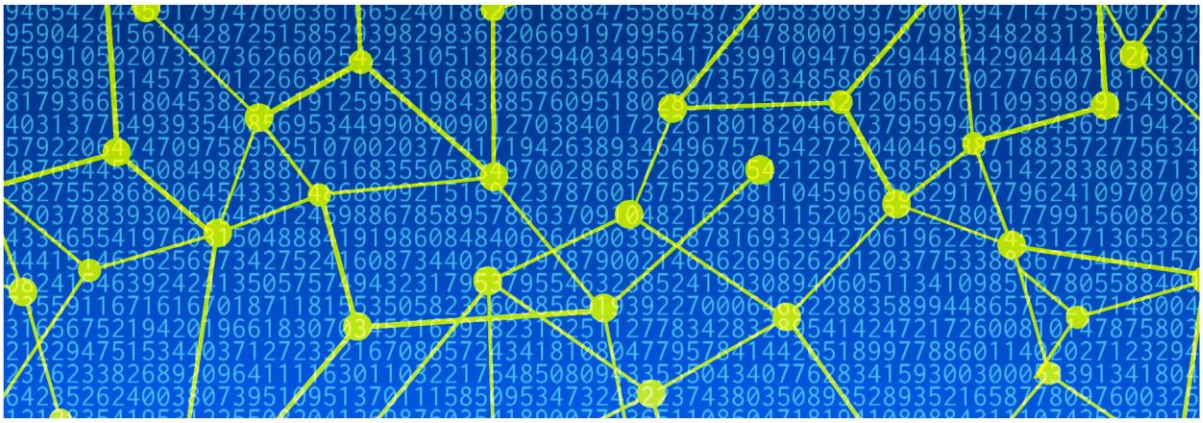

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 2/2019

EDPS Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence

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 agreements must comply with the provisions of TFEU and the respect for fundamental rights that stands at the core of EU law. In particular, compliance with Articles 8 of the Charter of Fundamental Rights of the EU and 16 TFEU must be ensured.

Executive Summary

On 5 February 2019, the European Commission issued a Recommendation for a Council Decision authorising the opening of negotiations to conclude an international agreement with the United States of America (US) on cross-border access to electronic evidence. The Annex to the Recommendation sets out the Council's directives to negotiate the agreement. The objective of the proposed agreement would be to address, through common rules, the legal issue of access to content and non-content data held by service providers in the EU and the US.

The EDPS welcomes and supports the objective of the Commission to conclude an agreement on cross-border access to electronic evidence with the US, thus ensuring a high level of protection for personal data in transfers between the EU and the US for law enforcement purposes, and appreciates the commitment to introduce sufficient safeguards. As the EDPS has long argued, the EU needs sustainable arrangements for sharing personal data with third countries for law enforcement purposes, which are fully compatible with the Charter of Fundamental Rights. Even when investigating domestic cases, law enforcement authorities increasingly find themselves in "cross-border situations" simply because a foreign service provider was used and the information is stored electronically in a third country. In practice, this often concerns service providers headquartered in the US due to their dominance on global markets. The growing volume of requests for electronic evidence 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 as the Council has to deliver its directives before the start of this delicate task. It builds on the case-law of the Court of Justice of the European Union in recent years, which 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.

Against this background, the EDPS wishes to make the following observations:

- he welcomes that the Recommendation already includes important data protection safeguards, including the need to make the Umbrella Agreement applicable by reference, and supports the need for certain additional safeguards as proposed by the Commission;
- given specific risks that arise in the context of direct cooperation between service providers and judicial authorities, he proposes to involve a judicial authority in the other party to the agreement;
- he recommends adding Article 16 TFEU as a substantive legal basis.

Additionally, the Opinion offers further recommendations for possible 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 future EU-US agreement.

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 natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[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] (hereinafter "the Recommendation"), 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)[8]. 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 the agreement on behalf of the EU. The latter recommendation is the subject of a separate EDPS Opinion[9]. However, the 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 and to start the negotiations with the US, along the negotiating directives annexed to the Recommendation. 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, as well as by the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. The EDPS also welcomes the reference to his Opinion in Recital 4 of the Recommendation. He wishes to underline that the present Opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information at a later stage.

