Council of the European Union
General Secretariat

Interinstitutional files:
2018/0107 (COD)
2018/0108 (COD)

Brussels, 09 September 2022

WK 11280/2022 INIT

LIMITE

CYBER
JAI
COPEN
ENFOPOL
TELECOM
EJUSTICE
MI
DATAPROTECT

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	E-Evidence - Internal rules - Examination of the Presidency note

During the last months, the four-column-tables describing the state of play of the draft Regulation and the draft Directive, respectively, have been discussed in a number of informal meetings with the negotiations team of the EP. Since no further changes in the tables have been agreed, reference is given to the version previously issued in July.

In order to account for the latest developments, delegations will in Annex instead find two indicative consolidated texts of the Regulation (Annex 1) and of the Directive (Annex 2). The texts take into account the written comments received from delegations[1] following the informal COPEN meeting of 18 July. Modifications in relation to the General Approach are indicated in **bold** and strikethrough, and explanations and comments can be found in the footnotes. It is the hope of the Presidency that these documents will facilitate the preparation of delegations for the COPEN meeting on 13 September. To facilitate the understanding of the documents, the Presidency would draw the attention of delegations to two technical aspects:

- The recital parts of the documents are of a very preliminary nature. The fact that the recitals to a large extent reproduce suggestions made by the EP is due to a wish to simplify the reading of the documents and does not in any way imply that the Presidency has the intention to follow these suggestions. It should also be underlined that some of the positions of the EP referred to in the Annex have been communicated in a purely informal manner to the Presidency and have not been formally confirmed.
- The numbering of a limited number of the provisions in the documents has been modified slightly, in order to ensure coherence of the text.

Delegations are invited to consider the content of the documents in annex in view of the informal (videoconference) COPEN meeting on 13 September and indicate what parts of the text they absolutely cannot agree with as part of a global compromise on the legislative package. The Presidency will base its positions in the upcoming negotiations in technical trilogues on the input thereby received by delegations.

[1] See WK 1181/2022.

To facilitate the reading, the Presidency wishes to draw the particular attention to a few issues of particular interest in the Regulation table:

- Article 4 (1) (b) second subparagraph–This solution has been proposed by the EP in order to solve problems of some Member States, which might arise from their national legislation. Based on the received comments, the Presidency is of the opinion, that this provision should be deleted.
- Article 5(6c) line 205 - Some Member States expressed concerns about the protection of professional secrecy. Member States are invited to reflect on what scope of flexibility they have on the formulation of a compromise solution.
- Some Member States are concerned about the newly proposed residence criterion. This matter is still being discussed with the EP, who has a very strong position on this matter. The EP insist on a definition of residence, which would be based on objective criteria. The EP also insists on the inclusion of the importance of a ”registration“ in a Member State, despite the efforts of the Presidency to explain that a formal registration is not necessary to reside in many of the Member States. The Presidency therefore asks the Member States, if they could consider, in spirit of an overall compromise, to include a list of objective criteria for residence (as included in the recital 35d) and if they could accept a reference to a timeframe with regard to the registration (e. g. 6 months).
- Article 9 (2b), line 277 - Member States seem to be divided in their opinions on the inclusion of this mechanism. Member States are invited to reflect on the exact limits of involvement of “the addressee” they could accept.
- Article 10a (1) Grounds for refusal – The Presidency understands and fully agrees that grounds for refusal should be optional. However, the current wording of this provision is a result of a delicate preliminary political compromise. Could the Member States accept this wording, if it is clarified in the recitals that the grounds for refusal are *de facto* optional?
- It is clear to the Presidency that the Council does not support suspensive effect in emergency cases. We will therefore continue the negotiations with the EP in order to achieve that such an effect will not be provided for. However, as it is likely that EP will insist on this point, would – as a possible compromise - a solution strengthening the obligations of the issuing authority to justify the emergency be envisagable?

- Recitals 11, 11a, Article 9(2a) – Could the Member States accept a link to Article 7 TEU, if it would not imply an automatic possibility to refuse the execution of orders from the affected Member State(s) as suggested by the EP, but only an obligation to take the situation into account?

Proposal for

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European Production and Preservation Orders for electronic evidence in criminal matters[2]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Union has set itself the objective of maintaining and developing an area of freedom, security and justice. For the gradual establishment of such an area, the Union is to adopt measures relating to judicial cooperation in criminal matters based on the principle of mutual recognition of judgments and judicial decisions, which is commonly referred to as a cornerstone of judicial cooperation in criminal matters within the Union since the Tampere European Council of 15 and 16 October 1999.

