Council of the
European Union

Brussels, 8 November 2019
(OR. en)

13908/19

COPEN 427
JAI 1163
CYBER 305
DROIPEN 178
JAIEX 166
ENFOPOL 489
TELECOM 348
DAPIX 329
EJUSTICE 142
MI 775
CODEC 1594

COVER NOTE

From:	Mr Wojciech Rafal WIEWIOROWSKI, Assistant Supervisor of EDPS
date of receipt:	8 November 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
Subject:	EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters

Delegations will find enclosed the European Data Protection Supervisor Opinion on the above mentioned Proposals.

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

President of the Council of
the European Union
General Secretariat
Council of the European Union
Rue de la Loi 175
1048 Brussels

Brussels, 06 NOV. 2019
WRW/LS/mt/D(2019)2316 **C2017-1128**
Please use edps@edps.europa.eu for all correspondence

Subject: Opinion of the European Data Protection Supervisor on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters

Dear Mr President,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC and in particular article 58(3)(c) we send you an Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.

We have sent this opinion to the President of the European Commission and the President of the European Parliament as well.

Yours sincerely,

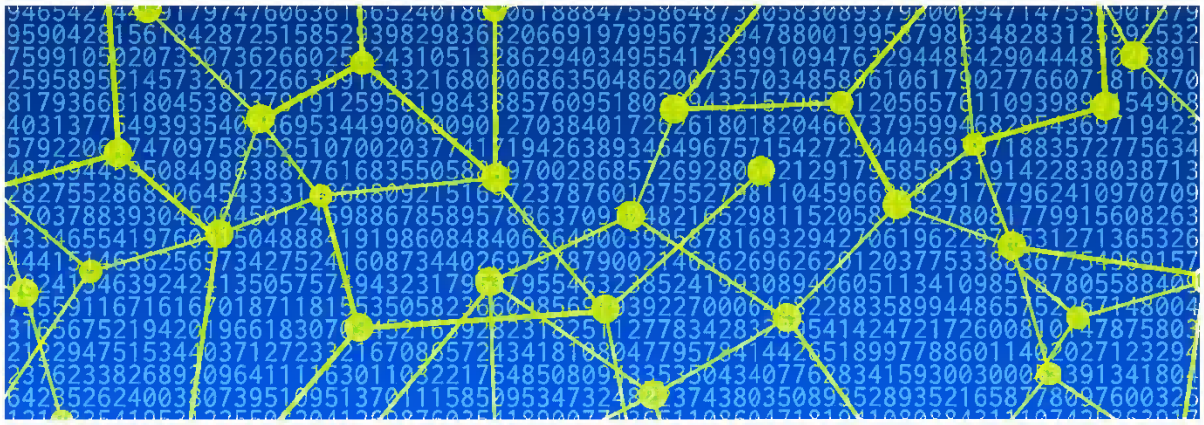
Wojciech Rafał WIEWIÓROWSKI

Encl.: Opinion

Cc: Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General
Ms Marja RISLAKKI, Permanent Representative of Finland
Mr Ralph KAESSNER, Secretariat General of the Council

Contact persons: *Lara Smit (tel: 02 2831966), Claire-Agnes Marnier (tel: 02 2831952)*

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



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2019

EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters

EDPS

6 November 2019

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under article 58(3)(c) of Regulation 2018/1725, the EDPS shall have the power 'to issue on his or her own initiative or on request, opinions to Union institutions and bodies and to the public on any issue related to the protection of personal data'. He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and to foster accountable policymaking in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS supports the objective of making cross-border access to electronic evidence more efficient but stresses the need to improve the legislative Proposals presented by the Commission to ensure respect for fundamental rights and compliance with data protection requirements. Both are key to establishing a functioning framework for the European Production and Preservation Orders to gather electronic evidence in criminal matters.

Executive Summary

In April 2018, the Commission tabled two Proposals - for one Regulation and one Directive - to establish a legal framework that would make it easier and faster for police and judicial authorities to secure and obtain access to electronic evidence in cross-border cases. Since then, the Council has adopted general approaches on the Proposals and the European Parliament issued several working documents. The European Data Protection Board issued its opinion. Related developments have taken place at international level, most notably with the launch of negotiations of an international agreement with the United States on cross-border access to e-evidence as well as work on a Second Additional Protocol to the Cybercrime Convention. With the present opinion, the EDPS wishes to provide the EU legislator with new input for the forthcoming work on the Proposals, taking into account the developments listed above.

In today's world transformed by new technologies, time is often of the essence to enable those authorities to obtain data indispensable to carry out their missions. At the same time, 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 another Member State. The EDPS **supports the objective** of ensuring that effective tools are available to law enforcement authorities to investigate and prosecute criminal offences, and in particular welcomes the objective of the Proposals to accelerate and facilitate access to data in cross-border cases by streamlining procedures within the EU.

At the same time, the EDPS wishes to underline that any initiative in this field must be **fully respectful of the Charter of Fundamental Rights of the EU and the EU data protection framework** and it is essential to ensure **the existence of all necessary safeguards**. In particular, effective protection of fundamental rights in the process of gathering electronic evidence cross-border requires **greater involvement of judicial authorities in the enforcing Member State**. They should be systematically involved as early as possible in this process, have the possibility to review compliance of orders with the Charter and have the obligation to raise grounds for refusal on that basis.

In addition, the **definitions of data categories** in the proposed Regulation should be clarified and their consistency with other definitions of data categories in EU law should be ensured. He also recommends reassessing the balance between the **types of offences** for which European Production Orders could be issued and the **categories of data** concerned in view of the relevant case law of the Court of Justice of the EU.

Furthermore, the EDPS makes specific recommendations on several aspects of the e-evidence Proposals that require improvements: the **authenticity and confidentiality of orders and data transmitted**, the **limited preservation** under European Preservation Orders**,** the **data protection framework applicable**, the **rights of data subjects**, data subjects benefiting from **immunities and privileges**, the **legal representatives**, the **time limits** to comply with European Production Orders and the **possibility for service providers** to object to orders.

Finally, the EDPS asks for more clarity on the interaction of the proposed Regulation with future international agreements. The proposed Regulation should maintain the high level of data protection in the EU and become a reference when negotiating international agreements on cross-border access to electronic evidence.

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND 7

2. AIMS OF THE PROPOSALS 9

3. MAIN RECOMMENDATIONS 10

3.1. CLEAR DEFINITIONS OF THE CATEGORIES OF PERSONAL DATA 10

3.2. THE TYPE OF OFFENCES CONCERNED 12

3.3. DATA SECURITY 14

3.4. GREATER INVOLVEMENT OF JUDICIAL AUTHORITIES IN THE ENFORCING MEMBER STATE 15

3.5. LIMITED PRESERVATION UNDER EUROPEAN PRESERVATION ORDERS 17

4. ADDITIONAL RECOMMENDATIONS 18

4.1. COMPLETE REFERENCE TO APPLICABLE DATA PROTECTION FRAMEWORK 18

4.2. RIGHTS OF THE DATA SUBJECTS 18

4.3. DATA SUBJECTS BENEFITING FROM IMMUNITIES AND PRIVILEGES 19

4.4. LEGAL REPRESENTATIVES 20

4.5. TIME LIMITS TO PRODUCE DATA 20

4.6. POSSIBILITY FOR SERVICE PROVIDERS TO OBJECT 21

4.7. INTERACTION WITH OTHER INSTRUMENTS 21

5. CONCLUSIONS 22

NOTES 25

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) 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[i], and in particular, Articles 42(1), 57(1)(g) and 58(3)(c) 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)[ii],

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[iii],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. On 17 April 2018, the Commission released two legislative Proposals (hereinafter "the Proposals"), accompanied by an Impact Assessment[iv], including:
   - a Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[v] (hereinafter "the proposed Regulation");
   - a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[vi] (hereinafter "the proposed Directive").

2. The proposed Regulation would co-exist with Directive 2014/41/EU regarding the European Investigation Order in criminal matters (hereinafter "EIO Directive")[vii], which aims at easing the process of gathering evidence in the territory of another Member State and covers every type of evidence gathering, including electronic data[viii]. All Member States which took part in the adoption of the EIO Directive[ix] had until May 2017 to implement it in their national legislation[x].

3. On 26 September 2018, the European Data Protection Board[xi] (hereinafter "EDPB") adopted an opinion[xii] on the Proposals.

4. On 7 December 2018 and 8 March 2019, the Council adopted its general approach on the proposed Regulation[xiii] and the proposed Directive[xiv] respectively. The European Parliament published a series of working documents.

5. The European Data Protection Supervisor (hereinafter "EDPS") welcomes that he has been consulted informally by the Commission services before the adoption of the Proposals. The EDPS also welcomes the references to the present Opinion in Recital 66 of the proposed Regulation and Recital 24 of the proposed Directive.

