and information**[5], as well as to general principles of EU law, such as the principle of non-discrimination. The fact that this interface is taken into account is in line, among others, with Regulation (EU) 2016/679 (hereinafter, 'the GDPR')[6], that refers explicitly to "the

[3] Procedure 2018/0331(COD), Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - general approach.
[4] The Opinion and Reports of the Committees of the European Parliament on the Proposal (documents related to procedure 2018/0331(COD)) are available at: http://www.europarl.europa.eu/committees/en/draft-opinions.html?urefProcYear=2018&urefProcNum=0331&urefProcCode=COD&source=&linkedDocument=true&ufolderComCode=&ufolderLegId=&ufolderId=#documents
[5] See Christopher Docksey, *Four fundamental rights: finding the balance*, International Data Privacy Law, 2016, Vol. 6, No. 3, page 203: "[I]n some context, such as mass surveillance and independent regulation, the rights of privacy and data protection and freedom of expression function in a wholly complementary fashion, each reinforcing the other." See, among others, on the impact of the measure on **fundamental rights linked to the right to privacy and to the protection of personal data,** case *Tele2* (CJEU, C-203/15 and C-698/15, ECLI:EU:C:2016:970): "the retention of traffic and location data could (...) have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, para. 28)".
[6] 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.

risks of varying likelihood and severity for the rights and freedoms of natural persons"[7].

2. General comments

2.1. The applicable data protection law

- 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[8]. In this respect, the EDPS 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". For the sake of clarity, the EDPS recommends adding in the aforesaid recital the **explicit reference to the applicable data protection law**, namely the GDPR and the Directive (EU) 2016/680 (hereinafter, 'the Law Enforcement Directive')[9]. A possible wording in this regard is: "*This Proposal does not affect the applicable rules on the processing of personal data, notably Regulation (EU) 2016/679 and Directive (EU) 2016/680*."

2.2. The need for a clear definition of the obligations imposed on HSPs in the Proposal

- Since the actions to be taken under the Proposal (the identification and removal of terrorist content) pertain to a 'public interest mission', **all actions to be taken by HSPs pursuant to the Proposal must be clearly described** by the legislator, and **adequate oversight must be ensured by clearly identified competent public authorities.** This would help address the concerns about so-called 'privatised' (delegated to private companies, in this case the HSPs) law enforcement powers, and would be in accordance with both overarching principles of "quality of law"[10] and

[7] Article 24(1) of the GDPR.
[8] See in particular Recital 7 and 17, and Article 3 and 6 of the Proposal.
[9] 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.
[10] In the *Digital Rights Ireland* judgment (Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238), the CJEU has ruled that the **discretionary power of the legislator** is reduced when restricting fundamental rights: "where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference" (para. 47). Replying in substance to the question 'What is the extent of the (reduced) discretion of the EU legislator?', the CJEU stated: "[T]he EU legislation in question **must lay down clear and precise rules governing the scope and application of the measure in question** and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data." (para. 54).
On the notion of 'provided for by law', see also the Opinion of the Advocate General of the CJEU, 8 September 2015, Opinion 1/15 on the draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Records, para. 193: "According to tha case law of the ECtHR, that expression ["quality of the law"] requires, in essence, that the measure in question be **accessible** and **sufficiently foreseeable**, or, in other words, that its terms be sufficiently clear to give an adequate indication as to the circumstances in which the conditions on which it allows the authorities to resort to measures affecting their rights under the ECHR." (emphasis added).
More recently, on this point, see judgement of the ECtHR, *Catt v. United Kingdom*, 24 January 2019.

"economic certainty" for economic operators (clarifying the legal responsibilities of HSPs).

- The Proposal, as further laid out in these formal comments, presents some deficiencies in this regard. For instance, the proposal does not contain a definition of the "**related data**" to be preserved by HSPs pursuant to Article 7, and Recital 20, by way of examples, elaborates 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" is necessary in order to avoid uncertainties for HSPs while also ensure legal certainty for all parties. He therefore recommends to clearly define the term "related data", providing an **exhaustive list** of data categories that should be preserved by the HSPs[11].