2. OBJECTIVES OF THE AGREEMENT

5. The objective of the Commission initiative is to address the specific legal issue of access to content and non-content data held by service providers in the EU and in the US, by establishing common rules in an international agreement. In doing so, it would complement the e-evidence Proposal by addressing conflict of laws between the EU and the US and, as the largest service providers are headquartered in the US, increase the Proposal's effectiveness.

6. The US has concluded bilateral Mutual Legal Assistance Treaties (MLAT) for the exchange of evidence in criminal matters with the majority of EU Member States. The EU-US MLAT[10], which was signed in 2003 and entered into force in 2010, complements those bilateral agreements. The Commission considers that there is a need to develop alternative channels of cooperation between the EU and the US and to allow direct cooperation between judicial authorities and service providers in transatlantic relations.

7. Direct cooperation with US service providers already exists in practice to a certain extent. US law allows US based service providers to cooperate directly with public authorities of foreign countries[11]. This cooperation only concerns non-content data and is voluntary from the perspective of US law[12]. US companies have adopted their own policies to answer requests from foreign authorities or decide on a case-by-case basis; as a result, requests to US service providers are often not fulfilled[13] and this practice lacks legal certainty. The US Stored Communications Act prohibits the disclosure of content data to foreign authorities. Under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act[14], US service providers could potentially answer positively to requests for content data from authorities of qualifying foreign governments which concluded an executive agreement with the US[15].

8. According to the Commission, an EU-US agreement on cross-border access to electronic evidence would complement the e-evidence Proposal, which may give rise to conflicting obligations for service providers deriving for third countries' laws, and address the legal issues faced by law enforcement authorities when seeking access to both content and non-content data held by service providers in the EU or the US[16]. The envisaged agreement

would pursue the three main objectives laid down in paragraphs 1, 2 and 3 of the negotiating directives in the Annex:

1) set common rules and address conflict of laws for orders for obtaining electronic evidence in the form of content and non-content data from judicial authorities to service providers in a cross-border context, which would enhance legal certainty;
2) allow for transfers of electronic evidence between those actors when they directly cooperate;
3) ensure respect of fundamental rights, freedoms and general principles of EU law, including the rights to privacy and data protection.

3. MAIN RECOMMENDATIONS

9. The EDPS supports the efforts to identify innovative approaches to obtain cross-border access to electronic evidence. He supports the Commission's assessment that the EU *"has an interest in a comprehensive agreement with the US, both from the perspective of protecting European rights and values such as privacy and personal data protection, and from the perspective of our own security interests"*[17]. An international agreement between the EU and the US 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.

3.1. Standards regarding international data transfers and the respect of fundamental rights

10. The negotiating directives set out as second objective of the envisaged international agreement that it would *"allow for a transfer of electronic evidence directly on a reciprocal basis by a service provider to a requesting authority"*[18].

11. Pursuant to Article 216(2) TFEU, international agreements to which EU is a party, such as the envisaged agreement, "*are binding upon the institutions of the Union and on the Member States*". Moreover, according to the settled case law of the Court of Justice of the EU (CJEU), international agreements become from their entry into force "*an integral part of [the European legal order]*"[19].

12. The CJEU found, with respect to international agreements concluded by the EU, 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 which it is for the Court to review in the framework of the complete system of legal remedies established by the Treaty"*[20]. The subsequent analysis takes as starting point the requirement for international agreements to be compliant with the EU system for the protection of fundamental rights. The Charter of Fundamental Rights of the EU (the Charter) not only guarantees the respect for private and family life (Article 7), but it has also raised data protection to the level of a fundamental right under EU law (Article 8).

13. The applicable standards of EU law with regard to international agreement providing for transfers of personal data have been considered by the CJEU. In July 2017, the CJEU delivered Opinion 1/15[21] 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"*[22]. It follows from Opinion 1/15 that the level of protection resulting from the envisaged agreement with the US for the exchange of personal data between national competent authorities and service providers for law enforcement purposes 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.

14. In this context, attention is drawn to Article 35(1) of the Law Enforcement Directive[23] (LED) 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[24] and only if further specific conditions[25] 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[26]. The EDPS considers that the future EU-US agreement 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.