6. 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[xv] 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 "Convention on Cybercrime")[xvi]. The two recommendations were the subject of two EDPS Opinions[xvii]. Both negotiations with the US and at the Council of Europe are closely linked.

7. In February 2019, the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament addressed similar letters to the EDPS and the EDPB to request a legal assessment of the impact of the US CLOUD Act[xviii] that was passed by the US Congress in March 2018, on the European legal framework for data protection. On 12 July 2019, the EDPS and the EDPB adopted a Joint Response to this request with their initial assessment[xix].

8. On 3 October 2019, the United Kingdom and the United States signed a bilateral agreement on cross-border access to e-evidence for the purpose of countering serious crime[xx]. It is the first executive agreement allowing US service providers to comply with requests for content data from a foreign country under the US CLOUD Act.

9. This Opinion covers both Proposals, with however a main focus on the proposed Regulation. In line with the EDPS mission, it is primarily focussed on the rights to privacy and to the protection of personal data and aims to be consistent and complementary to the EDPB Opinion 23/2018, also considering the general approaches of the Council and the working documents of the European Parliament.

2. AIMS OF THE PROPOSALS

10. The overarching objective of the proposed Regulation is to speed up the process of securing and obtaining electronic evidence across borders[xxi]. To this end, it would introduce two new types of binding orders: the European Production Order (hereinafter "EPO") for the production of data by a service provider and the European Preservation Order (hereinafter "EPO-PR") for the preservation of data in view of subsequent requests to produce these data, which may be used as evidence in criminal proceedings.

11. The proposed measures would entail the processing of personal data and limitations on both the right to privacy guaranteed by Article 7[xxii] of the Charter and the right to protection of personal data guaranteed by Article 8[xxiii] of the Charter. To be lawful, such limitations on the exercise of fundamental rights protected by the Charter must comply with the conditions laid down in its Article 52(1). This includes ensuring that any limitation on the right to personal data protection is "necessary" and "proportionate". In order to assist the EU legislator in assessing compliance of proposed legislative measures involving the processing of personal data, the EDPS published a "Necessity Toolkit"[xxiv] based on relevant case law and his previous opinions.
12. Under the proposed Regulation, the orders would be issued only in cross-border situations[xxv] and not in domestic ones[xxvi]. Production orders would only be issued or validated by a judicial authority of a Member State if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State. The orders would be directly addressed by the issuing authority to service providers offering services in the European Union (hereinafter "EU")[xxvii] and established or represented via a legal representative in another Member State. They would be transmitted to service providers through European Production Order Certificates (hereinafter "EPOC") or European Preservation Order Certificates (hereinafter "EPOC-PR"). The orders would be directly executed in the enforcing Member State, without a prior procedure for recognition and enforcement in this Member State. However, under certain conditions, limited grounds could be raised in the enforcing Member State to oppose the recognition or enforcement of the orders (Article 14) or to request in the issuing Member State the review of an EPO (Articles 15 and 16).

13. The proposed Directive aims at providing a common EU solution to identify the addressees of EPOC and EPOC-PR[xxviii]. To this end, it introduces an obligation for all service providers offering services in the EU to designate a legal representative in the EU[xxix], which would be responsible for the reception of EPOC and EPOC-PR and their timely and complete execution[xxx].

14. In light of the challenges faced by police and judicial authorities to gather electronic evidence in today's digital world which knows no borders, **the EDPS supports the objective of providing effective tools to law enforcement authorities to quickly obtain access to electronic evidence across borders. In many cases, time is of the essence to enable those authorities to obtain data that are indispensable for their investigations and prosecutions.** 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 another Member State. Therefore, **the EDPS welcomes the objective of the e-evidence proposals to accelerate and facilitate such access in cross-border cases and to increase legal certainty by streamlining procedures within the EU.** At the same time, **he insists on the need to ensure that the preservation of and access to electronic evidence are fully respectful of the Charter of Fundamental Rights of the EU (hereinafter "Charter") and the data protection framework**.

15. The EDPS notes that the Impact Assessment accompanying the Proposals envisages the right to liberty and security enshrined in Article 6 of the Charter as *"the fundamental rights of persons who are or may become victims of crime"*[xxxi]. The EDPS underlines that this right is intended to protect individual liberty and security against the State, not to guarantee it through the State[xxxii].

16. In order to comply with conditions of Article 52(1), the EDPS recalls that the CJEU found that the EU legislator should "*lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data*"[xxxiii]. The Proposals constitute the latest instalment of a series of legislative measures in which the EU legislator is called to balance data protection rights of individuals against public interest in combating and prosecuting criminal offences. Such measures are obviously liable to conflict with data protection rights[xxxiv]. **It is therefore essential to closely scrutinise these Proposals and pay particular attention to the existence of all necessary safeguards.**

3. MAIN RECOMMENDATIONS

3.1. Clear definitions of the categories of personal data

17. Electronic evidence is defined in Article 2(6) of the proposed Regulation and is divided in four sub-categories of "subscriber data", "access data", "transactional data" and "content data" defined in Article 2(7), (8), (9) and (10), respectively. This division focus on the "sensitivity"[xxxv] of each data category and, on this basis, provides for different requirements[xxxvi] for accessing data falling under these categories.

3.1.1. Consistent definitions of data categories in EU law

18. The EDPS stresses the importance of ensuring consistency between definitions of data categories in the proposed Regulation and other definitions of data categories in EU law. In this regard, the EDPS notes that the proposed Regulation takes into account the definitions proposed in the context of the draft ePrivacy Regulation, which would define electronic communications data[xxxvii] and distinguish between the two categories of electronic communications content data[xxxviii] and electronic communications metadata[xxxix].

19. While the category of content data in the proposed Regulation seems consistent with the one of electronic communications content data in the proposed ePrivacy Regulation, the categories of **transactional data and access data in the proposed Regulation are new data categories**. They are not currently defined in EU data protection law and they both include - but are not limited to - electronic communications metadata as defined by the proposed ePrivacy Regulation. The future ePrivacy Regulation would apply to the preservation and production of data of electronic communications service providers under the proposed Regulation on e-evidence. **The EDPS considers that it is therefore essential to ensure full consistency between the definitions of these two texts throughout the legislative process. The EDPS recalls that he has repeatedly called for a swift adoption of the ePrivacy Regulation to avoid legal uncertainty[xl].**

3.1.2. Lack of clarity and overlap of data categories

20. The EDPS stresses the importance of laying down clear and straightforward definitions of each data category in order to ensure legal certainty for all stakeholders involved - which is one of the main objectives of the proposed Regulation[xli]. The effectiveness of the orders could easily be undermined by the lack of precision and clarity of the core definitions in the proposed Regulation.

21. The proposed Regulation would introduce a new category of "access data" defined as "*data related to the commencement and termination of a user access session to a service*". Article 2(8) also defines access data in relation to the purpose for processing such data, *i.e.* they are "*strictly necessary for the sole purpose of identifying the user of the service*". It further specifies that they also include electronic communications metadata. The Explanatory Memorandum explains that it is essential to cover this category of access data since it often constitutes, with subscriber data, "*the starting point to obtain leads in an investigation about the identity of a suspect*"[xlii]. However, the EDPS observes that this new category of data is not consistent with existing definitions of data categories in EU law and Member States' law[xliii]. The creation of this data category seems artificial and to have as only objective to attach lower requirements to the production of such data, similar to those attached to the production of subscriber data (Article 4(1)). Therefore, **the EDPS recommends to reconsider the need for introducing this new data category of access data.**

22. Alternatively, should the category of access data remains in text, the EDPS considers, as already raised by the EDPB[xliv], that the proposed definition of access data lacks clarity. The EDPS notes that both definitions of transactional data and access data include "electronic communications metadata" as defined by the proposed ePrivacy Regulation. They both list a number of data falling in their category as examples. Some examples are explicitly covered by both definitions, such as the date and time. In addition, the definition of transactional data excludes data falling in this category if *"such data constitute access data"*. Service providers may have difficulty to distinguish between access data and transactional data in practice, while the proposed Regulation provides that these categories should be produced under different conditions. Therefore, **the EDPS recommends clarifying the definitions of access data and transactional data and making a clear delineation between these categories to ensure legal certainty. The same data should not be produced under different conditions depending on the category under which it is requested. Otherwise, EPO for access data must be subject to the same conditions as transactional data and content data (Article 4(2)).**

23. Furthermore, the EDPS shares similar concerns as regard the category of subscriber data. The Convention on Cybercrime already includes a definition of "subscriber information"[xlv], which is not always interpreted uniformly among Parties to the Convention[xlvi]. The proposed Regulation provides the first definition of subscriber data in EU law. The EDPS considers that defining this data category in the proposed Regulation is a difficult but important exercise. The EDPS points out that it is essential to avoid any confusion between the categories of transactional data and subscriber data, in particular with regard to point (b) of Article 2(7), since the production of these two data categories would also be submitted to different conditions. In this regard, the EDPS points out that IP addresses could fall in both categories of transactional data and subscriber data, in addition to the category of access data which specifically mentions IP address. **The EDPS recommends amending the proposed definition of subscriber data in order to further specify this category, in particular point (b) of Article 2(7) and in relation to IP address, and to avoid overlap with other data categories.**

3.2. The type of offences concerned

24. The EDPS takes note of the type of offences for which authorities may issue EPO and EPO-PR. First, EPO may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State (Article 5(2) of the proposed Regulation). EPO to produce subscriber data and access data may be issued for all criminal offences (Article 5(3) of the proposed Regulation), whereas EPO to produce transactional data and content data may be issued for a variety of offences listed in Article 5(4) of the proposed Regulation:

(a) all "*criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years*";
(b) offences "*if they are wholly or partly committed by means of an information system*" related to fraud and counterfeiting of non-cash means of payment, sexual abuse and exploitation of children, child pornography and attacks against information systems;
(c) terrorist offences.