- The EDPS also recommends, with the aim of providing a higher level of legal certainty to the HSPs, to **detail and clarify** in the Proposal **the information, necessary and proportionate to ensure the quick removal of the terrorist content by the HSP, to be included** by the 'competent authority' (to be specified as recommended under Section 3.2.2. of these formal comments) **in the removal order** (easily readable, 'standardised' information so as to locate the content, such as the URL, and other information functional to the prompt identification and removal of the terrorist content).

3. Specific remarks

3.1. Definitions of "terrorist content" and of "dissemination of terrorist content" and "hosting service provider"

- The term "**terrorist content**", defined in Article 2(1), point 5, encompasses one or more of the following: (a) "inciting or advocating, including by glorying, the commission of terrorist offences, thereby causing a danger that such acts be committed"; (b) "encouraging the contribution to terrorist offences"; (c) "promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive 2017/541[12]". The Proposal specifies, under Article 2(4), that 'terrorist offences' means offences as defined in Article 3(1) of Directive 2017/541.The aforesaid Directive, under Article 21, lays down that "Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, as referred to in Article 5.[13]"

[11] As HSPs obligations are unclear, there is a risk they would be 'incentivized' by the threat of penalties laid down in the Regulation -see Article 18(1)(e), referring to Article 7- to collect an **excessive amount of data**, which would be detrimental to the protection of personal data (as well as to other fundamental rights such as freedom of expression).

[12] 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.

[13] Article 5 of Directive 2017/541, Public provocation to commit a terrorist offence.

To avoid inconsistencies between the Proposal and the aforesaid Directive, the EDPS recommends that the definition of 'terrorist content' -to be identified and removed by the HSPs- is **consistent and closely aligned** in the two legal texts.

- The EDPS welcomes that Recital 9 sets out in particular that competent authorities and HSPs should take into account the context in which such content appears and that content which was disseminated for educational, journalistic or research purposes should be adequately protected. The aforesaid recital 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. These specifications, provided in the Proposal primarily as safeguards to the right of freedom of expression, are **also relevant from a privacy and data protection viewpoint**, since they 'carve out' categories of content (and the 'related data') that would not be made object of identification, removal and, ultimately, preservation/data retention by the HSPs.

- The term "**dissemination of terrorist content**" under Article 2(1), point 6, should also be aligned with Article 5 of Directive 2017/541. The latter refers, contrary to the current wording of the Proposal (using the unclear wording "to third parties"), to the making available of terrorist content "*to the public*". This last wording would better fit the purpose of the Proposal, which aims at preventing the online dissemination of terrorist content. The same consideration should be reflected under Article 2(1), point 1, in the definition of "**hosting service provider**" (replacing the wording 'third parties' with 'the public'). As a consequence of this specification, for instance, **cloud services** that do not make users' content accessible for dissemination -but are accessible to third parties- consistently with the objectives of the Proposal, would be out of its scope.

3.2. Removal orders

3.2.1. Take down decisions to be performed within one hour from receipt of the order

- Article 4(2) provides that HSPs should **remove terrorist content within one hour from receipt of the removal order** by the competent authority. In this regard, we note that the Impact Assessment shows that terrorist content is most harmful in the first hours from its 'publication' because of the speed at which it is disseminated online. The EDPS takes into account this consideration relating to the effectiveness of the measure (significantly less effective after one hour). However, we point out that it also has to be noted that performing such a fast removal -especially in case of small and medium-sized HSPs- could be challenging[14] and deprive HSPs of the possibility to perform a meaningful check on the removal order.

3.2.2. Authenticity of the removal orders

- Also in order to allow HSPs to perform the fast removal referred to in Section 3.2.1. of these formal comments, **smooth cooperation and speedy interaction between HSPs and the competent authorities** is an essential prerequisite. Therefore, the EDPS

[14] In this regard, the Impact Assessment accompanying the Proposal, SWD(2018)408 final, 12.9.2018, at page 8, explains that terrorist content is most harmful in the first hour. However, it does not provide evidence that such a short time period is indeed feasible. On the contrary, at page 86 it reports that HSPs highlighted that such a short time limit appears unworkable for smaller companies.

suggests to explore, in the context of the 'operational' implementation of the Proposal, the application of **digital signatures for electronically transmitted removal orders** and to establish an **official and easily accessible list of competent authorities in charge of issuing the removal orders for each Member State**. These would allow HSPs to quickly **verify the authenticity** of a removal order and contacting the competent authorities in case of doubts on the order (issuing authority, content, modalities for its execution, *etc*.). These specifications could be added under Recital 14.