---

2 Netherlands, Finland, Czech Republic and Latvia have a reservation on the entire compromise text. As regards Netherlands this reservation relates inter alia to Articles 5, 6, 7a, 11(3), 12a, 12b, 14 and 17.

3 OJ C , , p. .

(2) Measures to obtain and preserve electronic evidence are increasingly important to enable criminal investigations and prosecutions across the Union. Effective mechanisms to obtain electronic evidence are **essential**~~of the essence~~ to combat crime, subject to conditions **and safeguards** to ensure full **compliance**~~accordance~~ with fundamental rights and principles recognised in **Article 6 of the Treaty on European Union (TEU) and** the Charter of Fundamental Rights of the European Union **(`the Charter´)** ~~as enshrined in the Treaties~~, in particular the principles of necessity and proportionality, due process, ~~data~~ protection **of**, ~~secrecy of correspondence and~~ privacy **and personal data and confidentiality of communications**. [4]

(3) The 22 March 2016 Joint Statement of the Ministers of Justice and Home Affairs and representatives of the Union institutions on the terrorist attacks in Brussels stressed the need, as a matter of priority, to find ways to secure and obtain electronic evidence more quickly and effectively and to identify concrete measures to address this matter.

(4) The Council Conclusions of 9 June 2016 underlined the increasing importance of electronic evidence in criminal proceedings, and of protecting cyberspace from abuse and criminal activities for the benefit of economies and societies, and therefore the need for law enforcement and judicial authorities to have effective tools to investigate and prosecute criminal acts related to cyberspace.

(5) In the Joint Communication on Resilience, Deterrence and Defence of 13 September 2017[5], the Commission emphasised that effective investigation and prosecution of cyber-enabled crime was a key deterrent to cyber-attacks, and that today's procedural framework needed to be better adapted to the internet age. Current procedures at times could not match the speed of cyber-attacks, which create particular need for swift cooperation across borders.

(6) The European Parliament echoed these concerns in its Resolution on the fight against cybercrime of 3 October 2017[6], highlighting the challenges that the currently fragmented legal framework can create for service providers seeking to comply with law enforcement requests and calling on the Commission to put forward a Union legal framework for electronic evidence with sufficient safeguards for the rights and freedoms of all concerned.

---

4 Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council.

5 JOIN(2017) 450 final.

6 2017/2068(INI).

(7) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the relevant country **where the service is offered. Therefore,** ~~. As a consequence,~~ relevant **electronic** evidence is often stored outside of the investigating State or by a service provider established outside of this State**, creating challenges regarding the gathering of electronic evidence in criminal proceedings**. ~~Frequently, there is no other connection between the case under investigation in the State concerned and the State of the place of storage or of the main establishment of the service provider.~~ [7]

(8) Due to this lack of connection[8], judicial cooperation requests are often addressed to states which are hosts to a large number of service providers~~, but which have no other relation to the case at hand~~. Furthermore, the number of requests has multiplied in view of increasingly used networked services~~that are borderless by nature~~. **Directive 2014/41/EU of the European Parliament and of the Council provides for**[9] **the acquisiting, access and production of evidence in one Member State for criminal investigation and proceedings in another Member State. However, the procedures and timeslines foreseen in the EIO might not be appropriate for electronic evidence, which is more volatile and could more easily and quickly be deleted.** As a result, obtaining electronic evidence using judicial cooperation channels often takes a long time, **resulting in situations where —** ~~longer than~~ subsequent leads **might no longer** ~~may~~ be available. Furthermore, there is **harmonised** ~~no clear~~ framework for cooperation with service providers, while certain third-country providers accept direct requests for non-content data as permitted by their applicable domestic law. As a consequence, all Member States **increasingly** rely on **voluntary direct**~~the~~ cooperation channel**s** with service providers where available, **applying**~~using~~ different national tools, conditions and procedures. ~~In addition, f~~**F**or content data, some Member States have taken unilateral action, while others continue to rely on judicial cooperation. [10]

---

7 Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council.

8 The words ”lack of connection” have been kept due to a suggestion from lawyer linguists (“JL”).

9 JL suggestion: say “**possibility of issuing a European Investigation Order (EIO) for the purpose of gathering evidence” here, considering that the terms “acquisition, access and production” do not figure int the EIO.**

10 Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council.

