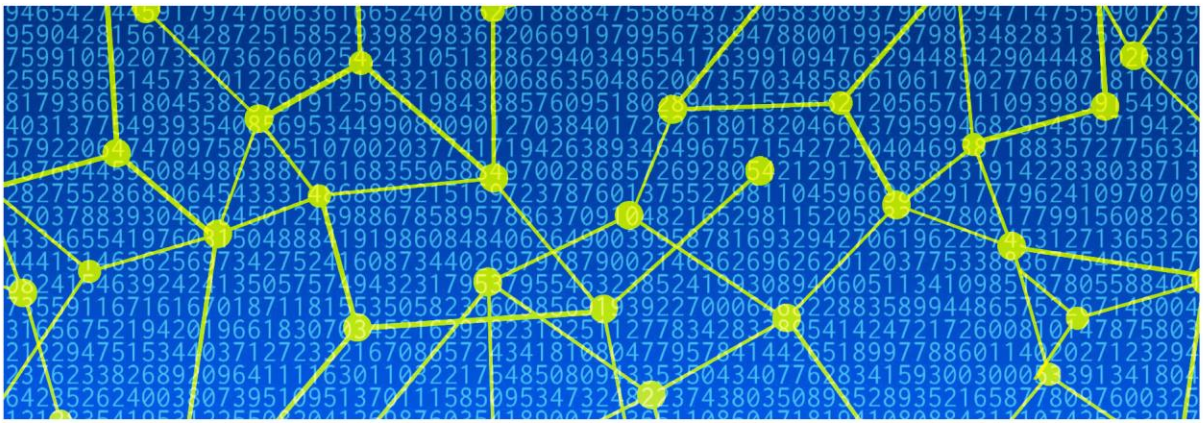

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2019

EDPS Opinion regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention

EDPS

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

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 coherently and consistently applying the EU data protection principles when negotiating agreements in the law enforcement sector, in line with Action 5 of the EDPS Strategy: 'Mainstreaming data protection into international agreements'. It builds on the general obligation that international agreement must comply with the provisions of the Treaty of the Functioning of the European Union (TFEU) and the respect for fundamental rights that stands at the core of EU law. In particular, compliance with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union and Article 16 TFEU must be ensured.

Executive Summary

On 5 February 2019, the European Commission issued a Recommendation for a Council Decision authorising the Commission to participate on behalf of the Union in the negotiations of a second additional protocol to the Budapest Convention on Cybercrime. The Annex to the Recommendation sets out the recommended Council's directives to negotiate the protocol. This protocol aims to improve the traditional cooperation channel and to include provisions for direct cooperation between law enforcement authorities and service providers cross-border as well as provisions on transborder direct access to data by law enforcement authorities.

The EDPS welcomes and actively supports the recommendation of the European Commission to be authorised to negotiate, on behalf of the European Union, a second additional protocol to the Cybercrime Convention. As the EDPS has long argued, the EU needs sustainable arrangements for sharing personal data with third countries for law enforcement purposes, fully compatible with the EU Treaties and the Charter of Fundamental Rights. Even when investigating domestic cases, law enforcement authorities increasingly find themselves in "cross-border situations" because information is stored electronically in a third country. The growing volume of requests and the volatility of digital information put a strain on existing models of cooperation, such as MLATs. The EDPS understands that authorities face a race against time to obtain data for their investigations and supports efforts to devise new models of cooperation, including in the context of cooperation with third countries.

This Opinion aims to provide constructive and objective advice to the EU institutions as the Council has to deliver its directives before the start of this delicate task, with broad ramifications. The EDPS stresses the need to ensure full respect for fundamental rights, including privacy and the protection of personal data. While the EDPS recognises that it is not possible to replicate entirely the terminology and definitions of EU law in an agreement with third countries, the safeguards for individuals must be clear and effective in order to fully comply with EU primary law. The Court of Justice of the European Union in recent years has affirmed data protection principles including fairness, accuracy and relevance of information, independent oversight and individual rights of individuals. These principles are as relevant for public bodies as they are for private companies and become all the more important considering the sensitivity of the data required for criminal investigations.

Many safeguards already envisaged are welcome, but they should be reinforced. The EDPS has identified three main improvements which he recommends for the negotiating directives, in order to ensure compliance with the Charter and Article 16 TFEU:

- ensuring the mandatory nature of the envisaged protocol,

- including detailed safeguards, including the purpose limitation principle, due to the various potential signatories, not all of them being parties to the Convention 108 or having concluded an equivalent agreement to the EU-US Umbrella agreement,

- opposing any provisions on direct access to data.

Additionally, the Opinion offers further recommendations for improvements and clarifications of the negotiating directives. The EDPS remains at the disposal of the institutions for further advice during the negotiations and before the finalisation of the protocol.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EU) 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 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 [2], in particular Articles 42(1), 57(1)(g) and 58(3)(c) thereof,

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. On 17 April 2018, the Commission issued a package of two legislative proposals: a Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[4] (hereinafter "the e-evidence Proposal"), and a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[5]. While work is ongoing at the European Parliament, the Council of the European Union (the Council) has reached a general approach on those two proposals[6].

2. On 5 February 2019, the Commission adopted two recommendations for Council Decisions: a Recommendation to authorise the opening of negotiations in view of an international agreement between the European Union (EU) and the United States of America (US) on cross-border access to electronic evidence for judicial cooperation in criminal matters[7] and a Recommendation to authorise the participation of the Commission, on behalf of the EU, in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) (hereinafter "the Recommendation")[8]. The first recommendation is the subject of a separate EDPS Opinion[9]. However, the European Data Protection Supervisor (EDPS) considers that both negotiations with the US and at the Council of Europe are closely linked.