3.2. Legal basis of the Council Decision

15. The explanatory memorandum of the Recommendation states that "*The Council shall authorise the opening of negotiations, adopt negotiating directives and authorise the signing and conclusion of the agreement as set out in Article 218 (3) and (4) of the Treaty on the Functioning of the European Union*"[27]. Article 218 (3) and (4) TFEU is also referred to in the preamble to the draft Council Decision. However, the preamble does not refer to any substantive legal basis for this legal act.

16. In accordance with Article 296 (2) TFEU and the settled case law of the CJEU[28], 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.

17. **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 agreement, among which allowing the transfer of personal data and ensure respect for the fundamental rights enshrined in the Charter, including the rights to privacy and the protection of personal data. The envisaged agreement would thus relate directly to the objective pursued by Article 16 TFEU. 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"[29].

3.3. Safeguards of the Umbrella Agreement and additional safeguards

18. The negotiating directives in the Annex provide that *"The agreement should make applicable by reference the EU-U.S. Data Protection and Privacy Agreement, otherwise known as the "Umbrella Agreement""*[30]. The Umbrella Agreement[31] entered into force on 1 February 2017 and establishes a framework for the protection of personal data exchanged between the EU and the US for law enforcement purposes[32]. The Umbrella Agreement does not constitute a legal basis for transfers of personal data, and a proper legal basis for transfers to the US is always required. A legal basis for the transfer of personal data produced in answer to orders for electronic evidence is still required under EU law.

19. **The EDPS welcomes that the Umbrella Agreement, which he actively supported, should apply by reference and that this is included in the mandate**. At the same time, the EDPS recalls that, in his Opinion 1/2016 on the Umbrella Agreement[33], he recommended essential improvements and insisted on the need to reinforce several safeguards**. Since those issues have not been resolved in the final text of the Umbrella Agreement, the EDPS considers that the necessary improvements** (addressed in sections below[34]) **should be included in the negotiating directives themselves.**

20. As a rule, the Umbrella Agreement provides a **minimum level** of safeguards for transfers of personal data to the US for law enforcement purposes. While the envisaged agreement should not weaken those safeguards, it should increase the level of data protection, taking into account the specificities of the envisaged agreement and the risks involved for the rights and freedoms of data subjects. Therefore, the EDPS welcomes that paragraph 15 of the mandate envisages such additional safeguards and provides that *"The agreement should complement the Umbrella Agreement with additional safeguards that take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities"*.

21. In this respect, the EDPS recalls that, to meet the proportionality condition of Article 52(1) of the Charter, the advantages resulting from the measures should not be outweighed by the disadvantages those measure causes with respect to the exercise of fundamental rights[35]. They would have to strike a fair balance between the need to speed up the process to secure and obtain electronic evidence for the purposes of investigating, detecting or prosecuting criminal offences and the sound protection of personal data and other fundamental rights of the persons concerned. **The EDPS welcomes the attention already paid to privacy and data protection throughout the negotiating directives included in the Annex, and supports the statement that the envisaged agreement "*should be conditional on strong protection mechanisms for fundamental rights*"[36].** He notes that paragraphs 16 and 17 of the negotiating directives provide a non-exhaustive list of additional safeguards to include in the agreement. **He recommends replacing the words "*inter alia*" in both paragraphs 16 and 17 by "at the very least" to better convey that these safeguards are indispensable.**

22. **Moreover, given the impact of the envisaged agreement on fundamental rights, the EDPS considers that certain further safeguards than those envisaged in the negotiating**

directives (that he will address individually in sections below[37]) **should be included to ensure that the final agreement meets the proportionality requirement.**

23. Finally, the EDPS recalls that **all safeguards provided in the envisaged agreement should not only be clear but also effective in order to fully comply with EU primary law and be in line with Opinion 1/15 of the CJEU[38].**

3.4. Involvement of judicial authorities of the other Party to the agreement

24. The negotiating directives clearly give instructions[39] to establish a model of direct cooperation between judicial authorities and service providers, which is similar to the model proposed by the e-evidence Proposal, with the important difference that it envisages such direct cooperation between authorities of a third country - the US - and service providers in the EU (and *vice versa*). The EDPS notes that those directives do not refer to any systematic involvement of competent judicial authorities of the other party when orders would be issued. Paragraph 16(c) provides *"that use by and disclosure to other U.S. authorities not bound by the Umbrella Agreement is subject to notification to, and prior authorisation by the competent judicial authority designated in the Member State in which the service provider is established or represented"*. It is unclear whether this requirement of prior notification and authorisation relates to all orders issued by US competent authorities not bound by the Umbrella Agreement, or whether it relates to the communication of data by US authorities bound by the Umbrella Agreement to other US authorities not bound by it. **The EDPS recommends clarifying paragraph 16(c)**.