(9) The fragmented legal framework creates challenges for **law enforcement, judicial authorities and** service providers seeking to comply with ~~law enforcement~~**legal** requests, **as they are increasingly faced with legal uncertainty and, potentially, conflicts of law.** Therefore there is a need to put forward **specific rules as regards cross-border judicial cooperaiton for preserving and producing** a ~~European legal framework for~~ electronic evidence**, addressing the specific nature of electronic evidence, including** ~~to impose~~ an obligation on service providers covered by the scope of the instrument to respond directly to **requests stemming from** authorities ~~without systematic the involvement of a judicial authority~~ in **another**~~the~~ Member State~~of the service provider in every case.~~ **With this, this Regulation complements the existing Union law and clarifies the rules of the cooperation between law enforcement, judicial authorities and service providers in the field of electronic evidence, while ensuring full compliance with fundamental rights.**[11]

(10) Orders under this Regulation should be addressed **directly to the designated establishment or** to **the** legal representatives **designated by**~~of~~ **the** service provider ~~designated~~ for that purpose **pursuant to Directive XXXX/XXX**. **Exceptionally, in emergency cases as defined in this Regulation**, **where the designated establishment or the legal representative of** ~~If~~ a service provider **does not reacht to an EPOC or an EPOC-PR within the deadlines, it should be possible to address thet EPOC or EPOC-PR may** ~~established in the Union has not designated a legal representative, the Orders can~~ be ~~addressed~~ to any **other** establishment **or legal representatives** of th~~e~~**is** service provider in the Union. ~~This fall-back option serves to ensure the effectiveness of the system in case the service provider has not (yet) nominated a dedicated representative.~~ [12]

---

11 Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council.

12 Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council. The wording of the EP has been slightly adapted following suggestions from JL.

(10a) This Regulation respects fundamental rights and observes the principles recognised by Article 6 TEU and the Charter, by international law and international agreements to which the Union or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in Member States' constitutions, in their respective fields of application. Such rights and principles include, in particular, the right to liberty and security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of legality and proportionality, as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence.

(10b) Nothing in this Regulation should be interpreted as prohibiting the refusal to execute a European Production Order where there are reasons to believe, on the basis of objective elements, that the European Production Order has been issued for the purpose of prosecuting or punishing a person on account of the person's gender, racial or ethnic origin, religion, sexual orientation or gender identity, nationality, language or political opinions, or that the person's position may be prejudiced for any of those reasons. [13]

[13] Most of the changes in this recital have been proposed by the EP and have not been discussed in or agreed by Council.

(11) The mechanism of the European Production Order and the European Preservation Order for electronic evidence in criminal matters **rely** ~~can only work~~ on the **principle**~~basis of a high level~~ of mutual trust between the Member State **and a presumption of compliance by Member States with** ~~which is an essential precondition for the proper functioning of this instrument.~~**Union law, the rule of law and, in particular, with fundamental rights, which are essential elements of the area of freedom, security and justice within the Union. This mechanism enables national competent authorities to send directly these orders to service providers. In that context, where the enforcing judicial authority is notified of an order for traffic data, except for data requested for the sole purpose of identifying the user, or for content data, it should examine whether it is appropriate to raise a ground for refusal, where, in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of a European Production Order or a European Preservation Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter.**[14]

14 **PL** has noted that the wording of this recital, in both versions visible here, is unacceptable. **BE, NL, FR** and others have noted that they support the current wording. **IE** and **ES** have noted that the previous wording also needs to be analysed carefully in order to imply a duty to analyse every order.

(11a) In particular, when assessing this ground for refusal, where the enforcing authority has at its disposal in particular evidence or material such as that set out in a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission adopted pursuant to Article 7(1) TEU, indicating that there is a clear risk, if the order were executed, of a serious breach of the fundament right to an effective remedy and to a fair trial guaranteed by Article 47(2)[15] of the Charter of Fundamental rights of the European Union, on account of systemic or generalised deficiencies as concerns the independence of the issuing Member State's judiciary, of the enforcing judicial authority should determine specifically and precisely whether, having regard to the concerned person's personal situation, as well as to the nature of the offense for which the criminal proceedings are conducted, and the factual context that forms the basis of the Order, and in the light of the information provided by the issuing Member State, there are substantial grounds for believing that that person will run such a risk of breach of his/her right to a fair trial[16].

[…]

(11c) The respect for private and family life and the protection of natural persons regarding the processing of personal data are fundamental rights. In accordance with Articles 7 and 8(1) of the Charter, everyone has the right to respect for his or her private and family life, home and communications and to the protection of personal data concerning them. When implementing this Regulation, Member States should ensure that personal data are protected and processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[4] and Directive (EU) 2016/680 of the European Parliament and of the Council[5], as well as Directive 2002/58/EC of the European Parliament and of the Council[6].