3. The Recommendation was adopted on the basis of the procedure laid down in Article 218 of the Treaty on the Functioning of the European Union (TFEU) for agreements concluded between the EU and third countries. With this Recommendation, the Commission seeks to

obtain authorisation from the Council to be appointed as the negotiator on behalf of the EU for the second additional protocol to the Budapest convention on cybercrime (CETS No 185)[10], along the negotiating directives annexed to the Recommendation. The Annex to the Recommendation (hereinafter "the Annex") is of utmost importance since it lays down the recommended Council's directives to the Commission to negotiate, on behalf of the EU, the protocol. Once the negotiations are completed, in order for the agreement to be concluded, the European Parliament will have to give its consent to the text of the agreement negotiated, after which, the Council will have to adopt a decision concluding the agreement. The EDPS expects to be consulted on the text of the draft agreement in due course in accordance with Article 42(1) of Regulation (EU) No 2018/1725.

4. The EDPS welcomes that he has been consulted following the adoption of the Recommendation by the European Commission pursuant to Article 42(1) of Regulation (EU) No 2018/1725. The EDPS also welcomes the reference to this Opinion in Recital 8 of the Recommendation. He wishes to underline that this Opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information, the provisions of the draft protocol during the negotiations and legislative developments in third countries.

2. OBJECTIVES OF THE SECOND ADDITIONAL PROTOCOL

5. The Convention of the Council of Europe on enhanced international cooperation on cybercrime and electronic evidence (hereinafter the "**Cybercrime Convention**") is open to Member States of the Council of Europe and non-members (upon invitation). At present 62 countries are parties to the Convention, including 26 EU Member States (all except Ireland and Sweden, who have signed it) and other third countries members of the Council of Europe such as Armenia, Azerbaijan, Turkey as well as countries who are not members of the Council of Europe, such as Australia, Canada, Ghana, Israel, Japan, Morocco, Paraguay, Philippines, Senegal, Sri Lanka, Tonga and the US[11]. The Cybercrime Convention is not open for signature by the EU.

6. The Cybercrime Convention is a binding international instrument requiring the contracting parties to lay down specific criminal offences committed against or by means of electronic networks in their national law and establish specific powers and procedures enabling their national authorities to carry out their criminal investigations, including for collecting evidence of an offence in electronic form. It entails minimum requirements on investigative powers available in a criminal investigation. The Cybercrime Convention also fosters international cooperation between the contracting parties.

7. In its guidance note # 3 adopted in 2014[12], the Cybercrime Convention Committee (hereinafter the "T-CY") stated that "*[o]verall, practices, procedures as well as conditions and safeguards vary considerably between different Parties. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdiction or "in the cloud" as well as national sovereignty persist and need to be addressed*".

8. In June 2017, to address the deficiencies and the ambiguities of the convention framework, the Parties to the Cybercrime Convention decided to start working on a **Second Additional**

Protocol to the Convention, with a view to finalise this process by the end of 2019[13]. The protocol may include:

- **Provisions for more effective mutual legal assistance**:
  - a simplified regime for mutual legal assistance requests for subscriber information;
  - international production orders;
  - direct cooperation between judicial authorities in mutual legal assistance requests;
  - joint investigations and joint investigation teams;
  - requests in English language;
  - audio/video hearing of witnesses, victims and experts;
  - emergency MLA procedures.
- **Provisions allowing for direct cooperation with service providers[14]** in other jurisdictions with regard to requests for **subscriber information, preservation requests, and emergency requests.**
- Clearer framework and stronger safeguards for existing practices of **transborder access to data[15].**
- **Safeguards, including data protection requirements**[16].

The European Commission takes part in plenary meetings of the T-CY as an Observer Organisation.

3. MAIN RECOMMENDATIONS

3.1. EU-level mandate and mandatory nature of the protocol

9. According to the Commission, the protocol "*is of direct relevance to existing and future development of common EU rules*". Once negotiations have been concluded, the protocol "*may eventually include measures covering areas where the EU has already adopted legislation – including on judicial cooperation and the protection of fundamental rights*". The negotiations on the protocol "*may also relate to future EU legislation – in particular on cross-border access to electronic evidence*"[17] (the e-evidence Proposal above mentioned). It is important that the EU participates in the negotiations to help shape this protocol. Given the significance of the topics discussed at international level for EU policy in the area of collecting electronic evidence in criminal matters, in particular for the protection of personal data and privacy, and the already advanced stage of the discussion after two years of negotiations, **the EDPS strongly supports the adoption of a Council Decision giving a clear mandate to the European Commission** to participate, on behalf of the EU, in these on-going negotiations. The Commission would be best placed to ensure that the protocol is compatible with current and future EU legislation. This should allow the EU together with its Member States to better ensure the legality of the future agreement within the EU legal order, including compliance with the Charter of Fundamental Rights of the EU (hereinafter the "Charter"), in particular the rights to privacy and to protection of personal data, and with Article 16 TFEU. Therefore, this Opinion aims to provide constructive and objective advice to the EU institutions. The EDPS will remain at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process.

10. As the various international agreements providing for cross-border exchanges of evidence impact on the fundamental rights of data subjects to the protection of their personal data and to privacy, it is important that the legal framework in which they operate is defined as clearly as possible. It stems from **paragraph (e)** of the Annex that the protocol "*may apply in the absence of other more specific international agreements binding the European Union or its Member States and other Parties to the Convention, or, where such international agreements exist, only to the extent that certain issues are not regulated by those agreements*"[18]. The use of the verb "may" leaves an ambiguity as to the nature of the envisaged protocol. **To ensure legal certainty, the EDPS recommends clarifying the binding and mandatory nature of the instrument as a principle[19]** and subject to bilateral agreements between parties to the protocol concluded on the same matters "*provided that this is done in a manner consistent with the convention's objectives and principles*". **It should be clarified that such bilateral agreements also concern future agreements as specified in the explanatory memorandum of the recommendation[20]. The EDPS would recommend to specify that it should be the case only if the application of the other specific international agreement provides the same or higher level of protection regarding privacy and personal data than the envisaged protocol**.