25. In the traditional approach to cross-border access to electronic evidence, it is primarily the responsibility of the enforcing State to ensure the review of limited grounds of refusal. While, as stated above, 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 EU Member States and in the US - *inter alia* on the admissibility of evidence gathered in another country and what constitutes a criminal offence - may diverge.

26. 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. Yet, 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[40]. EU Member States have the legal obligation to respect fundamental rights when implementing EU law[41]. In this regard, in the context of the EIO Directive 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*"[42].

27. The EDPS points out that the Council adopted a general approach[43] on the e-evidence Proposal in December 2018, which introduces a notification to the competent authorities of the executing Member States for orders to produce content data. This notification must take place at the same time as orders are sent to service providers and gives the possibility to the notified authorities to raise certain issues. Several Member States requested further involvement of the Member State where the service provider is located, beyond the

notification introduced in the general approach and covering also non-content data[44]. In addition, the European Data Protection Board (EDPB), which issued an Opinion on the e-evidence Proposal, found no justification for addressing orders to service providers to produce content data *"without any involvement at least of the competent authorities of the Member State where the data subject is"*[45].

28. Also, even in the EU context, 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*"[46]. 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. He therefore recommends including as specific safeguard in the negotiating directives the obligation for EU and US competent authorities to systematically involve judicial authorities designated by the other Party 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.** From an EU perspective, such involvement of EU judicial authorities would also be more in line with Article 82(1) TFEU (if this legal basis is included as one of the substantial legal basis of the Council Decision).

4. ADDITIONAL RECOMMENDATIONS

29. 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 the envisaged agreement with the US should satisfactorily address and mitigate these risks.

4.1. Mandatory nature of the agreement

30. The negotiating directives specify that the envisaged agreement should *"take precedence over the Council of Europe Convention on Cybercrime and any agreement or arrangement reached in the negotiations of the Second Additional Protocol"*. However, they do not specify whether the CLOUD Act - which has a clear extraterritorial reach - could still be used by US law enforcement authorities to serve warrants ordering the disclosure of data on EU companies, if an EU-US agreement on cross-border access to e-evidence is concluded.

31. The explanatory memorandum states that *"it is in the interest of both the European Union and United States of America to conclude a comprehensive agreement as this would provide legal clarity for judicial and law enforcement authorities from both sides and avoid conflicting legal obligations for service providers"*[47]. **To effectively achieve these objectives, the EDPS recommends clarifying in the negotiating directives the mandatory[48] nature of the envisaged agreement in bilateral relations between the EU and the US**.

32. In addition, treaties and executive agreements concluded by the US might not be self-executing as implementing legislation is required to make their provisions enforceable in the US. Therefore, **the EDPS recommends clarifying that the envisaged agreement should be self-executing from the perspective of US law**.

4.2. Onward transfers

33. Paragraph 16(d) of the negotiating directives provides that *"onward transfers to other third countries may only be made to law enforcement authorities (...) and should be subject to notification to, and prior authorisation by the competent judicial authority designated by the Member State in which the service provider is established or represented"*. The EDPS welcomes these requirements for onward transfers that are similar to those of Article 35 of the LED[49]. However, **the EDPS considers that as an additional requirement for onward transfers the second receiving competent authority in the other third country should provide an adequate level of protection**.

34. The EDPS points out that the CJEU held in Opinion 1/15 of July 2017 in relation to such onward transfers that the same requirement 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"* [50]. 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"*. Therefore, **the EDPS recommends including this additional requirement in paragraph 16(d) of the negotiating directives**.

4.3. Rights of data subjects

35. The EDPS takes note of the fact that the Annex does not include any specific directive regarding data subject rights. The EDPS first recalls that 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. If the exercise of data subjects' rights are usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations, the possibility for data subjects to exercise their rights should exist in practice and not remain purely theoretical, even if limited or performed by a trusted third party in situations where the exercise of these rights is denied to protect sensitive law enforcement information.