25. Second, EPO-PR to preserve any type of electronic evidence may be issued for all criminal offences without distinction (Article 6(2) of the proposed Regulation). The requirement of a similar measure available for domestic cases does not apply to EPO-PR.

26. The EDPS considers that the proposed threshold of three-year minimum of the maximum custodial sentence in Article 5(4)(a) and the list of cyber-dependent and cyber-enabled offences in Article 5(4)(b) are highly problematic given the sensitivity of the transactional data and content data and the seriousness of the interference with the rights to privacy and data protection that accessing such data would entail. The threshold of three-year minimum of the maximum custodial sentence in Article 5(4)(a) of the proposed Regulation would in practice apply to a very large number of offences in Member States' national criminal codes, including many offences that may not be considered as "serious"[xlvii].

27. The EDPS recalls that the CJEU found in relation to metadata retained 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"*[xlviii] 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"*[xlix]. In relation to content data, the CJEU found that access to such data may even affect the essence of the right to privacy and the right to data protection[l].

28. Furthermore, the EDPS raises that the CJEU held in its recent judgment in Case C-207/16 that *"[i]n accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'"* and *"in [those areas], only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of electronic communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned"*[li]. The EDPS considers that access by national competent authorities to the categories of transactional data and content data would allow such precise conclusions to be drawn concerning the private lives of persons whose data would be sought with EPO. Thus, it is essential that access to these categories of data is limited to cases of serious crime only.

29. In relation to the list of cyber-dependent and cyber-enabled offences in Article 5(4)(b), the EDPS is not convinced by the justification in Recital 32 that these offences are "*specific offences where evidence will typically be available exclusively in electronic form*" and that "*applying the same threshold as for other types of offences would predominantly lead to impunity*". The EDPS considers that not all cyber-dependent and cyber-enabled offences listed in Article 5(4)(b) may constitute "serious crimes". Nevertheless, recognising that it might be necessary and proportionate to obtain transactional or content data in certain cases, this could be achieved through the preservation of any type of data via EPO-PR, with a request for production of the preserved data through traditional channels of cooperation (such as EIO), thus preserving the necessary high safeguards.

30. **For these reasons, the EDPS recommends to reassess the balance between the types of offences for which EPOs could be issued and the categories of data concerned. In particular, the possibility to issue an EPO to produce transactional data and content data should be limited to serious crimes only[lii].**

31. **Furthermore, given the potentially revealing nature of transactional data and content data, the EDPS considers that access to such data should only be granted in the context of specific serious crimes.** Providing a closed list of such serious crimes would also increase legal certainty for all stakeholders involved. While the option to limit the scope of application of the EPO to certain crimes was discarded at an early stage of preparation of the Proposals[liii], **the EDPS recommends to reconsider this possibility, taking into account the relevant case law of the CJEU[liv].**

32. Finally, the EDPS points out that **similar considerations might also be relevant for EPO to produce subscriber data and access data as currently defined in the proposed Regulation, to the extent these categories are not further specified and circumscribed and could potentially include electronic communications "metadata"**[lv].

3.3. Data Security

33. Ensuring the security of personal data is a clear requirement under EU data protection law[lvi]. Data security is also essential to ensuring the secrecy of investigations and the confidentiality of criminal proceedings. While welcoming Article 11 on the confidentiality of information and Recital 57 of the proposed Regulation[lvii], the EDPS notes that it does not adequately address the question of the authenticity of the certificates received by service providers[lviii], the security of the transmission of personal data to the relevant authorities in response[lix] and the security of orders received by enforcing authorities[lx].

34. The **verification of authenticity of certificates and orders is essential** to ensure that all personal data transmitted remain confidential and avoid potential data breaches that could have adverse consequences for individuals concerned and engage the liability of the enforcing authorities, service providers or their legal representatives under the applicable data protection laws. Therefore, **the EDPS recommends introducing in the proposed Regulation provisions defining how the authenticity of certificates and orders can be ensured and verified.** The EDPS notably suggests investigating the use of digital signatures in cases where orders and certificates are transmitted electronically. He underlines that ensuring that the necessary means are put in place so that the personal data are disclosed and communicated under the Proposals in a secure environment with the means to ensure the authenticity of documents is key for achieving the objective of a fast gathering of electronic evidence in compliance with fundamental rights.

35. The EDPS welcomes that, with regard to the **security of the transmission of certificates and the requested data**, the Council general approach specifies that EPOC and EPOC-PR shall be transmitted "*in a secure and reliable way allowing the addressee to produce a written record and to establish the authenticity of the Certificate*"[lxi] and that the requested data shall be "*transmitted in a secure and reliable way allowing the establishment of authenticity and integrity*"[lxii]. **He considers however that more specific and effective safeguards are required, including with regard to the security of orders received by enforcing authorities**.

36. Regarding in particular the **transmission of certificates**, Article 8(2) of the proposed Regulation and of the Council general approach would allow, the use of already established dedicated platforms or secure channels to handle requests of law enforcement and judicial authorities. However, this remains optional and would not be expressly allowed for other communications by the issuing authority involving personal data that are to take place following that transmission.

37. The EDPS also notes that *"the Commission is working to strengthen the existing judicial cooperation mechanisms through measures such as the creation of a secure platform for the swift exchange of requests between judicial authorities within the EU"*[lxiii] and that the Commission suggests considering "*a possible expansion of the eCodex*[lxiv] *and SIRIUS platforms*[lxv] *to include a secure connection to service providers for the purposes of the transmission of the EPOC and EPOC-PR and, where appropriate, responses from the service providers"*[lxvi]. The EDPS notes in this regard that during the negotiations in Council, one Member State proposed "*the addition of a new recital requesting the Commission and the Member States to work on and establish as soon as possible secure electronic channels of communication allowing the establishment of authenticity and integrity*"[lxvii]. In this regard, the EDPS recalls that any establishment of a new IT system processing personal data requires a legal basis and that in particular, at least, where such IT system entails the involvement of an EU institution, body, agency or office, this legal basis shall be found in an EU legal act. **The EDPS therefore recommends to provide clearly in the Regulation for an explicit legal basis for an IT system to be used for the processing of personal data for the purpose of the Regulation**.

38. Additionally, the EDPS welcomes the fact that the publicity of the information related both to the **identification of the authorities and legal representatives** of services providers is provided for under the Proposals and under the Council general approach[lxviii]. However, **he recommends modifying the proposed texts so as to impose these obligations before the date of application of other provisions, thus ensuring that all the required information is available at the date of application of the main provisions and avoiding any risk of personal data breach**[lxix].

3.4. Greater involvement of judicial authorities in the enforcing Member State

39. According to the proposed Regulation, the control over compliance with fundamental rights of data subjects concerned by the EPO/EPO-PR, including over the necessity and proportionality of the orders and the possible applicability of immunities and privileges, would primarily be ensured by the issuing authority. Competent authorities in the enforcing Member State would only intervene as enforcing authorities in cases where service providers do not comply with an order. Hence, once orders are issued, given that in most cases data subjects would not be immediately informed of the orders[lxx], service providers would be the only actors having the possibility to protect data subjects privacy and data protection rights.

40. 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 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 has to be considered that relevant laws in the EU Member States - *inter alia* on the admissibility of evidence gathered in another Member State and what constitutes a criminal offence - may diverge[lxxi]. Even in the context of these Proposals if adopted, conditions for issuing an order are not fully harmonised across the EU and important objections, stemming from the respect of fundamental rights, against the execution of such order may exist[lxxii]. In the context of the EIO Directive negotiations, the Fundamental Rights Agency emphasised that *"respect for fundamental rights constitutes a key component of the area of freedom, security and justice, as foreseen by Article 67 (1) TFEU: 'The Union shall constitute an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States'*[lxxiii]*. So, even if mutual recognition is presented as a 'principle'*[lxxiv] *which is used by EU Member States to facilitate cooperation in the area of freedom, security and justice, Member States must comply with their legal obligations to respect fundamental rights*[lxxv]*"*.

