From: [redacted]
To: BUCHTA Anna; [redacted]
Subject: RE: Final_Draft_Formal_comments_Terrorist_Content_Online
Date: 04 October 2018 09:43:01
Attachments: Formal_comments_Terrorist__Content_Online.3.10.doc

---

Indeed, let me congratulate with [redacted] for his excellent work.
Of course, I fully subscribe to it.
Just as possible 'food for thought', 2 issues I also had in mind:
1. On the repository:
concerns on the necessity and proportionality of the 'repository' of content and related data established under Article 7 of the Proposal. The Impact Assessment does not seem to provide a sound justification, nor sufficient supporting elements.
Pursuant to recital 31 of the Proposal, the HSPs have the obligation to inform the competent law enforcement authorities of the existence of any evidence of terrorist offences that they become aware of. Hence, on the one hand, the added value of the repository for the countering of terrorist offences is unclear or however lessened by the obligation to inform law enforcement authorities. On the other hand, the Impact Assessment acknowledges the risks posed by the preservation of content and related data[1] (content and data not limited to the aforesaid terrorist evidence) for the 'double purpose' of allowing a check on removed content to identify 'false positives' but also for the purpose of criminal investigation[2].
Hence, the introduction of the obligation to preserve content and "related data" for the purpose of criminal law investigation on terrorism offences is most probably disproportionate having regard to the risks posed to fundamental rights and freedoms. The EDPS therefore recommends duly reconsidering the necessity and proportionality of this far-reaching measure. On the basis of such re-assessment, it may be considered more appropriate to restrict the purpose and use of the repository to the function of allowing checks on false positives only, thus abandoning the current 'dual purpose regime'.
+ the repository comes dangerously close to the processing of data under Article 10 GDPR, requiring strict control of a competent official authority.
2. On Opening black box:
taking into account the serious impact of the data processing operations foreseen by the Proposal, we could strongly recommend adding - to the transparency obligation *vis-à-vis* the users of the HSPs - a specific **transparency obligation *towards the competent authorities*** referred to under Article 17 of the Proposal ***and the competent Data Protection Authorities*** under the GDPR and the Police Directive. Such transparency obligation for HSPs would consist in **quality assurance checks** (auditing) of the automated systems in use to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results, providing the auditor with all necessary information about how the automated system works[3].
I attach a word with 'more narrative' and a conclusion part just in case it would suit the Opinion format.
Feel free of course to look at it or not. I am fine with the draft by [redacted] anyway.
Kindly yours,
[redacted]

From: [redacted]
Sent: 03 October 2018 18:11
To: BUCHTA Anna

Cc: [redacted]

Subject: Final_Draft_Formal_comments_Terrorist_Content_Online

Dear Anna,

Please find attached a first draft on the Proposal regarding Terrorist Content Online.

Since the Proposal is not big and is also (rather) well drafted, an Opinion would be quite brief, so I was not sure whether we want to go there. If you consider that we should go for an Opinion, the necessary changes can be done fast.

https://saas.fabasoft.com/edps/mx/COO.6515.100.2.339223

Best,

[redacted]

---

[1] See at page 105-106 of the Impact Assessment: "the requirement under option 3 for HSP to preserve content removed through proactive measures would have an impact on the right to data protection and privacy, as it is likely that preservation of the aforesaid content will also involve retention of the data related to the content provider (and possibly other third parties)."

[2] The Impact Assessment specifies the double function of this repository, namely "as a safeguard in cases of erroneous removal and to facilitate criminal investigations", at page 7; and "to ensure the existence of evidence for any potential criminal investigations", at page 29.

Recital 20 of the Proposal refers to the obligation to preserve content "for investigative and prosecutorial purposes"; "the required preservation of data is limited to data that is likely to have a link with terrorist offences".

[3] See, in this regard, the WP29 (now EDPB) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, at page 32, "Appropriate safeguards".

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 (v3.10)

1. Introduction

On 12 September 2018, the European Commission adopted a Proposal for a Regulation on preventing the dissemination of terrorist content online (hereinafter "the Proposal").