36. The Umbrella Agreement includes provisions on the right to be informed (Article 20), the right of access (Article 16), the right to rectification - which also refers to erasure and blocking (Article 17) and the right not to be subject to automated decisions (Article 15). **As raised in his Opinion on the Umbrella Agreement[51], the EDPS considers that exemptions provided in the Umbrella Agreement regarding the exercise of the right to information and the right of access are so considerable that they might not allow the exercise of those rights.**

37. As regard the right of access, the EDPS considers that the envisaged agreement should make sure that the possibility for data subjects to have access to their own data *de facto* exist, even if limited or performed by a trusted third party.

38. As regard the right to information, the EDPS notes that paragraph 17(e) of the negotiating directives provides that *"The confidentiality safeguards for authorities and service providers, including non-disclosure requirements"*. The right to information is of utmost importance as it allows the exercise of other data protection rights, including the right to

remedies, and ensures fair processing of the data[52]. Data subjects usually have no knowledge of the fact that their data are processed (or transferred) for law enforcement purposes. The EDPS recalls that the CJEU found in Opinion 1/15 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"*[53].

39. 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 agreement increase their efforts to 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

40. 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.

41. Article 21 of the Umbrella Agreement obliges the US to have in place one or more public oversight authorities which must *"exercise independent oversight functions and powers"*. The US must provide for oversight through more than one authority, which may notably include *"inspectors general, chief privacy officers, government accountability offices, privacy and civil liberties oversight boards, and other applicable executive and legislative privacy or civil liberties review bodies"*. The EDPS recalls that, pursuant to the CJEU case law[54], 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"*[55].

42. **The EDPS recommends clearly identifying the specific authority or authorities entrusted by the US with the independent oversight of compliance with the rules of the envisaged agreement in the agreement**. 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 agreement should also be specified.

4.5. Judicial redress and administrative remedies

43. The EDPS welcomes that the mandate provides that *"The agreement should include a clause enabling effective judicial remedies for data subjects during criminal proceedings"*[56].

44. The EDPS recalls that the CJEU found[57] 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 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*"[58].

45. Also, the CJEU has stressed that it is essential for individuals to be able to file complaints with independent supervisory authorities[59] and seek, therefore, administrative redress.

46. The Umbrella Agreement includes two provisions - Articles 18 and 19 - on administrative and judicial redress. As raised in his Opinion on the Umbrella Agreement[60], the EDPS still has serious concerns about the compliance of Article 19 with the Charter. He is aware that the US passed the Judicial Redress Act[61] in February 2016, which extends certain rights of judicial redress established under the US Privacy Act to citizens of designated countries. However, he needs further information regarding the **effective nature** of those legal remedies, which is also a requirement of Article 47 of the Charter, based on a review of the way this Agreement is implemented in the US law and complied with in practice.

47. Therefore, **the EDPS recommends including in the mandate that the envisaged agreement should ensure that both redresses are available to all data subjects**.

4.6. Categories of data subjects concerned

48. The negotiating directives provide that *"The agreement should be reciprocal in terms of the categories of persons whose data must not be requested pursuant to this agreement"*[62].

49. The EDPS notes that the CLOUD Act refers to so-called "US persons" and makes distinctions on this basis. For instance, it does not allow foreign service providers to object to orders from US law enforcement authorities on the basis of a conflict of law when the person whose data are sought is a "US person"[63].

50. The EDPS recalls that the protection afforded by Articles 7 and 8 of the Charter, according to which the fundamental rights to privacy and personal data protection applies to "everyone" in the EU, irrespective of the nationality or status. Similarly the GDPR does not distinguish based on nationality or status and ensures the same level of protection to personal data of both EU citizens or residents and non-EU citizens or residents. Therefore, the EDPS considers that any distinction in the envisaged agreement regarding the level of data protection and safeguards ensured for the processing of personal data falling within the scope of the GDPR due to the US nationality or the residence in the US of the data subject would be unacceptable. **The EDPS recommends making clear in the negotiating directives that the same level of data protection and similar safeguards should be ensured for all data subjects whose data will be processed based on the agreement.**

4.7. Definition and types of data

51. The negotiating directives provide that *"The agreement should set out the definitions and types of data that are to be covered, including both content and non-content data"*[64]. The EDPS welcomes that the envisaged agreement should provide definitions of data categories which would be covered. He considers that the sole distinction between content data and non-content data may not be sufficient as both types of data could be as sensitive.