---

15 **DE** has questioned why the reference is limited to this Article only, as Articles 7 or 8 are also relevant.

16 The EP has suggested the following text for recital 11a: "If the European Council were to adopt a decision determining, as provided for in Article 7(2) TEU, that there is a serious and persistent breach in the issuing Member State of the principles set out in Article 2 TEU, such as those inherent in the rule of law, the executing judicial authority may decide automatically to raise one of the grounds for refusal provided for in this Regulation, without having to carry out any specific assessment**". DE** has noted that this wording may be too broad.

(11d) Personal data obtained under this Regulation should only be processed when necessary and in a manner that is proportionate to the purposes of prevention, investigation, detection and prosecution of crime or enforcement of criminal sanctions and the exercise of the rights of defence. In particular, Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers for the purposes of this Regulation, including measures to ensure the security of the data. Service providers should ensure that the same safeguards apply for the transmission of personal data to relevant authorities. Only authorised persons should have access to information containing personal data.

(12) [This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. These include the right to liberty and security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of the legality and proportionality, as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence.[17]]

(12a) In case, the issuing Member State has indications that parallel criminal proceedings may be ongoing in another Member State, it **should**~~shall~~ consult the authorities of this Member State in accordance with Council Framework Decision 2009/948/JHA[18]. In any case, a European Production Order **or European Preservation Order** should not be issued, if the issuing Member State has indications that this would be contrary to the ne bis in idem principle.

(13) [In order to guarantee full respect of fundamental rights, this Regulation explicitly refers to the necessary standards regarding the obtaining of any personal data, the processing of such data, the judicial review of the use of the investigative measure provided by this instrument and the available remedies.[19]]

---

17 This text has, as suggested by EP, tentatively been reproduced in recital 10a above. The Presidency considers it possible to delete this recital.

18 Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009, p. 42).

19 This text has, as suggested by EP, tentatively been reproduced in recital 10a above. The Presidency would prefer to keep this recital in the GA version.

(14) ~~This Regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in Directives 2010/64/EU[20], 2012/13/EU[21], 2013/48/EU[22], 2016/343[23], 2016/800[24] and 2016/1919[25] of the European Parliament and of the Council.~~ **The procedural rights in criminal proceedings set out in Directives 2010/64/EU[7], 2012/13/EU[8], 2013/48/EU[9], 2016/343[10], 2016/800[11] and 2016/1919[12] of the European Parliament and of the Council should apply, within the scope of those Directives, to criminal proceedings covered by this Regulation as regards the Member States bound by those Directives. The procedural safeguards under the Charter apply to all proceedings covered by this Regulation.**

(14a) In order to guarantee full respect of fundamental rights, the probatory value of the evidence gathered in application of this Regulation should be assessed in trial by the competent judicial authority, in accordance with national law and in compliance with, notably, the right to a fair trial and the right of defence.

---

20 Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings (OJ L 280, 26.10.2010, p. 1).

21 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ L 142, 1.6.2012, p. 1).

22 Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).

23 Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (OJ L 65, 11.3.2016, p. 1).

24 Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132, 21.5.2016, p. 1).

25 Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297, 4.11.2016, p. 1).

(15) This instrument **should** lay down the rules under which**, in a criminal proceeding,** a competent judicial authority in the European Union may order a service provider offering services in the Union to produce or preserve electronic evidence through a European Production or Preservation Order. This Regulation **should apply to** ~~is applicable in~~ all **cross-border** cases where the service provider is [**has its designated establishment or legal representative** ~~established or represented~~ in another Member State. ~~For domestic situations where the instruments set out by this Regulation cannot be used, the Regulation should not limit the powers of the national competent authorities already set out by national law to compel service providers established or represented on their territory.~~] [26]

(16) The service providers most relevant for criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Providers of electronic communications services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services.
This Regulation should also be applicable to other information society service~~s~~ providers within the meaning of Directive (EU) 2015/1535 that do not qualify as electronic communications service~~s~~ providers, but offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf. This should be in line with the terms used in the Budapest Convention on cybercrime. Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, i.e. technical operations to produce or alter data by means of computer processing power. The categories of service providers included here are, for example online marketplaces providing consumers and businesses the ability to communicate with each other and other hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms.

---

26 The provision has been slightly adapted due to remarks of JL. The deleted text has, as suggested by EP, tentatively been reproduced in recital 10a above. The Presidency intends to keep/add: „For domestic situations where the instruments set out by this Regulation cannot be used, the Regulation should not limit the powers of the national competent authorities already set out by national law to compel service providers established or represented on their territory".