The Proposal seeks to establish a harmonised legal framework to prevent the misuse of hosting service providers (hereinafter "HSPs") for the dissemination of terrorist content[1]. In the Explanatory Memorandum it is stressed that terrorists exploit the internet to groom and recruit supporters, to prepare and facilitate terrorist activity, to glorify their atrocities and urge others to follow suit[2]. Even though HSPs have put in place measures to tackle terrorist content, it is argued that the scale and progress of HSPs actions is not sufficient to tackle the dissemination of terrorist content online[3]. Hence, further and enhanced measures would be needed to address this issue. Against this background, the Proposal introduces in particular the following measures:

- HSPs are obliged 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, Removal orders];

- HSPs shall assess **referrals** sent by Member States' competent authorities and by Union bodies (such as Europol) evaluating whether the content identified in the referral is in breach of the HSPs' respective terms and conditions and decide accordingly whether or not to remove that content or disable access to it [Article 5, Referrals];

- HSPs will be required to implement **proactive measures** against the dissemination of terrorist content, *inter alia* by using automated tools to assess the stored content [Article 6, Proactive measures];

- Member States will be required to designate one or several authorities competent to issue removal orders, detect or identify terrorist content and issue referrals to HSPs,

[1] The Proposal define the scope of "terrorist content" in Article 2(5) as follows:
"'terrorist content' means one or more of the following information:
(a) inciting or advocating, including by glorifying, 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 (EU) 2017/541;
(d) instructing on methods or techniques for the purpose of committing terrorist offences."

[2] The Explanatory Memorandum to the Proposal, at page 1, highlights that: "the ability to reach such a large audience at minimal cost also attracts criminals who want to misuse the internet for illegal purposes."

[3] See at page 25 of the Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 12.9.2018 (hence "the Impact Assessment").

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

oversee the implementation of proactive measures, enforce the obligations established by the Proposal through penalties.

The Proposal, as also acknowledged by the Impact Assessment, impacts on the fundamental right to privacy and to the protection of personal data, together with other fundamental rights and freedoms of the person concerned (notably, the freedom of expression and information). The EDPS has therefore decided to issue formal comments on this matter.

The EDPS regrets that he was neither consulted by the Commission during the inter-service consultation stage, nor immediately after the adoption of the Proposal. In this respect, the EDPS recalls that - in accordance with Article 28(2) of Regulation (EC) 45/2001[4] - the Commission should consult the EDPS when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

The comments below are limited to the provisions of the Proposal that are particularly relevant from a data protection perspective. Other aspects, such as due process safeguards for the content providers, or the issue of necessity of judicial authorization for issuing the removal orders under Section II of the Proposal, have **not** formed the object of these comments. In this regard, since these issues could impact on the fairness and lawfulness of the data processing activities at stake (the measures to prevent the dissemination of terrorist content online), the EDPS recalls, as pre-condition for the lawfulness of these measures, that the latters shall be put in place in compliance with the relevant national law of the Member State of the designated competent authority[5].

The EDPS issues these comments as guidance for the EU legislators for the negotiation on this legislative initiative having regard to its compatibility with the rights to privacy and to the protection of personal data as established under the Charter of Fundamental Rights of the European Union (hereinafter, "the Charter") and the Treaty on the Functioning of the European Union (hereinafter, "the TFEU").

2. EDPS Comments

2.1. Preliminary remarks

The EDPS acknowledges the objective of the Proposal (namely, the need to combat the dissemination of terrorist propaganda online) and welcomes in particular the establishment of points of contact by both HSPs and Member States to facilitate communication between them.

The EDPS welcomes that Recital 7 of the Proposal stresses that the Regulation will ensure the protection of the fundamental rights at stake by establishing "appropriate and robust safeguards". In this respect, he also welcomes that the aforesaid recital specifically refers, among others, to "the rights to respect for private life and to the protection of personal data". However, for the sake of clarity, the EDPS recommends to insert in a specific recital a reference to the applicable data protection legislation, i.e. the Regulation (EU) 2016/679[6]

[4] Regulation (EC) No 45/2001 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, OJ L8, 12.1.2001, p. 1.

[5] "In most cases, these powers can only be exercised within a criminal procedure", page 9 of the Impact Assessment.

[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.

(hereinafter "the GDPR") and the Directive (EU) 2016/680 (hereinafter "the Police Directive")[7] and to the monitoring of compliance with aforesaid legislation by the competent supervisory authorities.[8]

Furthermore, the EDPS notes that Article 3 of the Proposal provides that HSPs, when taking actions against the dissemination of terrorist content, should take into account the fundamental importance of the freedom of expression and information in an open and democratic society. As these actions will also have a significant impact on the fundamental rights to privacy and to the protection of personal data, the EDPS recommends to insert in Article 3 of the Proposal the reference to these fundamental rights, enshrined under Article 7 and 8 of the Charter and Article 16 of the TFEU.

The EDPS also observes that the Proposal **does not provide specifications (on the administrative or criminal law nature, for instance) on the "competent authorities"** to be designated by each Member State pursuant to Article 17. This may raise issues linked to lack of harmonization among Member States and potentially hinder the cooperation and the exchange of information between these authorities.