41. The EDPB 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*"[lxxvi]. The EDPB also expressed "*its concerns as regards the removal of any double check by the receiving competent authority of the order transmitted, compared to the other instruments*"[lxxvii]. In its general approach on the proposed Regulation, the Council has introduced a notification to the competent authorities of the enforcing Member States. This notification would take place at the same time as EPOC are sent to service providers. However it would have no suspensive effect; it would have a limited scope (it would only be required for EPOC concerning content data[lxxviii] - which is the least common requested data[lxxix] - where the data subject does not reside in the issuing Member State); finally, the notified authorities would only be able to raise a limited number of issues (there is no general ground for refusal based on fundamental rights as such), without the power to prevent directly the enforcement of the order[lxxx]. Hence, several Member States requested that greater power be granted to the notified authority and covering also orders for non-content data[lxxxi].

42. **The EDPS considers that effective protection of fundamental rights in this context requires a degree of involvement of judicial authorities of the enforcing Member State. He therefore recommends involving systematically judicial authorities designated by the enforcing Member State as early as possible in the process of gathering electronic evidence in order to give these authorities the possibility to effectively and efficiently review compliance of the orders with the Charter and ensure the obligation for these authorities to raise grounds for refusal on that basis[lxxxii].**

43. Furthermore, the systematic involvement of judicial authorities in the enforcing Member States could ensure compliance with the dual criminality principle. Considering that there is no harmonisation of criminal offences within the EU, the abandonment of the dual criminality principle in the proposed Regulation means that personal data may be disclosed by a service provider for the purpose of the prosecution of an act, which, under the law of the Member State where it is established, does not constitute a criminal offence[lxxxiii]. **The EDPS considers that the dual criminality principle is an additional safeguard for fundamental rights that should be part of the proposed Regulation**. As already raised by the EDPB[lxxxiv], such safeguard would *"ensure that a State cannot rely on the assistance of another to apply a criminal sanction which does not exist in the law of another State"*[lxxxv]. **The EDPS therefore recommends introducing the requirement of the dual criminality principle in the proposed Regulation, for all cases where data are requested on the basis of an offence which is neither defined at EU level nor agreed upon at EU level in a closed list to be inserted in the Regulation**[lxxxvi].

44. **Finally, the involvement of the judicial authorities of the enforcing State would also be more in line with the choice of Article 82(1) TFEU as legal basis for the proposed Regulation.** The EDPS notes indeed that so far this Article has been used to establish cooperation mechanism between judicial authorities only. Consistently with his Opinions 2/2019 and 3/2019[lxxxvii], the EDPS has strong doubts that this provision could serve as a legal basis to adopt an EU Regulation establishing cross-border direct cooperation between judicial authorities and service providers in criminal matters with - in principle - no involvement of any authority in the enforcing Member State[lxxxviii].

3.5. Limited preservation under European Preservation Orders

45. The proposed Regulation would establish EPO-PR to compel service providers to preserve data in view of a subsequent request to produce these data via a Mutual Legal Assistance (hereinafter "MLA") request, an EIO or an EPO. Such orders aim to *"prevent the removal, deletion or alteration of relevant data in situations where it may take more time to obtain the production of this data"*[lxxxix]. The EDPS understands that the EPO-PR concerns specific data stored by the service provider at the time of receipt of the EPOC-PR and does not relate to future data stored after this point in time. It is also important to stress that EPO-PR would not establish a general data retention obligation[xc].

46. The EDPS recalls the principle of storage limitation[xci] according to which personal data should be kept for no longer than is necessary for the purposes for which they are processed. The proposed Regulation provides that the preservation must be limited to a maximum of 60 days *"unless the issuing authority confirms that the subsequent request for production has been launched"* (Article 10(1)). If the issuing authority makes such a confirmation during the 60 days period, the addressee shall continue to preserve the data as long as necessary to allow their production (Article 10(2)). Recital 42 further explains that this 60 day period was calculated to allow for the launch of an official request and that such "launch" requires that at least some formal steps have been taken, *e.g.* by sending a MLA request to translation. When the preservation of the data is no longer necessary, the issuing authority must inform the addressee without undue delay (Article 10(3)). **The EDPS understands that each preservation order should in principle be linked to a subsequent request for production. The period of preservation of the data sought is therefore also linked to the future of this subsequent request. The EDPS thus suggests clarifying that the preservation would no longer be necessary and should stop if the subsequent request is rejected or withdrawn.** This specification is also valid for Article 9(6) last sentence[xcii].

47. Furthermore, as already raised by the EDPB[xciii], the EPO-PR should *"never serve as a basis for the service provider to process the data after the initial date of erasure"*. The EDPS also understands that **the data preserved should not be altered as from the time of receipt of the EPOC-PR and until their production following a subsequent request for production.** Therefore, **the EDPS recommends further specifying in the proposed Regulation that the data sought with an EPO-PR should be kept aside and their processing should be limited to their storage until their production.**

4. ADDITIONAL RECOMMENDATIONS

4.1. Complete reference to applicable data protection framework

48. The EDPS welcomes that the proposed Regulation takes into account the EU data protection framework and states that personal data may only be processed in accordance with the GDPR and the Law Enforcement Directive for the police and justice sectors in Recital 56 of the proposed Regulation. **The EDPS recommends to add a reference to the ePrivacy Directive 2002/58/EC (to be replaced by the proposed ePrivacy Regulation, once adopted[xciv]).**

49. The EDPS notes that in its general approach, the Council added a provision on the further transfer of the received data by Member States authorities to third State authorities, referring to the conditions set out in the proposed Regulation and Chapter V of the Directive (EU) 2016/680[xcv]. The EDPS recalls that pursuant to Article 35 of the Directive (EU)2016/680, a transfer of personal data to a third country is subject not only to the conditions provided for Chapter V but also to compliance with the national provisions adopted pursuant to other provisions of this Directive. **The EDPS therefore advises against including such a provision in the final text.**

4.2. Rights of the data subjects

4.2.1. Enhanced transparency

50. The EDPS considers that general awareness about the frequency and volume of preservation and production orders addressed to service providers would give citizens in general and also public bodies the possibility to benchmark and assess the general practice in the use of these instruments. Transparency may thus play an important role in helping ensure respect for fundamental rights. The EDPS notes that some service providers[xcvi] already publish transparency reports on a regular basis in which they indicate overall number of access requests received from public authorities and responses to these requests.

51. **The EDPS therefore suggests introducing an obligation to publicly disclose periodically and in an aggregate form the number of EPOC and EPOC-PR received by services providers under the proposed Regulation, and whether or not these requests were fulfilled[xcvii].**

4.2.2. Right to a remedy

52. The EDPS welcomes Article 17 of the proposed Regulation which clarifies that remedies available under the GPDR and the Law Enforcement Directive for the data subject whose data has been obtained remain. **He recommends adding the case where the data has been preserved** (as it cannot be excluded that a breach of data protection obligations arises in relation to such data).

53. The conditions for the remedies against service providers on grounds of a violation of a data protection provisions under EU law as controllers or processors are already provided for under the GDPR. For instance, under Article 82(3) GDPR, *"[a] controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage*".

54. Recital 46 of the proposed Regulation provides that *"[n]otwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR"*. **The EDPS considers that an instrument relating to cooperation in criminal matters should not amend the conditions for liability of controllers or processors (*i.e.* service providers or competent authorities) under data protection law. Recital 46 should therefore be deleted**.

4.3. Data subjects benefiting from immunities and privileges

55. The EDPS welcomes Article 5(7) of the proposed Regulation whereby an EPO concerning access, transactional or content data should not be issued if the issuing authority finds that the data are protected by immunities and privileges under the law of the Member State where the service provider would be addressed[xcviii]. He regrets that under the Council general approach, the obligation of the issuing authority to take immunities and privileges into account and, where necessary, not to issue an EPO or to adapt it has been limited only to situations where the immunities and privileges under the law of the enforcing States concern transactional data and the "person whose data are sought" is not residing in the issuing Member State[xcix].

56. In addition, the issuing authority might reasonably not be aware of immunities or privileges under the law of the enforcing Member State. Therefore, the EDPS welcomes the fact that, if an EPO has been issued despite such immunities and privileges under the law of the enforcing State, Article 14(2) of the proposed Regulation allows the enforcing authority to refuse the enforcement of an order, without limitations as to the data concerned[c]. However, the EDPS notes that it is only in cases where, for another reason, the certificate would not have been complied with by the service provider, that the enforcing authority could raise such objection[ci]. Under the Council's general approach, such objection has been limited to cases where the "person whose data are sought" does not reside in the issuing State and to content data[cii].

57. He also takes note of Article 18 of the proposed Regulation[ciii] which provides that if data were obtained despite such immunities and privileges, "*these grounds are taken into account in the same way as if they were provided for under their national law*"[civ].