52. In this respect, the EDPS first recalls that the CJEU found that access to content data may adversely affect the essence of the right to privacy[65].

53. In relation to non-content data, the CJEU found as regards 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"*[66] 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"*[67].

54. **The EDPS stresses the importance of laying down clear and straightforward definitions of data categories in the envisaged agreement in order to ensure legal certainty** for all stakeholders involved in the EU and the US - which is part of the first objective set out in paragraph 1 of the mandate. The effectiveness of orders to obtain electronic evidence could easily be undermined by the lack of precision and clarity of the core definitions of the envisaged agreement. To the extent the definitions of data categories in the e-evidence Proposal will be used as reference, as previously raised by the EDPB[68], **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 agreement.

4.8. Criminal offences covered by the agreement

55. The EDPS welcomes that the negotiating directives provide that *"The agreement should define its exact scope of application in terms of the criminal offences covered and the thresholds"*[69]. Paragraph 17(b) further specify that the agreement should provide *"adequate conditions to ensure necessity and proportionality of orders for access to electronic evidence, distinguishing in particular between the data categories as appropriate"*[70].

56. 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 paragraph 17(b) of the negotiating directives that distinctions should also be made based on the seriousness of the offences concerned**.

57. The EDPS recalls that, according to the CJEU case law, only the objective of fighting serious crime is capable of justifying the access by public authorities to personal data retained by service providers *"which, taken as a whole, allow precise conclusions to be drawn*

concerning the private lives of the persons whose data is concerned"[71]. Where such conclusions cannot be drawn and therefore the interference is not deemed serious, the Court further held that *"access to such data (...) is therefore 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'"*[72]. Thus, under the envisaged agreement, 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.

4.9. Information security

58. Article 9 of the Umbrella Agreement obliges the EU and the US to *"have in place appropriate technical, security and organisational arrangements for the protection of personal information"*. The negotiating directives envisages *"safeguards that take into account [...] the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities"*[73]. Among those specific safeguards, paragraph 16(f) provides that *"The notification of an information security incident to the competent authority designated by the Member State in which the service provider is established or represented shall be made under the conditions of Article 10(2) of the Umbrella Agreement"*.

59. Given the model of direct cooperation between service providers and judicial authorities on different sides of the Atlantic, the EPDS considers that the envisaged agreement raises important questions regarding the security of cross-border incoming and outgoing transmission of personal data related to the execution of orders for electronic evidence. The EDPS wishes to stress that ensuring the security of personal data is not only a clear requirement under EU law[74], 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.

60. Therefore, **the EDPS recommends including further safeguards in the mandate in order to ensure an appropriate level of security for the personal data produced and transferred. In addition to paragraph 16(f), 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**.

4.10. Authorities competent to issue orders

61. The EDPS considers that the envisaged agreement should clearly identify the authorities of both parties which would be competent to issue orders addressed directly to service providers. The EDPS notes that this is not specifically addressed in the negotiating directives. Therefore, **he recommends including in the mandate that the agreement should identify which authorities may issue orders for electronic evidence**.

62. The EDPS stresses that compliance with the purpose limitation principle is closely linked to the scope of competence of recipients in the receiving third country. To ensure respect of the purpose limitation principle, the scope of competence of the specific authorities in the US 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 agreement be**

accompanied by an exhaustive list of the competent authorities in the US to which data could be transferred as well as a short description of their competences. This should also be reflected in one of the directives of the Annex.

4.11. Possibility for service providers to object

63. Service providers receiving an order for electronic evidence addressed by US judicial authorities may find themselves caught between conflicting legal obligations under EU law and US law. The EDPS welcomes paragraph 9 of the negotiating directives which provides that *"The agreement should also define in which circumstances a service provider has the right to object to an order"*.

64. In this regard, the EDPS notes that the US CLOUD Act allows foreign service providers to object to orders from US law enforcement authorities on the basis of a conflict of law only in limited cases. It allows them to file a so-called "motion to quash" in front of US courts on the cumulative conditions that the subscriber or customer whose data are sought is not a US person and does not reside in the US, and that the order raises a conflict of laws with a qualifying foreign government[75].