2.2. On the proactive measures: respect for fundamental rights to privacy and the protection of personal data and risk-based approach

Pursuant to Article 6 of the Proposal, HSPs should take proactive measures to protect their services against the dissemination of terrorist content. Recital 18 of the Proposal elaborates that such 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 to identify **new** terrorist content (using reliable technical tools).

In this regard, the EDPS notes that according to Article 6 proactive measures should be taken by the HSPs "taking into account", among others, "the fundamental rights of the users." The EDPS considers that a stronger wording is needed, replacing "*take into account*" with *"respect*"[9].

We welcome that Article 6 states that proactive measures should be proportionate and take into account **the risk and level of exposure of the HSP to terrorist material**[10]. In this regard, the EDPS recommends inserting in the Proposal the requirements for the HSP to: (i) perform a **risk assessment** on the level of exposure of the HSP to terrorism content; and (ii)

[7] 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.

[8] In this sense, see the wording of Recital 39 of the Commission Recommendation (EU) 2018/334 of 1 March 2019 on measures to effectively tackle illegal content online, published on the Official Journal of the European Union, 6.3.2018, L63/50: "In order to ensure respect for the fundamental right to the protection of natural persons in relation to the processing of personal data, as well as the free movement of personal data, the processing of personal data in the context of any measures taken to give effect to this Recommendation should be in full compliance with the rules on data protection, in particular with Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council (1), and should be monitored by the competent supervisory authorities."

[9] This would also be in accordance with the wording of recital 7 of the Proposal.

[10] See at page 28 of the Impact Assessment: "provisions related to proactive measures would only apply to a subset of hosting service providers, i.e. those exposed to terrorist content, based on objective criteria."

to draw up a **remedial action plan** to tackle terrorist content proportionate to the level of risk identified[11]. The risk assessment and the remedial action plan would allow to better target the measures against terrorist content online and, at the same time, would be a useful accountability tool.

2.3. On the derogation of Article 15(1) of Directive 2000/31/EC laid down under Article 6(4) of the Proposal, as specified under Recital 19

The EDPS notes that pursuant to Article 17(1)(c) of the Proposal each Member State has to designate a competent authority to oversee, among others, the implementation of proactive measures by HSPs. In case a competent authority considers that the measures in place are insufficient and no agreement has been reached with the HSP, Article 6(4) of the Proposal provides that the authority can issue a decision imposing specific, additional proactive measures to the HSP. Recital 19 of the Proposal elaborates that such a decision "should not, in principle, lead to the imposition of a general obligation to monitor, as provided in Article 15(1) of Directive 2000/31/EC."[12] However, Recital 19 further elaborates that "the decisions adopted by the competent authorities on the basis of this Regulation could **derogate from the approach established in Article 15(1) of Directive 2000/31/EC**, as regards certain specific, targeted measures, the adoption of which is necessary for overriding public security reasons." (emphasis added).

Recital 19 thus provides a derogation from Article 15(1) of Directive 2000/31/EC that would enable competent authorities to impose a general monitoring obligation on HSPs. The EDPS recalls that any interference with the fundamental right to data protection must comply with the criteria set out in Article 52(1) of the Charter, in particular the principle of proportionality and necessity.

The EDPS considers that the imposition of a **general monitoring obligation** on HSPs, which would affect a large and undefined number of individuals, irrespective of whether they are under suspicion to disseminate terrorist content or not, constitutes a disproportionate measure exceeding the limits posed by the principles of necessity and proportionality.[13]

Furthermore, the EDPS reiterates his concerns regarding the 'delegated' monitoring of individuals by commercial companies in the context of activities traditionally falling under the competence of law enforcement authorities as regulated under the national law of the Member States and under Union legislation.[14]

---

[11] The Impact Assessment refers to these two safeguards ("risk assessment" and "remedial action plan", specified at page 32) as alternative options to option 3 concerning *the scope* of the proactive measures (option 3 extends the scope to 'new' terrorist content). We consider that option 1 and 2 refer to a feature that is different from the *scope*, namely to the implementation of *safeguards* for the measures under Article 6 of the Proposal pursuant to a risk-based approach.

[12] See also recital 23 of the 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: "The removal of online content constituting a public provocation to commit a terrorist offence or, where it is not feasible, the blocking of access to such content, in accordance with this Directive, should be without prejudice to the rules laid down in Directive 2000/31/EC of the European Parliament and of the Council (11). In particular, no general obligation should be imposed on service providers to monitor the information which they transmit or store, nor to actively seek out facts or circumstances indicating illegal activity."