58. The EDPS **recommends modifying the proposed Regulation so as to at least ensure that:**
- **an EPO cannot be issued where the transactional and content data are protected by immunities and privileges under the law of the enforcing Member State and it was not possible to obtain such immunities and privileges to be waived[cv];**
- **there is an obligation in the enforcing State to review this ground for all such data[cvi].**

4.4. Legal representatives

59. As already stressed by the EDPB[cvii], any confusion should be avoided between legal representatives appointed by service providers offering services in the EU for the purpose of gathering evidence in criminal proceedings and the representatives appointed to comply with Article 27 GDPR. Similarly, confusion should be avoided with the representatives that would have to be appointed to comply with the proposed ePrivacy Regulation[cviii].

60. Representatives appointed to comply with the proposed Directive and the GDPR may share some similarities as they would act as contact points of the service providers they represent. However, they would have very different tasks and responsibilities in nature and they would answer to different types of stakeholders[cix]. These two functions require different knowledge and competencies. Furthermore, these obligations to designate representatives may apply to different service providers, depending on whether they are subject to the proposed Directive or the GDPR[cx]. Therefore, **the EDPS recommends clarifying that these different types of representatives would pursue different objectives and have different tasks and responsibilities**.

4.5. Time limits to produce data

61. One of the main objectives of the proposed Regulation is to speed up the cross-border procedure to obtain evidence in another State compared to existing cooperation mechanisms. The EDPS notes that the time limits provided under the proposed Regulation are not only a time period to ensure a swift preservation and production of data but also the time in which the compliance check of the certificates with fundamental rights, among other grounds, has to take place.

62. While understanding the objectives of the proposed Regulation (such as preventing the volatility of data or ensuring the effectiveness of criminal proceedings), the EDPS considers that the time limits in all cases[*cxi*] are too short to appropriately assess the certificates received and identify if there are any grounds not to comply with them (*e.g.* violation of the Charter or conflict of laws) and take the appropriate decision. He notes that, comparatively, the EIO Directive provides a time limit of 30 days for judicial authorities in the executing State to perform their assessment and decide on the "*recognition or execution"* of an order[cxii] and for 90 days following the taking of that decision to carry out the investigative measure[cxiii]. He underlines also that in any event, in order to avoid the deletion of the data sought while assessing the EPOC, Article 9(6) obliges service providers to "*preserve the data requested, if it does not produce it immediately*" and "*[t]he preservation shall be upheld until the data is produced*".

63. Therefore, **the EDPS recommends setting longer time limits than 10 days, which would allow an appropriate assessment of the certificate as well as the transmission of the requested data in due time.**

64. Moreover, the EDPS notes that, besides emergency cases, the proposed Regulation allows in all cases issuing authorities to define shorter time limits than 10 days if they indicate "*reasons for earlier disclosure*". Unless further justification is provided for giving issuing authorities the possibility to define themselves shorter deadlines in all cases and to depart from the time limits allowed under the EIO Directive, **the EDPS recommends removing this possibility for issuing authorities to impose compulsory time limits on service providers that are shorter than the one provided by the proposed Regulation.**

65. Finally, the EDPS considers that the 6 hour time limit to produce the data in emergency cases might not always be realistic and **recommends making it a preferred time limit rather than a compulsory one**.

4.6. Possibility for service providers to object

66. The EDPS supports that the proposed Regulation allows service providers to object the enforcement of an order. Such objections should however be based on limited grounds. These 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. In this regard, the EDPS recommends in particular introducing a ground to object the execution of an EPOC (Article 9) and the enforcement of an EPO (Article 14) where the data is protected by immunities and privileges under the law of the enforcing Member State (see section 4.3). The EDPS notes that service providers are not obliged to assess such grounds before enforcing the order but only that they "may oppose" the enforcement of an order on that basis (Article 14(4) and (5)). The EDPS could support such approach if, on the other hand, a true review mechanism by the authorities of another Member State than the issuing State is introduced as explained above (see section 3.4). In particular, the EDPS is concerned that submitting service providers to possible pecuniary sanctions in case of non-compliance with their obligations - *inter alia* to preserve or transmit the data upon receipt of the certificates[cxiv] - might in practice dissuade them from raising objections in specific cases[cxv].

4.7. Interaction with other instruments

67. The EDPS notes that the scope of the proposed Regulation is so defined that it would allow as a matter of principle competent authorities in the EU to gather data from a service provider established in a third country, regardless of the location of the requested data, as long as it offers services in the EU. The service provider or the processing of such data may therefore be under the jurisdiction of a third country law, which may lead to conflicting obligations for service providers, under the EU framework, on the one hand and under a third country law, on the other hand. For instance, the US Stored Communications Act prohibits in principle the disclosure, by a provider of electronic communication services[cxvi] under US jurisdiction, of content data following requests from foreign authorities, unless such requests are from authorities of qualifying foreign governments which concluded an executive agreement with the US[cxvii] and the data concerns non-US persons.

68. The Commission sought to address this issue by providing in the proposed Regulation for a review procedure establishing a dialogue with the authorities of the concerned third country in case of conflicting obligations based on fundamental rights (Article 15), in an attempt to set an example for foreign legislators when drafting their own legislations[cxviii]. At the same time, the Commission issued recommendations for Council Decisions, for the opening of negotiations with the US on an international agreement and the authorisation to negotiate, on behalf of the EU, the second Additional Protocol to the Convention on Cybercrime (see section 1). In May 2019, the Council adopted the decisions[cxix]. The negotiating directives for a EU-US agreement provide specific objectives, among which "*address conflicts of law*" and "*set common rules for orders for obtaining electronic evidence, in the form of content and non-content data, from a judicial authority in one contracting party, addressed to a service provider that is subject to the law of the other contracting party*"[cxx]. The negotiating directives on the second Additional Protocol to the Convention on Cybercrime provide that the protocol should contain *"a clause providing that Member States shall, in their mutual relations, continue to apply rules of the European Union rather than the Second Additional Protocol"*[cxxi]. However, at this stage, it is not yet clear on the basis of which criteria the delineation between intra-EU cross-border cases (*i.e.* cases falling within the scope of the Proposals) and international cases (*i.e.* cases covered by an international agreement) will be defined. In this regard, the EDPS took note of the provision introduced by the Council in its general approach (Article 23)[cxxii]. **However the EDPS recommends providing more clarity on this issue in order to ensure legal certainty.** This is important for the lawfulness of any processing of personal data in this context.

69. The EDPS also recalls that, as far as data protection is concerned, the communication of personal data to third country authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties can only take place in accordance with the rules on transfer as provided by Chapter V of the Law Enforcement Directive in absence of international agreements applicable to the taking of evidence in criminal matters between the Member State and the third country concerned. In general, **the EDPS underlines that it is important to ensure that the final text of the proposed Regulation maintains the high level of data protection in the EU** so that, when negotiating any international agreement in matters of cross-border access to electronic evidence, **it constitutes a reference that ensures respect for fundamental rights, including the rights to privacy and data protection, and provides strong safeguards.**

5. CONCLUSIONS

70. The EDPS **supports the objective** of ensuring that effective tools are available to law enforcement and judicial authorities to investigate and prosecute criminal offences in a world transformed by new technologies. At the same time, the EDPS would like to ensure that this action is fully respectful of the Charter and the EU data protection acquis. The proposed Regulation would require the storage and communication of personal data inside and outside the EU between Member States' competent authorities, private entities and in some cases third countries' authorities. It would entail limitations on the two fundamental rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter. To be lawful, such limitations must comply with the conditions laid down in Article 52(1) of the Charter and notably meet the necessity condition.

71. The EDPS first considers that other **alternatives** that would provide greater safeguards while achieving the same goals should be further assessed.

72. Second, the EDPS takes note that the proposed Regulation already includes a number of procedural safeguards. However, the EDPS is concerned that the important responsibility of reviewing compliance of EPOC and EPOC-PR with the Charter is entrusted to service providers and recommends **involving judicial authorities designated by the enforcing Member State** as early as possible in the process of gathering electronic evidence.

73. The EDPS recommends ensuring further consistency between the definitions of categories of electronic evidence data and existing **definitions of specific categories of data** under EU law and **reconsidering the category of access data,** or to submit the access to these data to similar conditions to those for accessing the categories of transactional data and content data. The proposed Regulation should lay down clear and straightforward definitions of each data category in order to ensure legal certainty for all stakeholders involved. He also recommends **amending the proposed definition of the category of subscriber data** in order to further specify it.

74. He further recommends **reassessing the balance between the type of offences for which EPOs could be issued and the categories of data concerned**, taking into account the recent relevant case law of the CJEU. In particular, the possibility to issue an EPO to produce transactional data and content data should be limited to serious crimes. Ideally, the EDPS would favour the definition of a closed list of specific serious criminal offences for EPOs to produce transactional data and content data, which will also increase legal certainty for all stakeholders involved.