65. **The EDPS considers that service providers served with an order for electronic evidence should be able to object to an order on specific grounds defined in the envisaged agreement, such as missing or incorrect information or fundamental rights considerations[76].** 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, instead of defining "in which circumstances", **the EDPS recommends specifying in the negotiating directives that the agreement should also define "the specific grounds that a service provider may raise to object to an order".**

5. CONCLUSIONS

66. The EDPS understands the need for law enforcement authorities to secure and obtain electronic evidence quickly and effectively. He supports the efforts to identify innovative approaches to obtain cross-border access to electronic evidence. 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 negotiate with the US.

67. The EDPS agrees with the Commission's statement that the envisaged agreement should be conditional on strong protection mechanisms for fundamental rights. Several data protection principles and safeguards are already envisaged in the negotiating directives. He first recommends to include Article 16 TFEU as one of the substantive legal basis in the preamble of the Council Decision. He welcomes that the Umbrella Agreement, which he actively supported, should apply by reference to the future agreement. In his Opinion 1/2016 on the Umbrella Agreement, the EDPS recommended essential improvements and the reinforcement of several safeguards; he recommends to include those safeguards in the negotiating directives.

68. Given the impact of the envisaged agreement on fundamental rights, the EDPS also considers that further safeguards than those already envisaged should be included to ensure that the final agreement meets the proportionality condition. He notably recommends the involvement of judicial authorities designated by the other Party to the agreement as early

as possible in the process of gathering electronic evidence so that these authorities would have the possibility to review compliance of the orders with fundamental rights and raise grounds for refusal.

69. In addition to these general recommendations, the recommendations and comments of the EDPS in the present Opinion relate to the following specific aspects of the envisaged agreements to be negotiated with the US in the negotiating directives:

- the mandatory nature of the agreement;
- the onward transfers by US competent authorities;
- the rights of data subjects in the US, in particular the right to information and the right of access;
- the control by and independent authority in the US;
- the judicial redress and administrative redress in the US;
- the categories of data subjects concerned;
- the definition and types of data covered by the envisaged agreement;
- the criminal offences covered by the envisaged agreement;
- the specific safeguards to ensure an appropriate level of security of the data transferred;
- the type of authorities that can issue orders for electronic evidence;
- the possibility for service providers served with an order for electronic evidence to object based on specific grounds.

70. 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 on the text of the draft agreement 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 "Law Enforcement Directive").
[44] 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; Convention on enhanced international cooperation on cybercrime and electronic evidence, Budapest, 23 November 2001, CETS No. 185.
[9] EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.
[10] Agreement of 25 June 2003 on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, p. 34.
[11] Recent rulings and court cases in the US sought to clarify whether US authorities could order the production of data stored abroad by service providers which fall under US jurisdiction. Among those cases, the famous Microsoft Ireland Case reached the US Supreme Court after Microsoft refused to execute a US warrant to disclose data stored on its servers in Ireland and challenged the application of the US Stored Communication Act. On 23 March 2018, the US passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act. On the one hand, the CLOUD Act amends the Stored Communication Act and clarifies US law enforcement authorities' powers to order the production of data apply "regardless of whether such communication, record, or other information is located within or outside of the United States". Thus, it confirmed that the power of US law enforcement authorities to serve warrants ordering the disclosure of data has extraterritorial reach and rendered the Microsoft Ireland Case moot. It also enacts into US law a practice of US law enforcement authorities to bypass Mutual Legal Assistance Treaties in criminal matters (MLATs) currently in place between the US and foreign countries, including the MLAT in force between the EU and the US. On the other hand, the CLOUD Act provides the possibility for the US to conclude "executive agreements" with "qualifying foreign governments", which would allow law enforcement authorities of those third countries to directly request access to data in the US, including content data, under certain conditions.
[12] See Title 18 USC, § 2702.
[13] Commission Staff Working Document: Impact Assessment, SWD(2018) 118 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN.
[14] Available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.
[15] See Title 18 USC, §§2511, 2523 and 2702.
[16] Explanatory memorandum of the Recommendation, p. 4-5.
[17] Explanatory memorandum of the Recommendation, p. 4.
[18] Paragraph 2 of the negotiating directives.
[19] CJEU, Case 181/73, R. & V. Haegeman v. Belgian State, ECLI:EU:C:1974:41, par. 5.
[20] CJEU, Joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461, par. 285. [Emphasis added].
[21] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.
[22] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 214; see also par. 93 of Opinion 1/15.
[23] 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.