3.2. Need for detailed safeguards regarding international data transfers and the respect of fundamental rights

11. The Court of Justice of the EU (CJEU) found that "*the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness*"[21].

12. The EDPS considers that appropriate safeguards with regard to the right to data protection requires in the first place **full consistency with Article 8 of the Charter in the third countries to which personal data would be transferred.** He points out that according to the case law of the CJEU, both Articles 7 and 8 of the Charter have to be assessed in conjunction with the **right to effective remedy enshrined in Article 47 of the Charter**[22].

13. **The EDPS therefore welcomes the attention paid to privacy and data protection in the Annex**. The EDPS shares indeed the view that the safeguards should apply to "*all investigatory powers both existing in the context of the Convention and created by the Second Additional protocol*"[23]. **Paragraphs (b) and (c),** in particular, seem to oppose protection of personal data to protection of electronic communication data. The EDPS recommends clarifying that the envisaged Protocol should ensure the respect for both fundamental rights to privacy on the one hand, and to the protection of personal data, whether or not they constitute electronic communication data, on the other hand.

14. **Purpose limitation** is a key data protection principle. The recommended negotiating directives neither specify any limits to the cooperation under the envisaged protocol nor contain any specific limit with regard to the further processing of the transferred personal data by the requesting third country authority. **The EDPS recommends specifying narrowly the purposes of the transfers in the Annex and the prohibition of further processing incompatible with those purposes.**

15. The EDPS stresses that compliance with this principle is closely linked to the scope of competence of recipients in the receiving third countries. The scope of competence of the specific authorities in the third countries to which data would be transferred and which would process these data should be clearly defined in order to ensure that they are also competent for the purposes of the transfer. In that sense, therefore, the EDPS **recommends that the envisaged protocol be accompanied by an exhaustive list of the competent authorities in the receiving countries to which data would be transferred as well as a short description of their competences. This should also be reflected in one of the directives of the Annex**.

16. In addition, sending and answering orders for the production of data under the envisaged protocol would entail the **transfer of personal data**. In July 2017, the CJEU delivered Opinion 1/15[24] on the international agreement regarding the transfer of Passenger Name Records (PNR) data to Canada, in which it sets out the conditions under which an international agreement can provide a legal basis for transfers of personal data. The CJEU found that "*a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union*"[25]. **Therefore, it follows from Opinion 1/15 that the level of protection resulting from the envisaged protocol for the exchange of personal data with third countries should similarly** (to the agreement between the EU and Canada on the transfer of PNR data) **be essentially equivalent to the level of protection provided for in EU law.**

17. In this regard, the EDPS underlines that while all Member States are parties to the Convention 108[26] of the Council of Europe which is applicable in the law enforcement area, not all third countries parties to the Cybercrime Convention are parties to the Convention 108[27]. It is therefore **particularly acute to ensure the inclusion in the envisaged protocol of strong and detailed safeguards**. Also, the EDPS draws the attention on the importance of gathering information on the level of protection of personal data of third countries parties to the Cybercrime Convention[28] as well as on their political context**, so as to be able to define the precise safeguards necessary.**

3.3. Direct access by law enforcement authorities to data

18. According to the Recommendation[29], the protocol "*may include provisions in relation to the 'Extension of searches and access based on credentials'[30] and 'Investigative Techniques'*". The Commission assessed in the Impact Assessment for the e-evidence Proposal the possibility to introduce a direct access provision at EU level and decided not to. However, it stems from the Recommendation[31] that it is the Commission's view, that the adoption of an e-evidence package on the basis of the Commission proposals would not prevent Member States from maintaining or adopting such measures[32].

19. The EDPS notes that safeguards are envisaged in the mandate under **paragraph (m) of the Annex**. However, **the EDPS considers this measure as particularly intrusive and consequently with a bigger impact on the fundamental rights to privacy and data protection**. Hence, without further clarifications on the specific measures and stronger safeguards envisaged, **he recommends opposing the introduction of such provisions in the protocol**. He refers in this regard to the Article 29 Working Party comments on the issue of direct access by third countries law enforcement authorities to data stored in other

jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest convention on cybercrime[33]. He is not in favour of **paragraph (n) of the Annex** according to which the EU "*should also ensure that it does not restrict the possibilities for such access that are currently provided for in Member States*".

4. ADDITIONAL RECOMMENDATIONS

20. The EPDS wishes to express the following general observations and specific recommendations on the negotiation directives included in the Annex to the Recommendation. The EDPS welcomes that several directives refers to ensuring appropriate data protection safeguards. He considers that those principles and safeguards should be further specified and reinforced.

21. The EDPS would like to insist on the importance of providing concrete, specific and effective safeguards. Given the law enforcement context and the potential risks that such transfers of data could pose to data subjects, the safeguards included in this protocol with third countries should satisfactorily address and mitigate these risks.

4.1. Legal basis of the Council Decision

22. The explanatory memorandum of the Recommendation states that "*the subject matter of the Second Additional Protocol would fall [...] in particular in the field of instruments on judicial cooperation in criminal matters (Article 82(1) TFEU) and data protection ([Article]16 TFEU) (...)*"[34]. These two provisions are also referred to in Recital 6 of the Recommendation, according to which "*Articles 82(1) and 16 of the Treaty on the Functioning of the Union specify Union competencies in the area of judicial cooperation in criminal matters as well as in data protection and privacy. In order to protect the integrity of Union law and to ensure that the rules of international law and Union law remain consistent, it is necessary that the Union participates in the negotiations on the Second Additional Protocol*". However, the citations in the preamble of the Recommendation do not refer to the substantive legal basis of the legal act.