75. The EDPS also makes recommendations aiming at ensuring the respect for data protection and privacy rights while achieving a speedy gathering of evidence for the purpose of specific criminal proceedings. They focus on the **security of the transmission** of data between all stakeholders involved, the **authenticity** of orders and certificates and the **limited preservation** of data under an EPO-PR

76. Beyond the general comments and main recommendations made above, the EDPS has made additional recommendations in this Opinion regarding the following aspects of the Proposals:
- the **reference to the applicable data protection framework**;
- the **rights of the data subjects** (enhanced transparency and the right to a legal remedy);
- data subjects benefiting from **immunities and privileges**;
- the **appointment of legal representatives** for the gathering of evidence in criminal matters;
- the **time limits to comply** with EPOC and produce the data;
- the possibility for **service providers to object to orders based on limited grounds**.

77. Finally, the EDPS is aware of the **broader context** in which the initiative has been tabled and of the two Council Decisions adopted, one regarding the Second Additional Protocol to the Convention on Cybercrime at the Council of Europe and one regarding the opening of negotiations with the United States. He asks for more clarity on the interaction of the proposed Regulation with international agreements. The EDPS is eager to contribute constructively in order to ensure consistency and compatibility between the final texts and the EU data protection framework.

Brussels, 6 November 2019

Wojciech Rafał WIEWIÓROWSKI

NOTES

[i] OJ L 295, 21.11.2018, p. 39.
[ii] OJ L 119, 4.5.2016, p. 1 (hereinafter "GDPR").
[iii] OJ L 119, 4.5.2016, p. 89 (hereinafter "Law Enforcement Directive").
[iv] Commission Staff Working Document: Impact Assessment, SWD(2018) 118 final (hereinafter "Impact Assessment"), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN.
[v] 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.
[vi] 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.
[vii] Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014, regarding the European Investigation Order in criminal matters, O.J. L 130, 1.5.2014, p. 1; see Article 23 of the proposed Regulation.
[viii] The EIO Directive provides for a direct cooperation between the issuing authority in a Member State and the executing authority of another Member State or, as the case may be, via the central authority(ies) appointed by the Member State(s) concerned. It aims at facilitating and speeding up this cooperation by providing for standardised forms and strict time limits and removing several obstacles to cross-border cooperation; for instance, *"[t]he issuing authority may issue an EIO in order to take any measure with a view to provisionally preventing the destruction, transformation, removal, transfer or disposal of an item that may be used as evidence"* and *"the executing authority shall decide and communicate the decision on the provisional measure as soon as possible and, wherever practicable, within 24 hours of receipt of the EIO"* (Article 32); also the execution of a EIO for the identification of persons holding a subscription of a specified phone number or IP address is not subject to the double criminality requirement (Article 10(2)(e) combined with Article 11(2)).
[ix] All EU Member States except Denmark and Ireland.
[x] All participating Member States have implemented the EIO Directive in their national laws in 2017 or 2018. See the European Judicial Network implementation status: https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120.
[xi] The EDPB established by Article 68 GDPR succeeded the Working Party established by Article 29 of Directive 95/46/EC, which was repealed. Similarly to the Article 29 Working Party, the EDPB is composed of representatives of the national data protection authorities and the EDPS.
[xii] Opinion 23/2018 of 26 September 2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b) (hereinafter "EDPB Opinion 23/2018"), available at: https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.
[xiii] https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#.
[xiv] 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/.
[xv] 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.
[xvi] 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. To date, all Member States of the EU have signed the Convention of the Council of Europe on enhanced international cooperation on cybercrime and electronic evidence and almost all of them have ratified it. Ireland and Sweden are still in the process of ratifying the Convention on Cybercrime. The Convention on Cybercrime 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 also fosters international cooperation between the Contracting Parties. There are specific measures to address the challenges arising from the volatility of data. In this respect, the Convention provides for the expedited preservation of stored computer data. Since the transfer of the secured evidence to the requesting state is subject to a final decision on the formal Mutual Legal Assistance request, the preservation shall not be subject to the full set of grounds for refusal, in particular double criminality shall be required in exceptional cases only (Article 29).
[xvii] EDPS Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence and EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention.

[xviii] Available at: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[xix] https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_fr.

[xx] https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

[xxi] Explanatory Memorandum of the proposed Regulation, p. 2.

[xxii] Court of Justice of the European Union (hereinafter "CJEU"), Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 33, where the Court held in relation to the establishment of a limitation with the right to respect for private life that "*it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"*. See also CJEU, Case C- 207/16, Ministerio fiscal, ECLI:EU:C:2018:788, par. 51.

[xxiii] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 36, where the Court held that a measure *"constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data"*.

[xxiv] Available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf. See section II 4) of the EDPS Necessity Toolkit, p. 7 and CJEU, Opinion 1/15, ECLI:EU:C:2017:592, par. 140: "*[a]s regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary (...)"*.

[xxv] Cross-border situations refer to situations where the service provider addressed is established or represented in another Member State than the issuing authority.

[xxvi] Domestic situations refer to situations where the service provider addressed is established or represented in the same Member State as the issuing authority. In such cases, authorities of that Member State must use national measures to compel the service provider. See Recital 15 of the proposed Regulation.

[xxvii] See Article 2(4) of the proposed Regulation for the definition of " *offering services in the Union* ". It means not only enabling persons in one or more Member State(s) to use the listed services but also to have a substantial connection to such Member State(s).

[xxviii] Explanatory Memorandum of the proposed Directive, p. 3; see also Article 7 of the proposed Regulation. Article 7(1) provides that EPO and EPO-PR will have to be addressed directly to the legal representative designated by the service provider concerned. Article 7(2) provides as a fall-back option that *"[i]f no dedicated legal representative has been appointed, the European Production Order and the European Preservation Order may be addressed to any establishment of the service provider in the Union"*.

[xxix] Article 3 of the proposed Directive provides that Member States will ensure that, whether or not they are established in the EU, service providers offering services in the EU designate at least one legal representative in the Union.

[xxx] Under Article 7 of the proposed Regulation, the addressee of the orders is in principle the legal representative appointed by the service provider and in some instances, it can be the establishment of the service provider in the EU. The terms "service provider" and "addressee" are used in this Opinion to designate the legal representative or the establishment to whom an order, through a certificate, is transmitted.

[xxxi] Impact Assessment, pp. 94, 156 and 179.

[xxxii] The rights in Article 6 are the rights guaranteed by Article 5 of the European Convention on Human Rights, and in accordance with Article 52(3) of the Charter, they have the same meaning and scope. See Explanations relating to the charter of fundamental rights (2007/C 303/02).

[xxxiii] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 54-55.

[xxxiv] See speech by Prof. Koen Lenaerts, President of the CJEU, at a side-event of the 40th International Conference of Data Protection and Privacy Commissioners ("The General Data Protection Regulation five months on*"*), available at: https://webcast.ec.europa.eu/the-general-data-protection-regulation-five-months-on-25-10-2018#.

[xxxv] Explanatory Memorandum of the proposed Regulation, p. 16: *"[t]ransactional and content data should be subject to stricter requirements to reflect the more sensitive nature of such data and the correspondingly higher degree of invasiveness of Orders for such data, as compared to subscriber and access data"*.

[xxxvi] These requirements are laid down in Articles 4, 5 and 6 of the proposed Regulation and concern the criminal offences for which orders for the production or preservation of these data categories can be issued and the judicial authority issuing or validating the order.

[xxxvii] Article 4(3)(a) of the proposed ePrivacy Regulation defines 'electronic communications data' as "*electronic communications content and electronic communications metadata*".

[xxxviii] Article 4(3)(b) of the proposed ePrivacy Regulation defines 'electronic communications content' as "*the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound*".

[xxxix] Article 4(3)(c) of the proposed ePrivacy Regulation defines 'electronic communications metadata' as "*data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging*

electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication".

[xl] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en.

[xli] Explanatory Memorandum of the proposed Regulation, p. 2: *"[t]his proposal aims to improve legal certainty for authorities, service providers and persons affected and to maintain a high standard for law enforcement requests, thus ensuring protection of fundamental rights, transparency and accountability"*.

[xlii] Explanatory Memorandum of the proposed Regulation, p. 14.

[xliii] Impact Assessment, p. 129: *"[t]he definition of types of data (subscriber, traffic and content data) varies significantly among Member States, while specific categories of data exist in several countries. Data requested from service providers are generally subscriber (21 Member States) and traffic data (18 Member States), while in a few Member States (9) it is also possible to request content data and "other data" (4 Member States)"*.

[xliv] See EDPB Opinion 23/2018, p. 12: *"the four categories proposed do not appear to be clearly delineated, and the definition of "access data" still remains vague"*.