Where an information society service provider does not provide its users the ability to communicate with each other, but only with the service provider, or does not provide the ability to process or to store data, or where the ability to store/process data is not an essential part of the service provided to users, such as legal, architectural, engineering and accounting services provided online at a distance, it would not fall within the scope of the definition, even if within the definition of information society services pursuant to Directive (EU) 2015/1535.[27]

(17) [In many cases, data is no longer stored or processed on a user's device but made available on cloud-based infrastructure for access from anywhere. To run those services, service providers do not need to be established or to have servers in a specific jurisdiction. Thus, the application of this Regulation should not depend on the actual location of the provider`s establishment or of the data processing or storage facility.][28]

(18) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and privacy and proxy service providers, or regional internet registries for internet protocol ('IP') addresses, are of particular relevance when it comes to the identification of actors behind malicious or compromised web sites. They hold data that **could** ~~is of particular relevance for criminal proceedings as it can~~ allow for the identification of an individual or entity behind a web site used in **a** criminal activity, or the victim of **a** criminal activity ~~in the case of a compromised web site that has been hijacked by criminals~~[29].

(19) This Regulation regulates gathering of ~~stored~~ data **stored by a service provider** ~~only, that is, the data held by a service provider~~ at the time of receipt of a European Production or Preservation Order Certificate **only**. It does not stipulate a general data retention obligation **for service providers and it should not have the effect of resulting in any general and indiscriminate retention of data. The Regulation also does not** ~~, nor does it~~ authorise interception of data or obtaining to data stored at a future point ~~in time~~ from the receipt of a **European** production or preservation order certificate. ~~Data should be provided regardless of whether it is encrypted or not.~~ [30]

---

27 EP has kindly invited Council to consider if changes are needed in this recital. The Presidency intends to suggest to stick to the GA version.

28 EP considers that this text is covered by recitals 7 and 10 above.

29 The changes in the text have been proposed by EP but have not been discussed in Council.

30 The changes in the text have been proposed by EP but have not been discussed in Council. **BE, NL** and **ES** have noted their opposition to any reference to data retention and encryption.

(19a) The application of this Regulation should not affect the use of encryption by service providers or their users. Data sought by means of a European Production or Preservation Order should be provided or preserved regardless of whether it is encrypted or not. However, this Regulation does not stipulate any obligation for service providers to decrypt data.[31]

(20) The categories of data **which** this Regulation covers include subscriber data, **traffic** ~~access~~ data~~, transactional data (these three categories being referred to as 'non-content data'~~ and content data. **Such categorisation would be in line with the** ~~This distinction, apart from the access data, exists in the legal~~ laws of many Member States**, Union law such as Directive 2002/58/ES and the case law of the Court of Justice, as well as internationall law, notably the Convention on Cybercrime of the Council of Europe (CETS No.185)(´Budapest Convention´).** ~~and also in the current US legal framework that allows service providers to share non-content data with foreign law enforcement authorities on a voluntary basis.~~

(21) [It is appropriate to single out access data as a specific data category used in this Regulation. Access data is pursued for the same objective as subscriber data, in other words to identify the underlying user, and the level of interference with fundamental rights is similar to that of subscriber data. Access data is typically recorded as part of a record of events (in other words a server log) to indicate the commencement and termination of a user access session to a service. It is often an individual IP address (static or dynamic) or other identifier that singles out the network interface used during the access session. If the user is unknown, it often needs to be obtained before subscriber data related to that identifier can be ordered from the service provider.][32]

(22) [Transactional data, on the other hand, is generally pursued to obtain information about the contacts and whereabouts of the user and may be served to establish a profile of an individual concerned. That said, access data cannot by itself serve to establish a similar purpose, for example it does not reveal any information on interlocutors related to the user. Hence this proposal introduces a new category of data, which is to be treated like subscriber data if the aim of obtaining this data is similar.][33]