23. In accordance with Article 296 (2) TFEU and the settled case law of the CJEU[35], the EDPS questions the fact that the citations in the preamble to the Council Decision only refer to the appropriate procedural legal basis and do not equally refer to the relevant substantive legal basis.

24. **The EDPS recommends that the citations in the preamble of the Council Decision not only refer to the appropriate procedural legal basis but also to the relevant substantive legal basis, among which Article 16 TFEU.** It already follows from section 1 of the Annex on the negotiating directives that the Commission should simultaneously pursue several objectives during the negotiations of the envisaged protocol, among which ensuring respect for the fundamental rights enshrined in the Charter, including the rights to privacy and the protection of personal data so as to allow for the lawful transfer of personal data. The envisaged protocol would thus indeed relate directly to the objective pursued by Article 16 TFEU.

25. The EDPS recalls that, in a similar law enforcement context, the CJEU found that "*the Council Decision on the conclusion of the envisaged Agreement [between Canada and*

the European Union on the transfer and processing of Passenger Name Record data] must be based jointly on Article 16(2) and Article 87(2)(a) TFEU"[36].

4.2. Onward transfers

26. In relation to onward transfer by the receiving authority in the third country to another third country, the EDPS points out that the CJEU held in Opinion 1/15 of July 2017 that the same requirement as for transfers of ensuring a level of protection essentially equivalent to that guaranteed in the EU *"applies in the case of the disclosure of PNR data by Canada to third countries (...) in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law"*. The Court added that *"such disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or [an adequacy] decision of the Commission (...) covering the authorities to which it is intended PNR data be transferred"*[37]. Therefore, **the EDPS recommends including this additional requirement in the negotiating directives.**

4.3. Rights of data subjects

27. The EDPS takes note of the fact that the Annex does not include any specific directive regarding the data subject rights. The right of access and the right to rectification are essential elements of the right to data protection under Article 8(2) of the Charter. The EDPS recognises that exercise of data subjects' rights are usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations. He recalls however that in its Opinion 1/15, the CJEU found that "*air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities*" considering that *"[t]hat information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal*"[38].

28. Therefore, **the EDPS recommends including the right to information and the right of access in the negotiating directives so that the parties to the envisaged protocol ensure that restrictions to the exercise of the right of access are selectively limited to what is indispensable to preserve the public interests pursued and to strengthen the obligation for transparency upon competent authorities.**

4.4. Control by an independent authority

29. Article 16 TFEU and Article 8(3) of the Charter include as essential guarantee of the right to data protection: the control by an independent authority. While each Member State has appointed an independent authority in charge of supervising the data processing activities, including the transfer of data to third countries, there is also a need for an effective independent oversight once the data have been transferred in the receiving third countries.

30. The EDPS recalls that, pursuant to the CJEU case law[39], an independent supervisory authority within the meaning of Article 8(3) of the Charter is an authority able to make

decisions independently from any direct or indirect external influence. Such a supervisory authority must not only be independent from the parties it supervises, but it should also not be "*subordinate to a further supervisory authority, from which it may receive instructions*" as this would imply that it is "*not free from any external influence liable to have an effect on its decisions*"[40].

31. The EDPS notes that the negotiating directives do not specifically address this requirement.

32. The EDPS recommends that the negotiating directives aim at introducing in the protocol a **mechanism requiring each country party to the protocol to clearly identify the specific authority or authorities entrusted** by it with the independent oversight of compliance with the rules of the envisaged protocol. The **effective powers** that this specific authority or authorities may exercise over authorities to which personal data would be transferred on the basis of the envisaged protocol should be specified in the protocol.

4.5. Judicial redress and administrative remedies

33. The EDPS recalls that the CJEU found[41] that the lack of effective judicial redress when personal data are transferred to a third country goes to the essence of Article 47 of the Charter, which provides for the right to an effective judicial protection. In that context, the CJEU found that "*legislation not providing for <u>any</u> possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" and that "*the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to **an effective remedy** before a tribunal in compliance with the conditions laid down in that article*"[42].

34. Also, the CJEU has stressed that it is essential for individuals to be able to file complaints with independent supervisory authorities[43] and seek, therefore, administrative redress.

35. **The EDPS recommends including in the mandate the objective of ensuring that the Protocol does ensure that both redresses are available to all data subjects,** all the more that not all parties to the Cybercrime Convention fall under the jurisdiction of the European Court of Human Rights.

4.6. Criminal offences covered by the protocol and categories of personal data

36. According to the CJEU case law, only the objective of fighting <u>serious crime</u> is capable of justifying the access by public authorities to personal data retained by service providers "*which taken as a whole, allow very precise conclusions to be drawn concerning the private lives of the persons concerned*"[44]. Where such conclusions cannot be drawn and therefore access could not "*be defined as a serious interference with the fundamental rights of the persons whose data is concerned*", the Court further held that "*the interference that access to such data entails is capable of being justified by the objective*

of (...) preventing, investigating, detecting and prosecuting 'criminal offences' generally without it being necessary that those offences be defined as 'serious'"[45].

37. In relation to the acquisition of knowledge of the **content data**, it stems from the CJEU case law that it may adversely affect the essence of the right to privacy[46].

38. In relation to non-content data, the CJEU found as regard metadata such as traffic data and location data, stored by providers of publicly available electronic communications, that *"taken as a whole, [they] may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"*[47] and *"[provide] the means [...] of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications"*[48].