[24] 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.

[25] 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".

[26] See also EDPB 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"), p. 9, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.

[27] Explanatory memorandum of the Recommendation, p 7.

[28] CJEU, Case C-687/15, European Commission v Council of the EU, ECLI:EU:C:2017:803, par. 48 and following.

[29] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 232.

[30] Paragraph 14 of the negotiating directives.

[31] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 10.12.2016, p. 3 (hereinafter "the Umbrella Agreement").

[32] It mainly applies to personal data transfers between EU and US law enforcement authorities. It may also apply to personal data "otherwise transferred in accordance with an agreement concluded between the United States and the [EU] or its Member States" for law enforcement purposes (Article 3(1)). Thus, the Umbrella Agreement can also cover transfers of personal data from relevant private companies where they are based on international agreements between the EU and the US, such as transfers by service providers under the envisaged agreement on cross-border access to electronic evidence.

[33] EDPS Opinion 1/2016 of 12 February 2016 on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences (hereinafter "EDPS Opinion 1/2016"), available at: https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf.

[34] See sections 4.3., 4.4., 4.5. below.

[35] The EDPS is working on guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. A draft version of those guidelines were recently submitted to stakeholders' consultation before the publication of the final version. They are available at: https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[36] Explanatory memorandum of the Recommendation, p 5.

[37] See sections 3.4., 4.2., 4.9., 4.11. below.

[38] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, specifically par. 134, where the Court found that *"[e]ven though the means intended to ensure such a level of protection may differ from those employed within the European Union [...], those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union"*.

[39] Paragraph 1 of the negotiating directives.

[40] 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).

[41] See Articles 6 TUE and 67(1) TFUE. See also Fundamental Rights Agency Opinion of 14 February 2011 on the draft Directive regarding the European Investigation Order, 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".

[42] See Fundamental Rights Agency Opinion of 14 February 2011 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.

[43] Available at: http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf.

[44] 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".*

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

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

[47] See explanatory memorandum of the Recommendation, p. 8.

[48] 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; and judgment of United States Supreme Court in Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, 482 US 522, 535, 548 (1987).

[49] Article 35(1)(b) provides that the onward transfer occurs between authorities responsible for the prevention, investigation, detection and prosecution of criminal offences. Article 35(1)(e) provides the principle of prior authorisation of the sending Member State.

[50] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 214.

[51] EDPS Opinion 1/2016, § 39 and 41.

[52] CJEU, Case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală, ECLI:EU:C:2015:638, in particular par. 32 and 33 where the Court found that *"the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, and their right to object to the processing of those data"* and that *"That information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data"*.

[53] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 220. [Emphasis added].

[54] See CJEU, Case C-518/07, Commission v Germany, ECLI:EU:C:2010:125, par. 25; CJEU, Case C-614/10, Commission v Austria, ECLI:EU:C:2012:631, par. 36-37; CJEU, Case C-288/12, Commission v Hungary, par. 48; CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 41.

[55] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 230.

[56] See paragraph 9 of the negotiating directives.

[57] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95.

[58] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 95. [Emphasis added].

[59] CJEU, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, par. 56-58.

[60] EDPS Opinion 1/2016, par. 46.

[61] Available at: https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

[62] Paragraph 13 of the negotiating directives.

[63] See Title 18 USC, § 2703.

[64] See paragraph 6 of the negotiating directives.

[65] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 39.

[66] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 27.

[67] CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson, ECLI:EU:C:2016:970, par. 99.

[68] See EDPB Opinion 23/2018, 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"*.

[69] See paragraph 7 of the negotiating directives.

[70] See paragraph 17(b) of the negotiating directives.

[71] CJEU, Case C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, par. 54, see also par. 56.

[72] CJEU, Case C-207/16, Ministerio fiscal, ECLI:EU:C:2018:788, par. 62. [Emphasis added].

[73] See paragraph 15 of the negotiating directives.

[74] 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) of the Law Enforcement Directive). The security of the processing covers in particular the ability to ensure the ongoing confidentiality and integrity of processing systems.

[75] See Title 18 USC, § 2703.

[76] 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"*.