3.3. Proactive measures

3.3.1. Measures to be taken by HSPs to prevent the dissemination of terrorist content online according to a targeted, "risk-based approach" and ensuring accountability

- Article 3 (Duties of care) provides that HSPs "shall take appropriate, reasonable and proportionate actions" against the dissemination of terrorist content, "act[ing] in a diligent, proportionate and non-discriminatory manner, and with due regard to the fundamental rights of the users". Article 6, as one of the set of actions to be taken by HSPs (together with measures addressing removal orders and referrals) to comply with the "duties of care" set out in the 'chapeau' provision under Article 3, lays down that HSPs: "shall, where appropriate, take **proactive measures** to protect their services against the dissemination of terrorist content."[15] The EDPS highlights that Article 6(1) also refers to the "risk and level of exposure of the HSP to terrorist content" (risk-based approach') and recommends streamlining this approach throughout the Proposal.

- In this regard, the EDPS point out, as overarching principle to be complied with, that any measure restricting the fundamental rights and freedoms should be necessary and proportionate[16], which implies that they should be **as targeted as possible**.

- In accordance with this principle, the EDPS recommends introducing in the Proposal an obligation for HSPs, *before* they put in place any proactive measure, to:

  (i) Perform and make public a **risk assessment on the level of exposure** to terrorism content (also based on the number of removal orders and referrals received);
  (ii) Draw up a **remedial action plan** to tackle terrorist content proportionate to the level of risk identified[17]. The aforesaid assessment and action plan would also serve the purpose of representing useful **accountability** tools for a periodic review of the measures.

[15] Recital 18 further specifies that 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.
[16] Article 52(1) of the Charter states that: "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".
[17] The Impact Assessment refers to the "risk assessment" and "remedial action plan" in the context of the implementation of measures under Article 6 pursuant to a risk-based approach. However, such requirements have not been finally introduced in the Proposal.

As further accountability tool, HSPs should perform a **periodic reporting** on the actions taken and on the residual level of threat (exposure to terrorist content).

3.3.2. Use of automated tools in the context of proactive measures and safeguards regarding the use of such measures

- Recitals 16 and 18 and Article 6(2) specifically provide that proactive measures may include **the use of automated tools**. The EDPS stresses that such automated tools should only be used in a **cautious and targeted** way, on the basis of the outcome of the risk assessment referred to in section 3.3.1. of these formal comments.

- The EDPS stresses that the procedures envisaged by the Proposal in some, if not most, of the cases, lead to the **identification of the user** who has uploaded the terrorist content (it is the case of the preservation of data related to removed content to be stored by HSPs under Article 7 and possibly accessed by law enforcement authorities; of a complaint mechanism lodged by the user under Article 10; of the provision of information about the removal by the HSP to the user).

- In this respect, the EDPS also draws attention to the fact that it cannot be excluded that the **proactive measures by HSPs, including automated tools, for recognition and removal of content uploaded by users** can also be considered as "automated decision-making, including profiling[18]" in the meaning of Article 22 of the GDPR.

- The EDPS recalls that Article 22(1) of the GDPR provides a **general prohibition of solely automated individual decision-making**, which produces legal effects or similarly significant effects on data subjects[19]. However, Article 22(2) of the GDPR foresees exceptions to this general prohibition and sets out specific cases and requirements under which such decision-making is permissible. In particular, Article 22(2)(b) of the GDPR provides that Union or Member States law can authorise such decision-making when it also lays down "**suitable measures**" to safeguard the data subject's rights and freedoms as well as legitimate interests. In this respect, Recital 71 of the GDPR stresses that such "suitable safeguards" should include in any case specific information to the data subject, the right to obtain human intervention, in order to express his or her point of view and to obtain an explanation of the decision reached after such assessment and to challenge the relevant decision.