39. **The EDPS stresses the importance of laying down clear and straightforward definitions of data categories in the envisaged protocol in order to ensure legal certainty** for all stakeholders involved. To the extent the definitions of data categories in the e-evidence Proposal would be used as reference, as previously raised by the EDPB[49], **the EDPS recommends ensuring a clear delineation between data categories and avoiding any overlap, which would also highly contribute to ensuring legal certainty** regarding the substantive provisions of the protocol.

40. To comply with the proportionality condition of Article 52(1) of the Charter, the EDPS considers that a balance between the types of offences for which the production and transfer of personal data could be ordered and the categories of data concerned should be reached. Thus, distinctions should also be based on the seriousness of the offences investigated or prosecuted and the level of intrusiveness and sensitivity of the data categories sought. Thus, **the EDPS recommends specifying in the negotiating directives that distinctions should also be made based on the seriousness of the offences concerned**. In this regard, the **EDPS is in favour of defining a common list of offences distinguishing between the seriousness of the offences and which may vary depending on the intrusiveness of the measures foreseen in the protocol**.

4.7. Information security

41. The EPDS considers that the envisaged protocol raises important questions regarding the security of cross-border incoming and outgoing transmission of personal data. The EDPS wishes to stress that ensuring the security of personal data is not only a clear requirement under EU law[50], but it is also considered by the CJEU in relation to the essence of the fundamental right to data protection. Data security is also essential to ensuring the secrecy of investigations and the confidentiality of criminal proceedings.

42. Therefore, **the EDPS recommends to include further additional privacy and data protection safeguards in the mandate in order to ensure an appropriate level of security for the personal data produced and transferred. In addition, the mandate should notably address the questions of the authenticity of orders and the security of**

the transmission of personal data to the requesting authorities which should be ensured.

4.8. Privileges and immunities

43. The EDPS recommends including in the mandate that in addition to providing for appropriate safeguards for personal data protection, the protocol should ensure the respect of other safeguards attached to the data such as privileges and immunities.

4.9. Emergency mutual assistance[51]

44. According to **paragraph (g),** the EU should support the draft text and explanatory report preliminary adopted and the scope of mutual assistance should be identical to that set forth in Article 25 of the Cybercrime Convention. In absence of any cross reference to a specific version of the draft, the EDPS bases his comments on the provisional draft dated 28 November 2018 available online on the Council of Europe website[52]. **The EDPS recommends to provide for the possibility to reconcile both objectives of fighting against crime and respecting fundamental rights by ensuring that the protocol will allow the requested party to impose specific safeguards and conditions** for the transfer and to be able to refuse assistance for data protection reasons[53].

4.10. Cross-border direct cooperation between law enforcement authorities and service providers

a) Specific conditions under EU law for the transfer of personal data by Member States' law enforcement authorities directly to services providers established in third countries

45. In this context, attention is drawn to Article 35(1) LED[54] that lists specific conditions for a Member State law enforcement authority to lawfully transfer data to addressees established in third countries, including the principle that, as a rule, the addressee of such transfers shall be a competent authority of a third country for the purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Transfers from Member States law enforcement authorities to other addressees, including private parties established in third countries, are allowed only as a derogation under Article 39 LED[55] and only if further specific conditions[56] are met. Such specific conditions include notably information to be provided to the competent data protection authority in their Member State, and an obligation to document the transfer[57]. **The EDPS considers that the envisaged protocol should at least include those additional conditions inspired by Article 39 LED so as not to lower the level of data protection required by the LED.**

b) Definitions and types of data

46. According to the Recommendation, the provision envisaged would concern subscriber information[58]. The EDPS welcomes **paragraph (k)** providing that the protocol should include "*appropriate fundamental rights safeguards, taking into account the different level of sensitivity of the categories of data concerned and the safeguards included in the European Production Orders for the different categories of data*".

47. The protocol could be an opportunity to further refine the definitions of the categories of data in order to facilitate the implementation of the convention, taking into account the outcome of the negotiations on the e-evidence Proposal as the case may be. **In this regard, the EDPS stresses the importance of laying down clear and straightforward definitions of data categories in the envisaged protocol in order to ensure legal certainty for all stakeholders involved in the EU and third contracting countries**. The possibility to order the production and transfer of content data or non-content data which taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons concerned should be limited to serious crimes only (see section 4.6 above).

c) Involvement of judicial authorities in other countries parties to the protocol

48. With regard to **paragraph (l) of the Annex**[59], the EDPS points out that it appears premature to deem the safeguards consisting in "*notification and consent by the state of the service provider and a prior review carried out either by a court or by an independent administrative body*" as being additional to the e-evidence Proposal as the latter is still under negotiations. The EDPS **recommends a more cautious approach by providing in the Annex for directives to support relevant additional safeguards and grounds for refusal compared to the EU secondary law on the collection of electronic evidence in criminal matters, as required for ensuring the appropriate level of safeguards, in particular with regard to data protection and privacy.**

49. In particular, even in the EU context, in its Opinion on the e-evidence Proposal, the EDPB, to which the EDPS is a member, found "*no justification for the procedure foreseen in the draft e-Evidence Regulation to allow for the production of content data without any involvement at least of the competent authorities of the Member State where the data subject is*"[60]. In Council, no notification to the authorities of the Member State where the data subject is was introduced.

50. Also, the EDPB expressed in its Opinion on the e-evidence Proposal "*its concerns as regards the removal of any double check by the receiving competent authority of the order transmitted, compared to the other instruments*"[61]. In Council, several Member States requested greater power to the notified authority, beyond the notification introduced in the general approach and covering also non-content data[62].