[xlv] Article 18(3) of the Cybercrime Convention defines 'subscriber information' as "*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"*.

[xlvi] See Council of Europe Cybercrime Convention Committee, "Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments", T-CY (2018)26, 25 October 2018, on whether dynamic IP addresses should be submitted to rules to obtain subscriber information or rules to obtain traffic data (defined under Article 1(d) of the Convention), which notably concluded that *"Introducing new categories of data, such as "access data", may lead to further misunderstandings regarding applicable rules on the retention of or access to such data and may be difficult to apply by practitioners"*.

[xlvii] See Advocate General Opinion, Case C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:300, par. 117 and 118:
"(...)the Court should refrain from adopting a position in favour of a precise quantum of penalty incurred, since what is appropriate for certain Member States will not necessarily be appropriate for others, and what applies today for a type of offence will not necessarily apply irrevocably in the future (...)
(...) I observe that, in the present case, the referring court mentions a risk of inversion of the general rule and the derogations provided for in Directive 2002/58, a risk referred to above, (132) where it states that 'the threshold of three years' imprisonment [introduced by the Spanish legislature in 2015 (133)] covers a significant majority of criminal offences'. In other words, according to the referring court, the current list of offences capable of justifying, in Spain, restrictions of the rights protected under Articles 7 and 8 of the Charter, which was established by the reform of the Code of Criminal Procedure, would lead in practice to the majority of offences provided for in the Criminal Code being included in that list".

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

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

[l] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238, par. 39 and CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson, ECLI:EU:C:2016:970, par. 101.

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

[lii] See Advocate General Opinion, Case C-207/16, Ministerio Fiscal, ECLI:EU:C:2018:300, which provided indications on the criteria that might be used to define "serious crimes" within the meaning of the CJEU case law, including regarding the criterion of the sentence incurred.

[liii] Impact Assessment, p. 240.

[liv] CJEU, Case C- 207/16, Ministerio fiscal, ECLI:EU:C:2018:788.

[lv] See section 3.1 of this Opinion on the imperative to clarify the categories of data under the proposed Regulation.

[lvi] 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.

[lvii] Recital 57 specifies that *"Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers […] to ensure the security of the data. Service providers should ensure the same for the transmission of personal data to relevant authorities. Only*

authorised persons should have access to information containing personal data which may be obtained through authentication processes. The use of mechanisms to ensure authenticity should be considered, such as notified national electronic identification systems or trust services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC".

[lviii] Article 8(2) only provides that *"[t]he EPOC or the EPOC-PR shall be directly transmitted by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity"* [emphasis added].

[lix] Article 9 provides that *"the addressee shall ensure that the requested data is transmitted directly to the [authority] indicated in the EPOC"*. It does not refer to any appropriate security measures for the transmission of the data produced by the addressees of EPOC. The proposed Regulation remains silent as to the security of the communications following the transmission of an EPOC-PR.

[lx] Article 14 (1) only provides that the issuing authority may transmit the order with other documents *"by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity"* [emphasis added].

[lxi] Article 8 of the general approach on the proposed Regulation.

[lxii] Article 9 of the general approach on the proposed Regulation.

[lxiii] Explanatory Memorandum of the proposed Regulation, p. 2.

[lxiv] See Inception Impact Assessment on Cross-border e-Justice in Europe (e-CODEX), available at: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3600084_en, p. 1: *"'e-CODEX' is an IT system for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. It operates as a decentralised network of access points, interlinking national and European IT systems to one another. Specific software is required to establish an e-CODEX access point.*

The e-CODEX system has been developed in the context of the Digital Single Market by a group of Member States with the help of EU grants. Various Member States are already using e-CODEX to support cross border legal procedures both in civil and criminal matters, for example for the exchange of requests for mutual legal assistance between public prosecutors".

See also the e-Codex website, which indicates that it has come to an end but that *"[t]he goal of Me-CODEX (Maintenance of e-CODEX) is bridging the time between the end of e-CODEX as a project and the uptake of e-CODEX maintenance by an EU agency. It will take 2-4 years to make the necessary extension of the mandate of the EU agency. Since the Member States exchanging information through e-CODEX will not switch off their solutions after the end of e-CODEX as a project, an intermediary maintenance solution has to be found. The EC has urged the permanent expert group on e-CODEX to deliver a solution to assure operations and expand the community of users. The solution, "Me-CODEX", will work on a smooth handover to an EU agency, the maintenance of the e-CODEX building blocks, the extension to other countries, stakeholder/community management and R&D. The support for other cross border legal procedures than those already supported by e-CODEX will require different projects. These projects can of course count on the operational management of Me-CODEX"*, available at: https://www.e-codex.eu/sites/default/files/newsletter/newsletter_2016-6.html.

[lxv] For more information on SIRIUS, see the answer given by the Commission to the written question E-007204/2017: *" [i]n light of the increasingly greater number of requests for operational support received from Member States, the EU Internet Referral Unit (EU IRU) at Europol recently launched SIRIUS to support online law enforcement investigation. SIRIUS provides a secure environment covering information related to Online Service Providers (OSPs) with manuals, tips, forums, questions & answers — as well as law enforcement developed tools to support Internet-based investigations. It provides guidance, amongst others, to investigators on the type of data that can be directly retrieved from their services.*

The information contained within SIRIUS does not include personal data, or requests for deletion of user accounts. SIRIUS is a capacity-building tool fostering knowledge exchange. Currently, 372 law enforcement representatives from EU Member States are members of SIRIUS and are making use of the guidelines on 19 OSPs as well as of the 13 tools which (contributed by the EU IRU and EU Member States) to support Internet-based investigations.

The EU IRU remains committed to flagging terrorist content to host platforms. To date, the EU IRU has assessed in total 42 066 pieces of content, which triggered 40 714 decisions for referral across over 80 platforms in more than 10 languages".

[lxvi] Explanatory Memorandum of the proposed Regulation, p. 19.

[lxvii] See Council general approach 15292/18, footnote 33, p. 36.

[lxviii] Article 22 of the proposed Regulation and Article 6 of the proposed Directive.

[lxix] See for instance Regulation (EU) No 1215/2012 of the European Parliament and of the Council, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1, specifically Articles 75 and 81, where the obligations for communication of information had to be fulfilled one year before the date of application of the other provisions of the Regulation.

Under Article 4(12) GDPR and Article 3(11) of the Law Enforcement Directive, a personal data breach is defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

[lxx] See Article 11 of the proposed Regulation.

[lxxi] See http://www.ejtn.eu/Documents/About%20EJTN/Criminal%20Justice%202017/CJSWG%20meeting%20Brussels%2013-14%20March%202017/COMMON%20CONCLUSIONS%20EJTN%20Barcelona%20seminar.pdf

[lxxii] See the list of grounds to object mentioned under Article 14 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).

[lxxiii] See Fundamental Rights Agency, Opinion on the draft Directive regarding the European Investigation Order, 14 February 2011, p. 10. *"In general, EU secondary law must comply with fundamental rights standards. See CJEU, joined cases C-92 and 93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, where the CJEU struck down a piece of EU secondary law for non-compliance with fundamental rights"*.

[lxxiv] "*See, Article 70 TFEU*".

[lxxv] "*The EU asylum system where primary law establishes the principle that EU Member States shall regard each other as 'constituting safe countries of origin' still allows to deviate from this presumption in order to ensure that fundamental rights of an individual can be taken into account in exceptional cases. See the sole Article (d) of Protocol 24 to the Treaties*".

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

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

[lxxviii] Recital 35c of the Council general approach seems to justify this limitation with the following reasoning : "*As opposed to non-content data, content data is of particularly sensitive nature because persons may reveal their thoughts as well as sensitive details of their private life. This justifies a different treatment and an involvement of the authorities of the enforcing State early on in the procedure"*. In this regard, the EDPS would like to recall that as stated in his pleading at the joint hearing in Case C-623/17 (Privacy International) with joined Cases C-511/18 and C-512/18 (La Quadrature du Net and Others) and Case C-520/18 (Ordre des barreaux francophones et germanophone and Others), "*[o]ther data relating to electronic communications – so-called metadata (...) can be as revealing as the actual contents of the communication*.". "*We should also keep in mind that the distinction between "content" and "metadata" is not clear-cut in a multiple service environment as the Internet. This is why in the context of the proposal for the ePrivacy Regulation, the EDPS advised to attribute a high level of protection to metadata, as well as to content data*", see EDPS pleading note (pp. 4-5), available on the EDPS website: https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-cases-c-62317_en

[lxxix] Impact assessment, p. 14: *"Requests for non-content data outnumber those for content within the EU and beyond. Non-content data from electronic communications is most commonly requested"*.

[lxxx] See Article 7a.

[lxxxi] See footnote 32, p. 34 of the Council general approach on the proposed Regulation: "*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"*.