---

31 Recital proposed by EP.

32 Deletion suggested by EP, with reference to a new recital 22a.

33 Deletion suggested by EP, with reference to a new recital 22b.

(22a) **IP addresses as well as access numbers and related information can constitute a crucial starting point for criminal investigations in which the identity of a suspect is not known. They are typically part of a record of events (in other words a server log) to indicate the commencement and termination of a user access session to a service. It is often an individual IP address (static or dynamic) or other identifier that singles out the network interface used during the access session. Related information on the commencement and termination of a user access session to a service such as the source ports and time stamp are needed as IP addresses are often shared amongst users, e.g. where carrier grade network address translation (CGN) or *technical equivalents* are in place. However, according to the EU acquis as interpreted by the European Court of Justice, IP addresses are to be considered personal data and have to benefit from the full protection under the EU data protection acquis. In addition, under certain circumstances, they can be considered traffic data. Also, access numbers and related information are considered traffic data in some Member States. However, for the purpose of a specific criminal investigation, law enforcement authorities might have to request an IP address as well as access numbers and related information for the sole purpose of identifying the user before subscriber data related to that identifier can be ordered from the service provider. In such cases, it is appropriate to apply the similar regime as for subscriber data, as defined under this Regulation.**

(22b) **[Where IP addresses, access numbers and related information are not requested for the sole purpose of identifying the user in a specific criminal investigation, it is generally pursued to obtain more privacy-intrusive information, such as the contacts and whereabouts of the user and could servee to establish a comprehensive profile of an individual concerned, while it can be processed and analysed more easily than content data, as it is already brought into a structured and standardised format. It is therefore essential that, in such situations, they are to be treated as traffic data and requested under the similar regime as for content data, as defined under this Regulation.]**[34]

34 New recital suggested by EP.

(23) All data categories contain personal data, and are thus covered by the safeguards under the Union data protection *acquis*. **However,**~~but~~ the intensity of the impact on fundamental rights varies **between the categories**, in particular between subscriber data **as well as IP addresses, access numbers and related information, where requested for the sole purpose of identifying the user** ~~and access data on the one hand and transactional data and content data on the other hand. While subscriber data and access data are~~ **could be** useful to obtain first leads in an investigation about the identity of a suspect, **traffic** ~~transactional~~ and content data are the most relevant as probative material. It is therefore essential that all these data categories are **often more relevant as probatory material, which could finally lead to a conviction of the suspect.**~~covered by the instrument~~. **It is therefore essential that all these data categories are covered by the instrument.** Because of the different degree of interference with fundamental rights, different **safeguards and** conditions are imposed for obtaining **such** ~~subscriber and access~~ data~~on the one hand, and transactional and content data on the other~~.[35]

(24) The European Production Order and the European Preservation Order are investigative measures that should be issued only in the framework of specific criminal proceedings **concerning** ~~against the specific known or still unknow perpetrators of~~ a concrete criminal offence that has already taken place, after an individual evaluation of the proportionality and necessity in every single case, **taking into account the rights of the suspected or accused person**.[36]

(24a) As proceedings for mutual legal assistance may be considered as criminal proceedings in accordance with applicable national law in the Member States, it should be clarified that a European Production Order or a European Preservation Order should[37] not be issued to provide mutual legal assistance to another Member State or third country. In such cases, the mutual legal assistance request should be addressed to the Member State or third country which can provide mutual legal assistance under its domestic law. ~~However, if electronic evidence had already been obtained under this Regulation by the issuing authority for its own criminal investigations or proceedings and afterwards this evidence is subject to transfer or transmission, the conditions on the speciality principle should apply.~~ [38]

---

35 New wording suggested by EP.

36 New wording suggested by EP.

37 JL suggestion: "it should be clarified that this Regulation should not apply to proceedings initiated by the issuing authority for the purpose of providing"

38 New wording suggested by EP.

(24b) This Regulation should apply to criminal proceedings initiated by the issuing authority in order to localise a convict that absconded from justice to execute custodial sentences or detention orders. However, in case the sentence or detention order was rendered in absentia it should not be possible to issue a European Production Order or a European Preservation Order as national law of the Member States on judgments in absentia vary considerably throughout the European Union.[39]

(25) This Regulation is without prejudice to the investigative powers of authorities in civil or administrative proceedings, including where such proceedings can lead to sanctions.

(26) This Regulation should apply to service providers offering services in the Union, and the Orders provided for by this Regulation may be issued only for data pertaining to services offered in the Union. Services offered exclusively outside the Union are not in the scope of this Regulation~~, even if the service provider is established in the Union~~. [40]

(27) ~~The determination~~**Determening** whether a service provider offers services in the Union requires an assessment **of** whether **it is apparent that** the service provider **envisages offering services to data subjects, either** ~~enables~~ legal or natural persons, in one or more Member States **in the Union.** ~~to use its services.~~ However, the mere accessibility of an online interface as for instance the accessibility of the service provider's or an intermediary's website or of an email address **or** ~~and of~~ other contact details **of a service provider or an intermediary, or the use of a language also used in a Member State, should not be considered sufficient to ascertain such intention.** ~~in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.~~ [41]

---

[39] EP has noted that it could accept this recital, depending on the content of a general agreement on the package.