[13] 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.

[14] EDPS Opinion of 23 June 2008 on the Proposal for a Decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies; EDPS Opinion of 22 February 2010 on the current negotiations by the European Union of an Anti Counterfeiting Trade Agreement (ACTA); EDPS Opinion of 10 May 2010 on the proposal for a Directive of the European Parliament and of the

The EDPS is therefore deeply concerned about the envisaged derogation of Article 15(1) of Directive 2000/31/EC and strongly recommends reassessing the need forsuch a far-reaching measure.

2.4. On the use of automated tools in the context of proactive measures

The EDPS notes 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 may be necessary to enable HSPs to search for terrorist content. However, in the light of factual (reports of misidentification of lawful content[15]) and legal considerations (compliance with the GDPR, which sets principles and safeguards for data subjects subjected to automated processing of their personal data), the EDPS highlights the following.

(i) The EDPS welcomes that Article 8(1) of the Proposal requires HSPs to 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**", since this will enable users to understand what measures are applied by the HSP.
The EDPS observes that, pursuant to Article 9(1) of the Proposal, HSPs are required to introduce effective and appropriate safeguards to ensure that decisions, which are based on automated tools, are accurate and well-founded. In particular, Article 9(2) of the Proposal provides that such safeguards should consist of "**human oversight and verifications** *where appropriate* and, in any event, where a detailed assessment of the relevant context is required [...]".
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. 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. Recital 71 of the GDPR stresses that "*in any case"* such **suitable safeguards** should include: specific information to the data subject; the right to obtain human intervention; to express his or her point of view; to obtain an explanation of the decision reached after such assessment and to challenge the relevant decision.
Against this background, the EDPS recommends replacing the wording "*where appropriate*" with "*in any case*" in Article 8(1) and 9(2) of the Proposal.

(ii) Moreover, taking into account the serious impact of the data processing operations foreseen by the Proposal, we strongly recommend adding - to the transparency obligation *vis-à-vis* the users of the HSPs - a specific **transparency obligation *towards the competent authorities*** referred to under Article 17 of the Proposal ***and the competent Data Protection Authorities*** under the GDPR and the Police Directive. Such transparency obligation for HSPs would consist in **quality assurance checks** (auditing) of the automated systems in use to prove that they are actually performing as intended, and not producing discriminatory,

Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.
[15] See at page 14 of the Impact Assessment.

erroneous or unjustified results, providing the auditor with all necessary information about how the automated system works[16].

(iii) It is of utmost importance that the automated tools are used in a cautious and targeted way and that their search parameters are **not based solely on sensitive information**, as for instance religious beliefs [in accordance with Article 22(4) of the GDPR, laying down the prohibition to take automated decisions based exclusively on special categories of data listed under Article 9 of the GDPR]. The EDPS recommends the insertion of a provision in the Proposal addressing this issue.

(iv) The EDPS recalls that the GDPR introduced in Article 25 the concept of **data protection by design and by default**. This concept requires controllers to implement appropriate technical and organisational measures in order to effectively ensure compliance with the data protection principles and to integrate the necessary safeguards to meet the requirements of the GDPR and in particular to protect the rights of data subjects. Moreover, the concept requires controllers to ensure that by default only those personal data are processed, which are necessary for the specific purpose of the processing.
Given the nature, scope, context and purpose of the processing, we consider that the HSP shall also carry out a **data protection impact assessment** on the automated processing via the IT tool.
The EDPS therefore recommends the insertion (in recital 17 of the Proposal) of a reference to the principle of **data protection by design and by default** and to the need to perform a **data protection impact assessment** pursuant to the GDPR.

2.5. On the preservation of content and related data

As preliminary observation, the EDPS has **strong concerns on the necessity and proportionality of the 'repository' of content and related data established under Article 7 of the Proposal**. In this regard, we observe that the Impact Assessment does not seem to provide a sound justification, nor sufficient supporting elements.
We note that, pursuant to recital 31 of the Proposal, the HSPs have the obligation to inform the competent law enforcement authorities of the existence of any evidence of terrorist offences that they become aware of. Hence, on the one hand, the added value of the repository for the countering of terrorist offences is unclear or however lessened by the obligation to inform law enforcement authorities. On the other hand, the Impact Assessment acknowledges the risks posed by the preservation of content and related data[17] (content and data not limited to the aforesaid terrorist evidence) for the 'double purpose' of allowing a check on removed content to identify 'false positives' but also for the purpose of criminal investigation[18].
Hence, the EDPS considers that the introduction of the obligation to preserve content and "related data" for the purpose of criminal law investigation on terrorism offences is most probably disproportionate having regard to the risks posed to fundamental rights and