[lxxxii] The issue has been also raised by ECHR Judge Prof. Dr. Bošnjak, in his personal capacity, at the e-evidence hearing held by the LIBE Committee of the European Parliament on 27 November 2018 (especially 16.55-16.58 explicitly on the issue - "A*s far as the law of the enforcing state is concerned it seems to be of no relevance according to the existing proposal. From the point of view of the Convention this can create a problem because the High Contracting Parties to the ECHR, including all 28 MS EU, are responsible for protection of human rights on the territory under its jurisdiction They have to put in place a regulatory framework and also guarantee legal, if no judicial, protection in particular cases. [...] If the authorities of the enforcing state are faced with a complaint that the protection of Convention right has been manifestly deficient and this cannot be remedied by EU law, they cannot refrain from examining the complaint on the ground the they are just applying EU law. This has clearly been stated in the judgement of Avotinš v. Latvia and has been confirmed later on in a number of instances. The proposal, as it is before you, creates a rather unique situation from the point of ECHR jurisprudence. Namely the interferences with Article 8 are without any involvement of the authorities of the enforcing state. I wonder, whether this is in line with the ECHR because there might be a legitimate expectation that the law of the enforcing state would apply in each and every particular situation. This would of course affect the assessment of lawfulness..."*, available at http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEELIBE.

[lxxxiii] Except for those offences which are defined at EU level, listed under Article 5 (4) (b) of the proposed regulation.

[lxxxiv] EDPB Opinion 23/2018, section 2, point b).

[lxxxv] See also ECHR Judge Prof. Dr. Bošnjak's presentation, in his personal capacity, at the e-evidence hearing held by the LIBE Committee of the European Parliament on 27 November 2018 (footnote 82 *supra*).
[lxxxvi] See section 3.2 of this Opinion.
[lxxxvii] See EDPS Opinion 2/2019, par. 28, and EDPS Opinion 3/2019, par. 53.
[lxxxviii] Impact Assessment, p. 37.
[lxxxix] Recital 36.
[xc] Recital 19 of the proposed Regulation: *"This Regulation regulates gathering of stored data only, that is, the data held by a service provider at the time of receipt of a European Production or Preservation Order Certificate. It does not stipulate a general data retention obligation, nor does it authorise interception of data or obtaining to data stored at a future point in time from the receipt of a production or preservation order certificate".*
[xci] Article 5(1)(e) GDPR and Article 4(1)(e) of the Law Enforcement Directive.
[xcii] This is the case where the data is preserved if the service provider who received an EPOC does not produce the data immediately.
[xciii] EDPB Opinion 23/2018, section 7, point d) European preservation orders shall not be used to circumvent data retention obligations of the service providers.
[xciv] See Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final (hereinafter "proposed ePrivacy Regulation").
[xcv] Article 12b(3).
[xcvi] For instance, Facebook, Google, Microsoft, Twitter and Apple; see Impact Assessment, p. 14.
[xcvii] For instance, a similar provision is included in Article 8 of the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)640 final).
[xcviii] Article 5 lays down the conditions for issuing EPO. The wording of the provision lacks however of clarity: Article 5(7) provides that *"[i]f the issuing authority has reasons to believe that, transactional or content data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, [it] has to seek clarification before issuing the [EPO], including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network"*. Furthermore, *"[i]f the issuing authority finds that the requested access, transactional or content data is protected by such immunities and privileges (...), it shall not issue the [EPO]"* [emphasis added].
[xcix] See Article 5(7) of the Council general approach.
[c] It seems that this ground for objection is also available for EPO-PR.
[ci] See Explanatory Memorandum of the proposed Regulation, p. 21: *"[s]hould the procedure for enforcement be initiated, the addressee itself will be able to oppose the Order before the enforcing authority. The addressee may do this on the basis of any of such grounds, excluding immunities and privileges"*.
[cii] See Article 7a of the Council general approach. The provision sets only a possibility for the competent authority in the enforcing State to inform the issuing authority (and not an obligation).
[ciii] Article 18 provides that *"the court in the issuing State shall ensure during the criminal proceedings for which the Order was issued that these grounds are taken into account in the same way as if they were provided for under their national law when assessing the relevance and admissibility of the evidence concerned. The court may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust"*.
[civ] In the Council general approach, it has been limited to situations where the data subject does not reside in the issuing State (Article 12a).
[cv] The Council general approach provides only for the power but not the obligation of the issuing authority to request the authorities of the enforcing State to exercise their power to waive the privilege or immunity (Article 5(8)).
[cvi] Such ground exists under Article 11 of the EIO Directive.
[cvii] EDPB Opinion 23/2018, section 5, point b) Legal representative, p. 11.
[cviii] The Explanatory Memorandum of the proposed Directive states on p. 3 that: *"[t]he obligation to designate a legal representative for service providers not established in the EU but offering services in the EU already exists in certain acts of EU law applicable in particular fields, e.g. in the General Data Protection Regulation (EU) 2016/679 (Article 27) and in Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (Article 18). The Commission proposal for an ePrivacy Regulation also contains such an obligation (Article 3)"*. The Explanatory Memorandum (p. 5) also suggests that the legal representatives appointed under the proposed Directive may accumulate other functions, including those of representatives under the GDPR and the ePrivacy Proposal. In addition, Recital 6 of the proposed Directive refers to the GDPR and the obligation therein to designate a legal representative in the Union under certain conditions. Furthermore, the Impact Assessment (p. 91) states that the legal representative appointed under the proposed Directive *"could cover several functions (e.g. GDPR, ePrivacy and EPO), reducing the costs"* for service providers.
[cix] In this respect, the Article 29 Working Party pointed out in its Statement on Data protection and privacy aspects of cross-border access to electronic evidence that "*[w]hile the legal representative under the GDPR is meant to be the contact point of the Supervisory Authorities of the controllers or processors for the performance of their obligations,*

the representative under the envisaged measure aims to enforce the production order issued by the competent authority".

[cx] Under the proposed Directive, the obligation to designate a legal representative is imposed on all service providers offering services in the Union within the meaning of the Proposal (Article 2(3) in conjunction with Recital 13), whether or not they are established in the Union.
Under the GDPR (Article 3(2) combined with Article 27), the obligation to designate a representative is imposed on controllers or processors which do not have an establishment in the Union but are processing "*personal data of data subjects who are in the Union*" and the processing activities are related to either the offering of goods or services or to "*the monitoring of the behaviour*" of the above mentioned data subjects "*as far as their behaviour takes place within the Union*" [emphasis added]. Moreover, Article 27(2) GDPR provides an exemption to this obligation for "*processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing" or for "a public authority or body*".

[cxi] Article 9 sets time limits to comply with EPOCs. The requested data must be transmitted "*at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure"*. In addition, the proposed Regulation provides that *"[i]n emergency cases the addressee shall transmit the requested data without undue delay, at the latest within 6 hours upon receipt of the EPOC"*. For EPOC-PR, the addressee shall preserve the data or contact the issuing authority if the certificate cannot be complied with, without undue delay upon receipt of the certificate (Article 9(2)). Emergency cases are defined in Article 2(15) as *"situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC"*.

[cxii] Article 12(3) of the EIO Directive.

[cxiii] Article 12(4) of the EIO Directive.

[cxiv] Article 13 of the proposed Regulation imposes on Member States to lay down pecuniary sanctions in their national legislation which are *"effective, proportionate and dissuasive"* for cases of non-compliance with an order. In cases of non-compliance with an order, Article 14(3) provides that the enforcing authority shall inform the addressee of the possibility to raise the objections listed in Article 14(4) and (5) and also remind of the applicable sanctions in cases of non-compliance.

[cxv] Such sanctions should in any event not be imposed on addressees which oppose an order because they believe in good faith that it violates the EU Charter.

[cxvi] It covers "any service which provides to users thereof the ability to send or receive wire or electronic communications" (18 U.S.Code § 2510(15)).

[cxvii] See new subsection (i) as inserted in Chapter 119 « Wire and electronic communications interception and interception of oral communications » of USC Title 18 by the US CLOUD Act.

[cxviii] Articles 15 and 16 of the proposed Regulation. Explanatory Memorandum of the proposed Regulation, p. 21*:"[b]y setting a high standard, [these provisions] aim to encourage third countries to provide for a similar level of protection. In the opposite situation, where authorities of a third country seek to obtain data of an EU citizen from an EU service provider, Union or Member States laws protecting fundamental rights, such as the data protection acquis, may similarly prevent disclosure. The European Union expects third countries to respect such prohibitions as this proposal does*".

[cxix] Council documents 9114/19 and 9116/19, available at https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[cxx] Addendum to the Decision, point I. 1, Council document 9666/19.

[cxxi] Addendum to the Decision, point II.1. (a), Council document 9664/19.

[cxxii] This provision states that « this Regulation does not affect EU and other international instruments, agreements and arrangements on the gathering of evidence that would also fall within the scope of the Regulation ».