51. In the traditional approach to cross-border access to electronic evidence, it is primarily the responsibility of the enforcing country to ensure the review of limited grounds of refusal. While the EDPS recognises the need to identify alternative approaches to gathering evidence in a cross-border context, the need for effective guarantees for fundamental rights of data subjects remains of paramount importance. It is important to consider that relevant laws in the countries parties to the protocol - inter alia on the admissibility of evidence gathered in another country and what constitutes a criminal offence - may diverge. Conditions for issuing an order are not harmonised on substance at international level and important objections against the recognition and enforcement of such order may exist[63]. Furthermore, private entities may not be equipped to effectively deliver the required assessment. It is critical to keep in mind that despite being the addressees of orders, service providers are not the ones whose rights to privacy and to personal data protection are limited by the order.

52. EU Member States have the legal obligation to respect fundamental rights when implementing EU law[64]. In this regard, in the context of the European Investigation Order (EIO) Directive[65] negotiations, the Fundamental Rights Agency recalled that "***a failure to ensure proper respect for fundamental rights in the execution of an EIO will engage the responsibility of the executing state under instruments such as the ECHR***"[66].

53. **The EDPS considers that effective protection of fundamental rights in this context requires a degree of involvement of public authorities of the requested party to the envisaged agreement.** It is also an additional safeguards in cases where the data subject cannot be located or is located in a third country not party to the protocol. **He therefore recommends including as specific safeguard in the negotiating directives the obligation for the competent authorities of the countries parties to the protocol to systematically involve judicial authorities designated by the enforcing country as early as possible in the process of gathering electronic evidence in order to give these authorities the possibility to effectively review compliance of the orders with fundamental rights and possibly to raise grounds for refusal on the basis of sufficient information and within realistic deadlines**. Such involvement would also be more in line with Article 82(1) TFEU (if this legal basis is included as one of the substantial legal bases of the Council Decision)[67].

d) Possibility for service providers to object

54. Service providers receiving an order for electronic evidence addressed by competent authorities of a third country party to the protocol may find themselves caught between conflicting legal obligations under EU law and third country law. The EDPS welcomes **paragraph (c)** of the negotiating directives, which provides that the protocol should prevent conflicts of laws.

55. The EDPS considers that service providers served with an order for electronic evidence should be able to object to it on specific grounds defined in the envisaged protocol, such as missing or incorrect information or fundamental rights considerations[68]. Those grounds should be clearly defined so as not to allow providers to decide on a case-by-case basis on whether and how to cooperate. Therefore, **the EDPS recommends specifying in the negotiating directives that the protocol should provide for a mechanism allowing a service provider the right to object to an order on specific grounds defined therein**.

4.11. Suspension of the protocol in relation to a country in breach of the protocol and review

56. The EDPS notes that the **section 3** of the Annex provides for the possibility to denounce the protocol along the provisions of the Cybercrime Convention. Similarly to existing adequacy decisions based on Article 45 GDPR and to Article 36(5) LED regarding adequacy decisions for law enforcement purposes, the **EDPS considers it is of utmost importance to include in the negotiating directives the introduction of a clause allowing for the suspension of the protocol with a third country in cases of breaches of its provisions by the said country.**

57. Also, t**he EDPS recommends that the negotiating directives provide for requesting the introduction of a clause setting out the mandatory periodical review of the practical operation of the protocol.** To ensure a meaningful review, it should be provided

for at the latest one year after its entry into force and then at regular intervals, specifying the frequency of these additional reviews. The content of the review should be specified. The review should focus not only on the implementation of the protocol but also on the evaluation of its necessity and proportionality. For the purposes of such a review, it should provide that Contracting parties shall co-operate with the T-CY in the gathering of information, including statistics and case law, concerning the practical operation of the Convention. The review teams should include data protection experts and involve EU Data Protection Authorities.

5. CONCLUSIONS

58. The EDPS understands the need for law enforcement authorities to secure and obtain electronic evidence quickly and effectively. He is in favour of using innovative approaches to obtain cross-border access to electronic evidence and finding an EU response to existing issues in this context. A second additional protocol to be negotiated at EU level would better preserve the level of protection guaranteed by the EU data protection framework and ensure a consistent level of protection throughout the EU, rather than distinct agreements concluded by Member States bilaterally. Therefore, this Opinion aims to provide constructive and objective advice to the EU institutions as the Commission seeks to obtain authorisation from the Council to participate in the negotiations in view of this protocol.

59. The EDPS welcomes that the mandate aims at ensuring that the protocol contains appropriate safeguards for data protection.

60. There are three major recommendations, the EDPS makes for the envisaged protocol to ensure compliance with the Charter and Article 16 TFEU. The EDPS recommends that the negotiating directives aim at:
    - ensuring the mandatory nature of the envisaged protocol,
    - introducing detailed safeguards - including the principle of purpose limitation - due to the various potential signatories, not all of them being parties to the convention 108 or having concluded an equivalent agreement to the EU-US Umbrella agreement,
    - opposing any provisions on direct access to data.

61. In addition to these general recommendations, the recommendations and comments of the EDPS in the present Opinion relate to the following specific aspects:

    - the legal basis of the Council Decision;
    - the onward transfers by third countries competent authorities;
    - the rights of data subjects, in particular the right to information and the right of access;
    - the control by an independent authority;
    - the judicial redress and administrative remedies;
    - the criminal offences covered by the envisaged protocol and the categories of personal data;
    - the specific safeguards to ensure an appropriate level of security of the data transferred;
    - the specific safeguards for data protected by privileges and immunities;
    - the emergency mutual assistance;
    - in the case of direct cooperation, the transfer of personal data, the definition and types of data, the involvement of other authorities, the possibility for service providers served with an order for electronic evidence to object based on specific grounds;

- the possibility to suspend the protocol in cases of breaches of its provisions and to review it.

62. Finally, the EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process. The comments in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise and would then be addressed once further information is available. He expects to be consulted later on the provisions of the draft protocol before its finalisation.