---

[18] The GDPR, under Article 4(4), defines profiling: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."
Recital 30 of the GDPR specifies that: "Natural persons may be associated with **online identifiers** provided by their devices, applications, tools and protocols, such as **internet protocol addresses**, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." (emphasis added)

[19] Since the automated tools, as envisaged by the Proposal, could lead not only to the removal and retention of content (and related data) concerning the uploader, but also, ultimately, to criminal investigations on him or her, these tools would **significantly affect** this person, impacting on his or her right to freedom of expression and posing significant risks for him or her rights and freedoms.
The provisions of Article 22 of the GDPR have made object of the WP29 (now EDPB) Guidelines on Automated Individual Decision Making and Profiling, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 , specifying, at page 21, that: "Even if a decision-making process does not have an effect on people's legal rights it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly significant in its impact."

- Article 8(1), under the "transparency obligations", provides that HSPs should set out in their terms and conditions their policy on the prevention of terrorism content, "including, **where appropriate**, a **meaningful explanation** of the functioning of proactive measures including the use of automated tools" (emphasis added).

- Moreover, Article 9(1) provides that HSPs using automated tools shall introduce effective and appropriate safeguards to ensure that decisions taken in particular to remove or disable content are accurate and well-founded. Article 9(2) specifies that such safeguards shall consist of "**human oversight and verifications where appropriate** and, in any event, where a detailed assessment of the relevant context is required [...]" (emphasis added).

- Having regard to these safeguards, the EDPS recommends replacing in Article 8(1) and 9(2) the wording "where appropriate" with "**in any case**", or, alternatively, deleting the wording "where appropriate"[20].

- The EDPS also notes that, pursuant to Article 6(2), HSPs should submit a **report on the proactive measures taken, including the ones based on automated tools, to the authority competent** to oversee the implementation of proactive measures under Article 17(1)(c).

  The EDPS recommends specifying in the Proposal, under Recital 18, that HSPs should provide the competent authorities with all necessary information about the automated tools used to allow a thorough public oversight on the **effectiveness** of the tools and to ensure that the latters **do not produce discriminatory, untargeted, unspecific or unjustified results**[21].

[20] From a 'technical' viewpoint, on the **capabilities and limitations of automated content recognition**, which, however, should be considered taking into account the specificities of the illegal content at stake and the evolution of technologies (so-called 'state of the art'), see *Mixed messages? The limits of automated media content analysis*, November 2017, CDT, at page 21: "any use of automated content analysis tools should be accompanied by human review of the output/conclusions of the tool."
available at: https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf
Another key point highlighted by this paper is the need to provide **clear, consistent, precise definition of the type of content** to be identified.

[21] See the *Declaration on Ethics and Data Protection in Artificial Intelligence*, adopted at the 40th International Conference of Data Protection & Privacy Commissioners, 23 October 2018, available at:
https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.p
See, in particular, point 3, letter (c): "Artificial intelligence systems transparency and intelligibility should be improved, with the objective of effective implementation, in particular by: **making organizations' practices more transparent, notably by promoting algorithmic transparency and the auditability of systems, while ensuring meaningfulness of the information provided**."
In other words, we consider that **the accountability of the HSP** shall be strengthened. This calls for a high level of **transparency** on how the possible 'take down' of uploaded content' takes place (clear guidance on the circumstances under which content is blocked, removed or restricted). In any case, it seems common understanding that decisions on take down should be **subject to human verification**, and that HSPs should provide **meaningful explanations and reporting** on the functioning and effectiveness of the envisaged measures. This would also allow to **check and ensure** that any measure put in place by the HSP: a) strictly complies with the purpose limitation principle (it is not used for other 'aims'); b) does not produce discriminatory, unspecific or unjustified results (also taking into account of the 'distribution' of false positives, not just of their quantity).

4. Mandatory preservation of content and related data by the HSPs

- Pursuant to Article 7, HSPs would be required to **preserve terrorist content** (removed or disabled as a result of any of the three possible sets of actions under the Proposal, i.e., executing removal orders, referrals or proactively) and **related data**[22] for the purpose of subsequent administrative proceedings and judicial review (as a safeguard in cases of erroneous removal), as well as for the purpose of prevention, detection, investigation or prosecution of terrorist offences[23].