[16] See, in this regard, the WP29 (now EDPB) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, at page 32, "Appropriate safeguards".
[17] See at page 105-106 of the Impact Assessment: "the requirement under option 3 for HSP to preserve content removed through proactive measures would have an impact on the right to data protection and privacy, as it is likely that preservation of the aforesaid content will also involve retention of the data related to the content provider (and possibly other third parties)."
[18] The Impact Assessment specifies the double function of this repository, namely "as a safeguard in cases of erroneous removal and to facilitate criminal investigations", at page 7; and "to ensure the existence of evidence for any potential criminal investigations", at page 29.
Recital 20 of the Proposal refers to the obligation to preserve content "for investigative and prosecutorial purposes"; "the required preservation of data is limited to data that is likely to have a link with terrorist offences".

freedoms. The EDPS therefore recommends duly reconsidering the necessity and proportionality of this far-reaching measure. On the basis of such re-assessment, it may be considered more appropriate to restrict the purpose and use of the repository to the function of allowing checks on false positives only, thus abandoning the current 'dual purpose regime'.

Without prejudice to this preliminary observation, regarding the 'repository' established under Article 7 of the Proposal, we point out that:
(i) HSPs shall ensure that **not only 'data at rest' (stored) in the repository, but also 'data in transit'** (transmitted to and from) are subject to appropriate security measures. We hence recommend an addition in this regard to Article 7(3);
(ii) HSPs shall provide for regular **data quality reviews** of the content and related data preserved in order to ensure that only relevant, accurate and up to date data are stored and processed. A provision in this regard should be added to Article 7.

Furthermore, we observe that the data related to the terrorist content ("related data") that are subject to the preservation requirement are broadly described by way of examples under recital 20 of the Proposal ("related data can include data such as '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 or log-off from the service, together with the IP address allocated by the internet access service provider to the content provider").
In the light of the interference of this 'preservation requirement' and of its impact (potentially allowing the starting of a criminal law procedure), the EDPS strongly recommends to **clearly and specifically define "related data"** as a close, exhaustive list of data categories, to be established in accordance with the principle of 'data minimisation' [Article 5(1)(c) of the GDPR].

3. Concluding remarks

The EDPS considers that, in the absence of the safeguards specified in these comments, the overall interaction of the measures envisaged by the Proposal determines a **serious interference** on the right to the protection of privacy and personal data and to the other fundamental rights and freedoms of the persons concerned.

Such assessment is based on the consideration that the Proposal puts forward a system for the detection of terrorist content that (in its 'worst-case scenario') potentially combines the following elements:
- **proactive** (that is, upon the HSP's own initiative), **automated** [and **general monitoring**] system of detection of 'terrorist content'[19];
- stored (preserved in an ***ad hoc*** **repository)** together with (unspecified) **"related data"** by the HSP for six months (or longer where needed) and made available to law enforcement authorities and to the Courts for the purpose of **prevention, detection, investigation and prosecution of terrorist offences**.

The EDPS observes that the Commission, in the Impact Assessment to the Proposal[20], has **not sufficiently evaluated** the impact of such 'system' on the right to the protection of personal data and the possible mitigating safeguards. The Impact Assessment broadly identifies "the

[19] Including terrorist content under letter (a) of Article 2(5) of the Proposal, referring to "inciting or advocating, the commission of terrorist offences", which are less directly linked to terrorist offences compared to Article 2(5)(c) and in relation to which the risk of misidentification is higher.
[20] See in particular at pages 40-43 of the Impact Assessment.

need to **lay down clear and precise rules** governing the scope and application of measures [..] especially in cases of retention for law enforcement purposes"[21], taking into account that "technology is still prone to errors [..] and presents risks of erroneous removal of legal content"[22]. Nonetheless, in a non-consequential way, many provisions of the Proposal (for example the reference to "related data") **still need specification** or provide for a **broad discretion** (see wording: "where appropriate") having regard to the safeguards for the persons concerned.

In the light of all of the above, the EDPS considers that the Proposal, in its current text, due to its serious interference on fundamental rights and freedoms, impacting on both suspects and non-suspects persons, is at risk of being considered by the Court of Justice of the European Union, following its consolidated case-law[23], as not proportionate to the aim pursued and therefore unlawful.

Brussels, .. October 2018

[21] See at page 43 of the Impact Assessment.

[22] See ta page 41 of the Impact Assessment.

[23] See Joined Cases C203/15 and C-698/15, *Tele2 Sverige AB, already referred to under footnote 5 of these comments.*