Brussels, 2 April 2019

Giovanni Buttarelli

European Data Protection Supervisor

NOTES

[1] OJ L 119, 4.5.2016, p. 1 (hereinafter "GDPR").
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89 (hereinafter "LED").
[4] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final.
[5] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018)226 final.
[6] The Council adopted its general approach on the proposed Regulation on 7 December 2018, available at https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#. The Council adopted its general approach on the proposed Directive on 8 March 2018, available at https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.
[7] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final.
[8] Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final.
[9] EDPS Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence.
[10] Convention on enhanced international cooperation on cybercrime and electronic evidence, Budapest, 23 November 2001, CETS No. 185.
[11] See the Chart of signatures and ratification of the Cybercrime Convention for a complete and updated list of countries parties to the Cybercrime Convention, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ZZawh58m
[12] T-CY Guidance Note # 3 Transborder access to data (Article 32) T-CY (2013)7 E , p. 3, available at: https://rm.coe.int/16802e726a
[13] See Council of Europe webpage available at: https://rm.coe.int/t-cy-pd-pubsummary/168076316e.
[14] This concerns cases where authorities may directly request to a service provider in another jurisdiction the preservation and production of data.
[15] This concerns cases where authorities may themselves directly access data transborder, without the help of an intermediary.
[16] Terms of References for the Preparation of a Draft 2nd Additional Protocol to the Budapest Cybercrime Convention, June 2017, available at: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.
[17] See European Commission fact sheet available at: http://europa.eu/rapid/press-release_MEMO-19-865_en.htm
[18] Emphasis added.
[19] See Prel. Doc. No 10 of December 2008 - The mandatory / non-mandatory character of the Evidence Convention [in civil and commercial matters]: https://assets.hcch.net/upload/wop/2008pd10e.pdf.
[20] P. 7.
[21] Joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461, par. 285. [Emphasis added].
[22] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.
[23] See in particular par. (b), (c) (m) and (o) of the Annex.
[24] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.
[25] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 214; see also par. 93 of Opinion 1/15.
[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108 (hereinafter "Convention 108").
[27] See in this regard, Art. 29 WP Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, of 22 March 2001 (5001/01/EN/ Final WP 41), p. 6: "signatories should be requested to sign up to the Council of Europe's Convention 108".
[28]It appears in particular that not all third countries parties to the Cybercrime Convention are parties to the Convention 108 or to the European Convention of Human Rights and that some are parties to the African Union Convention on Cyber Security and Personal Data Protection. The protocol amending the Convention 108 so called Convention 108 + has not yet entered into force. It has been signed by many Member States but has not yet been ratified - see table of signature and ratification of the convention 108+: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

[29] Explanatory memorandum p. 6.
[30] Commission Staff Working Document: Impact Assessment, SWD(2018) 118 final (hereinafter "Impact Assessment on the e-evidence Proposal"), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN, p. 33: *"*Extended access, i.e. use of a device of a suspect or witness seized as part of an investigation (e.g. with a search and seizure warrant) to access the data accessible from the device (which can include the cloud). Most Member States allow their public authorities to carry out this type of direct access*"*.
[31] Explanatory memorandum p. 6.
[32] Impact Assessment on the e-evidence Proposal, p. 11: *"*The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it, or to use credentials for an account to access and search data stored under that account. This tool becomes more relevant as data is now regularly stored not on the local device but on servers in a different location, possibly outside of the Member State concerned or even outside of the EU.
Often, the location of this data is not known to law enforcement (so-called "loss of knowledge of location"), and it may be practically impossible to determine, such as in cases where the data is hosted on Darknet services that use multiple layers of IP relays to disguise their location. As a result, it can be difficult to determine whether such searches have a cross-border component.
Member States have different approaches to direct access and the data storage location*"*.
[33] Comments of 5 December 2013, available at https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf
The Article 29 Working Party drew "the attention to the risks involved in a potential Additional Protocol that would legitimise a direct access to data by law enforcement authorities of a Party to data stored within the jurisdiction of another Party. The Article 29 Working Party stresses that the application of such a principle, independently of the way in which it is implemented (e.g. by applying the law or the definitions of consent of the searching Party) would infringe upon key data protection rules and have an adverse impact on individuals' fundamental rights". It added: "An additional protocol to an international Convention that would appear to provide for access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party would be in violation of the EU data protection acquis." It insisted also that "transborder data transfers in the field of law enforcement must exclude blanket/mass transborder access, collection or transfer to/of data, which is incompatible with the EU Charter of Fundamental Rights and the European Convention of Human Rights."
[34] P. 6.
[35] See CJEU Case C-687/15, European Commission v Council of the EU, ECLI:EU:C:2017:803, par. 48 and following.
[36] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 232.
[37] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 214.
[38] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 220. [Emphasis added].
[39] See Case C-518/07, Commission v Germany, ECLI:EU:C:2010:125, par. 25; Case C-614/10, Commission v Austria, ECLI:EU:C:2012:631, par. 36 and 37; Case C-288/12, Commission v Hungary, par. 48; Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 41.
[40] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 230.
[41] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.
[42] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95. [Emphasis added].
[43] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 56 to 58.
[44] Case C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, par. 54, see also par. 56.
[45] CJEU, Case C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, par. 62. [Emphasis added].
[46] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 39.
[47] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 27.
[48] CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson, ECLI:EU:C:2016:970, par. 99.
[49] See European Data Protection Board Opinion 23/2018 of 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (hereinafter "EDPB Opinion 23/2018"), available at: https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf, p. 12: "Indeed, the four categories proposed do not appear to be clearly delineated, and the definition of "access data" still remains vague, compared to the other categories".
[50] Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of 'integrity and confidentiality' under

Article 5(1) (f) GDPR and Article 4(1)(f) LED). The security of the processing covers in particular the ability to ensure the ongoing confidentiality and integrity of processing systems.