[40] EP has noted that it could accept this recital, depending on the content of a general agreement on the package.

[41] New wording suggested by EP.

(28) A substantial connection to the Union should also be relevant to determine the ambit of application of the present Regulation. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be bas~~is~~ed on specific factual criteria such as a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States **should**[42] ~~can~~ be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. [The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.[43] On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302[44] cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union]**[45]**.

---

42 Note from JL: this appears to introduce an obligation, which is however not mirrored in the operative part.

43 Regulation (EU) 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).

44 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (OJ L 601, 2.3.2018, p. 1).

45 EP considers that the part between brackets still need to be discussed.

(28a) Situations, where there is an imminent threat to life or physical integrity or safety of a person, should be treated as emergency cases and allow for shorter time limits on the service provider and the executing authority. Where the disruption or destruction of a critical infrastructure as defined in Council Directive 2008/114/EC would imply such a threat, including through a serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State, such a situation should also be treated as an emergency case, in accordance with Union law.[46]

(29) A European Production Order should only be issued if it is necessary and proportionate. **It should take into account the rights of the suspected or accused person in a proceeding relating to a criminal offence. It should only be issued if it could have been ordered under the same conditions in a similar domestic case and if its execution seems proportionate, adequate and applicable to the case in hand.**The assessment should take into account whether the Order is limited to what is **strictly** necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the individual case only~~, taking due account of the impact of the measure on fundamental rights of the person whose data are sought~~. **[47]**

46 New recital proposed by EP. It has not been discussed in Council.

47 New wording suggested by EP.

(30) When a European Production or Preservation Order is issued, there should always be a judicial authority involved either in the process of issuing or validating the Order. In view of the more sensitive character of **traffic data except for the sole purpose of identifying the user as defined in this Regulation** and content data, the issuing or validation of European Production Orders for production of these categories requires review by a judge. As subscriber and access data are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent **public** prosecutors, except where **in accordance with national law, the execution of an order requires the procedural involvement of a court in the enforcing State. In such situations, such Member State should make a corresponding declaration to the General Secretariat of the Council and to the Commission. In accordance with the right to a fair trial, as protected by the European Union Charter of fundamental rights and the European Convention on Human rights, public prosecutors exercise their responsibilities objectively, taking their decision solely on the basis of the factual elements in the [case file~~/order~~], and taking into account all incriminatory and exculpatory evidence**[48]**.**

---

48 EP has proposed the part "***in accordance with national law, the execution of an order requires the procedural involvement of a court in the enforcing State. In such situations, such Member State should make a corresponding declaration to the General Secretariat of the Council and to the Commission***.". **PL** has declared that this is unacceptable. As an alternative, the EP has suggested the following text in a second subparagraph: "*Where so provided by national law, the execution of the order might require the procedural involvement of a court in the executing State".* **NL** has warned against the complicated wording suggested by EP. **FR** calls for caution as this provision may depend on the substance of a global compromise. The Presidency intends to, in a spirit of compromise, keep the second suggested alternative.

(31) For the same reason, a distinction has to be made regarding the material scope of this Regulation: Orders to produce subscriber data and **IP addresses, access numbers and related information, where requested for the sole purpose of identifying the user** ~~access data~~ can be issued for any criminal offence, whereas access to transactional and content data should be subject to stricter requirements to reflect the more sensitive nature of such data. A threshold allows for a more proportionate approach, together with a number of other ex ante and ex post conditions and safeguards provided for in **this Regulation**~~the proposal~~ to ensure respect for proportionality and the rights of the persons affected. At the same time, a threshold should not limit the effectiveness of the instrument and its use by practitioners. Allowing the issuing of Orders for investigations that carry at least a three-year maximum sentence limits the scope of the instrument to more serious crimes, without excessively affecting the possibilities of its use by practitioners. It excludes from the scope a significant number of crimes which are considered less serious by Member States, as expressed in a lower maximum penalty. It also has the advantage of being easily applicable in practice. [49]

(32) There are specific offences where evidence will typically be available exclusively in electronic form, which is particularly fleeting in nature. This is the case for cyber-related crimes, even those which might not be considered serious in and of themselves but which may cause extensive or considerable damage, in particular including cases of low individual impact but high volume and overall damage. For most cases where the offence has been committed by means of an information system, applying the same threshold as for other types of offences would predominantly lead to impunity. This justifies the application of the Regulation also for those offences where the penalty frame is less than 3 years of imprisonment. Additional terrorism related offences as described in the Directive 2017/541/EU **of the European Parliament and of the Council**[17] **as well as offences concerning the sexual abuse and sexual exploitation of children as described in Directive 2011/93/EU of the European Parliament and of the Council**[18] do not require the minimum maximum threshold of 3 years. [50]

---

[49] New wording suggested by EP.