- The EDPS notes that the imposition of such a data retention obligation on HSPs entails that private entities are required to retain data (including personal data relating to the uploaders and concerning offences, 'terrorist offences', having a criminal law nature) for law enforcement purposes for the period of six months.[24] In this respect, the EDPS recalls that pursuant to Article 10 of the GDPR the processing of personal data relating to criminal offences should be carried out only under the control of official authority *or* when the processing is authorised by Union or Member State law providing for **appropriate safeguards** for the rights and freedoms of data subjects.

- Since the processing in question (preservation of terrorist content and related data) would *not* be under the control of official authority, the appropriate level of safeguards to be ensured is a key issue. The EDPS observes that Article 7(3) provides that HSPs should "ensure that the terrorist content and related data [...] are subject to appropriate technical and organisational safeguards" and 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 EPDS recalls that Article 7 of the repealed Directive 2006/24 (hereinafter, 'the Data Retention Directive')[25] provided, with a wording similar to the one of the Proposal, 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 "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*, that the Data Retention Directive did *not* provide sufficient safeguards to ensure effective protection of the retained data against the risk of abuse, unlawful access and subsequent use of the data[26].

---

[22] On the need to define 'related data', see considerations made under Section 2.2. of these formal comments.
[23] See Recital 21.
[24] In particular Recital 22 provides: "To ensure proportionality, the period of preservation should be limited to six months to allow the content providers sufficient time to initiate the review process **and to enable law enforcement access to relevant data for the investigation and prosecution of terrorist offences**. However, **this period may be prolonged for the period that is necessary in case the review proceedings are initiated but not finalised within the six months period upon request by the authority carrying out the review. This duration should be sufficient to allow law enforcement authorities to preserve the necessary evidence** in relation to investigations, while ensuring the balance with the fundamental rights concerned" (emphasis added).
[25] 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.
[26] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, see in particular at paras. 54-55 and 65-67. We point out specifically to para. 55: "The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to **automatic processing** and where there is a significant risk of unlawful access to those data", as well as to para 67: "Article 7 of Directive 2006/24 (...) does not ensure that a

- The EDPS observes that it can be argued that the Proposal, similarly to the Data Retention Directive, does *not* lay down substantive and procedural conditions relating to **the access and the subsequent use of the preserved data** by "competent authorities", as required by the CJEU in *Digital Rights Ireland*[27]. The mere mention, in Recital 23, that the Proposal "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"[28] can be considered **inadequate to provide the required substantive and procedural conditions for the access and use of data** to be mandatorily retained by the HSPs pursuant to the data retention obligation established by the Proposal.

- Furthermore, the EDPS is not persuaded about the **necessity and proportionality** of the data retention obligation on HSPs for the purpose of prevention, detection, investigation or prosecution of terrorist offences, since Article 13(4) already obliges HSPs to promptly inform the competent law enforcement authorities of any evidence of terrorist offences they become aware of. In addition, Article 13(4) of the Proposal provides that HSPs could also, in case of doubt, transmit such information to Europol for appropriate follow up.

- In light of the above, the EDPS recommends to **reconsider the proposed data retention obligation** on HSPs for terrorist content and related data as laid down in Article 7(1)(b).

5. The complaint mechanism

- Article 10 provides that HSPs shall establish effective and accessible mechanism allowing content providers, whose content were removed or access to it was disabled, to submit a complaint against the measure taken by the HSP. In accordance with Article 10(2), the HSP shall promptly examine the complaint and inform the content provider about the outcome of the examination.

---

particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period." (emphasis added).

[27] See *Digital Rights Ireland*, para. 61-62, "(...) Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it **merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled** in order to gain access to the retained data in accordance with necessity and proportionality requirements. (62) In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits." (emphasis added).

[28] See similar wording under Article 4, *Access to data*, of Directive 2006/24.

- The EDPS welcomes the introduction of a **complaint mechanism** as this may contribute to strengthen the safeguards for the uploaders against erroneous removals. However, the EDPS recommends inserting in Article 10 a **deadline for the HSP's decision** on the complaint, as well as the indication that the complaint mechanism to be established by the HSP is **without prejudice to the applicable laws and procedures** of the Member States (including without prejudice to the remedies available under the applicable data protection law).

Brussels, 12 February 2019

(signed)

Giovanni BUTTARELLI