[51] According to the draft explanatory report, par. 2, p. 6: "[e]mergencies involving a significant and imminent risk to the life or safety of a person often involve hostage situations in which there is a credible risk of imminent loss of life, serious injury or other harm to the victim and the suspect is negotiating for ransom via email or social media so that the location of the victim may be determined through data stored by the provider, sexual abuse of a child as evidenced by the discovery of recently produced child sexual exploitation or child sexual abuse materials, or other indicia of abuse, immediate post terrorist attack scenarios in which authorities seek to determine with whom the attackers communicated in order to determine if further attacks are imminent, and threats to the security of critical infrastructure in which there is a significant and imminent risk of danger to life or safety of a natural person".

[52] https://rm.coe.int/t-cy-2018-23rev-protoprov-pub-text-v4/16808ff490

[53] See Art. 29 WP Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, of 22 March 2001 (5001/01/EN/ Final WP 41), p. 5 and following.

See also Study "Criminal procedural laws across the European Union - A comparative analysis of selected main differences and the impact they have over the development of EU legislation" commissioned by the European Parliament's Policy Department for Citizen's rights and Constitutional Affairs, PE 604.977, p. 30.

See finally Fundamental Rights Agency, Opinion on the draft Directive regarding the European Investigation Order, 14 February 2011, p. 11: *"[a] fundamental rights-based refusal ground could act as an adequate tool to prevent fundamental rights violations occurring during cross-border investigations. At the same time, the executing state would be required to be familiar with the criminal law rules and procedures of the issuing state, as well as the details of the case at hand. Therefore, a fully-fledged fundamental rights assessment in every case would not only counteract the idea of mutual recognition, but due to complex and long procedures it might also undermine some of the fundamental rights standards set out in section 2.2. For this reason, any establishment of a fundamental rights-based refusal ground in the directive should ideally be complemented by explicit parameters. Such parameters could limit the refusal ground to circumstances where an EU Member State has a well-founded fear that the execution of an EIO would lead to a violation of fundamental rights of the individual concerned. In this way, a fundamental rights-based refusal ground could serve as a 'safety-valve', facilitating EU Member States' compliance with fundamental rights obligations flowing from EU primary law without Member States having to deviate from EU secondary law"*.

[54] 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.

[55] This is a specific derogation from Article 35(1)(b) LED that personal data are transferred by law enforcement authorities in the EU Member States to a controller in a third country or international organisation that is also a law enforcement authority.

[56] The additional conditions are :

"1 (...) (a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary. (...)

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented".

[57] See EDPB Opinion 23/2018, p. 9.

[58] Subscriber information is defined under the convention in Article 18(3): "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographical address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; (c) any other information on the site of the installation of communication equipment,

available on the basis of the service agreement or arrangement". See also explanatory report of the Cybercrime Convention par. 177 and following.

[59] Par. (l) states that: "[W]ith regard to the provisions on 'International productions orders', the European Union should not oppose the inclusion in the Second Additional Protocol of additional safeguards and grounds for refusal compared to the Commission's e-evidence proposals, including as they evolve in the legislative procedure negotiations by the co-legislators and eventually in their final (adopted) form, such as a notification and consent by the state of the service provider and a prior review carried out either by a court or by an independent administrative body, as far as this does not disproportionately reduce the effectiveness of the instrument under the Second Additional Protocol (for example in cases of validly established urgency). Any additional safeguards and grounds for refusal should not affect the functioning of the EU's e-evidence proposals amongst Member States".

[60] See EDPB Opinion 23/2018, p. 16.

[61] See EDPB Opinion 23/2018, p. 17.

[62] See footnote 34 of the Council general approach: "*Czech Republic, Finland, Germany, Greece, Hungary and Latvia have a reservation on the notification procedure advocating for a procedure with more effect that also includes transactional data and a fundamental rights clause, i.e. providing for grounds for refusal to the notified authority; furthermore also rule on what should be considered a "national case" should be reversed; finally Germany advocating for submission of the Order instead of the Certificate, whereas Czech Republic is of the view that both the Order and the Certificate should be submitted"*.

[63] See the list of grounds to object mentioned under Article 14 of the e-evidence Proposal and the case law developed by the CJEU in the context of the European Arrest Warrant (CJEU, Case C-404/15, Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen, ECLI:EU:C:2016:198, par. 82 and following).

[64] See Articles 6 TUE and 67(1) TFUE. See also Fundamental Rights Agency, Opinion on the draft Directive regarding the European Investigation Order, 14 February 2011, footnote 56: "*[i]n this context, one should be reminded of the principle of extraterritorial responsibility under the ECHR. EU Member States are responsible under the ECHR for human rights violations committed in another territory where through their action they have placed someone in that situation; see ECtHR, Soering v. United Kingdom, No 14038/88, 7 July 1989. See also ECtHR, Bosphorus v. Ireland, No. 45036/98, 30 June 2005, par. 156 'the presumption will be that a State has not departed from the requirements of the Convention when it does no more than implement legal obligations flowing from its membership of the [EU].' This presumption was considered to be rebuttable"*.

[65] Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014, regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1.

[66] See Fundamental Rights Agency, Opinion on the draft Directive regarding the European Investigation Order, 14 February 2011, footnote 61 referring to ECtHR Case, MSS v. Belgium and Greece, No. 30696/09, 21 January 2011.

[67] See Recital 6 of the Recommendation.

[68] See EDPB Opinion 23/2018, p. 17, where the EDPB recommended that the e-evidence Proposal "*should at least foresee the minimum classic derogation that if there are substantial grounds for believing that the enforcement of an Order would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the enforcement of the order should be refused"*.