[50] New wording suggested by EP.

(33) Additionally, it is necessary to provide that the European Production Order **or the European Preservation Order** may only be issued if **an** ~~a similar~~ Order **c**ould **have been ordered under the same conditions in a similar** ~~be available for the same criminal offence in a comparable~~ domestic case[51].

(33a) In cases where an Order is issued to obtain different data categories the issuing authority has to ensure that the conditions and procedures, such as notification of the enforcing State, are met for all of the respective data categories.

(34) **European Production Orders should be addressed to service providers, acting as data controllers, in accordance with Regulation (EU) 2016/679. As an exception, where the data is stored or processed as part of an infrastructure provided by a service provider to a data controller other than natural persons, the European Production Order may be directly addressed to the service provider, processing the data on behalf of the controller, where the data controller cannot be identified despite reasonable efforts on the part of the issuing authority, or where addressing the data controller might be detrimental to the investigation.** ~~In cases where an order is issued to obtain different data categories, the issuing authority has to ensure that the conditions and procedures, such as notification to the enforcing state, are met for all of the respective data categories.~~ ~~the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, typically in case of hosting services, the European Production Order should only be used when other investigative measures addressed to the company or the entity are not appropriate, especially if this would create a risk to jeopardise the investigation.~~

~~This is of relevance in particular when it comes to larger entities, such as corporations or government entities, that avail themselves of the services of service providers to provide their corporate IT infrastructure or services or both. The first addressee of a European Production Order, in such situations, should be the company or other entity. This company or other entity may not be a service provider covered by the scope of this Regulation. However, for cases where addressing that entity is not opportune, for example because it is suspected of involvement in the case concerned or there are indications for collusion with the target of the investigation, competent authorities should be able to address the service provider providing the infrastructure in question to provide the requested data. This provision does not affect the right to order the service provider to preserve the data.~~ [52]

---

51 New wording suggested by EP.

52 New wording suggested by EP.

(34a) ~~In case data are stored or processed as part of an infrastructure provided by a service provider to a public authority only authorities of the same Member State should be able to issue a European Production or Preservation Order because such data can be considered particularly sensitive. Public authority should be understood as any authority that, by its applicable national law has a mandate to govern, administrate a part or aspect of public life, such as branches of the judiciary, the legislative or executive power of a state, province, municipality.~~**In accordance with Regulation (EU) 2016/679, the data processor, storing or processing the data on behalf of the controller, should inform the data controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the data controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. In this case, the issuing authority should indicate [in the case file/order] the reasons for the delay.** [53]

(34b) Where the data is stored or processed as part of an infrastructure provided by a service provider to a public authority, a European Production Order may only be issued where the public authority for which the data is stored or processed is in the issuing State.

(34c) In cases where the data is stored or processed by a service provider as part of an infrastructure, provided to professionals protected by professional privilege, in their business capacity, which stores data protected by a professional privilege under the law of the issuing State, a European Production Order to produce traffic data except for data requested for the sole purpose of identifying the user as defined in Article 2(8) and content data may only be issued where the privileged professional resides in the issuing State, where addressing the privileged professional might be detrimental to the investigation, or where the privileges were waived in accordance with the applicable law. [54]

---

[53] New wording suggested by EP. The Presidency would like to remark that there is an ongoing discussion with the EP on whether there should be "case file" or "order" in the last sentence (similar wording can be found in more provisions)-. The Presidency insist on the "case file".

[54] New wording suggested by EP.

(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege or the right of journalists not to disclose their sources of information), are referred to in other mutual recognition instruments such as the European Investigation Order. Their range and impact differ according to the applicable national law that should be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order **if it could have been ordered under the same conditions in a similar domestic case**~~if a similar order would be available in a comparable domestic situation.~~ **It should be possible for the enforcing State, where it is notified according to this Regulation, to refuse the execution of the European Production Order where it would involve a breach of an immunity or privilege. There is no common definition of what constitutes an immunity or privilege in Union law, the precise definition of these terms is therefore left to national law, which may include protections which apply to*, for instance,* medical and legal professions including when specialized platforms in these areas are used. This may also include rules relating to freedom of the press and freedom of expression in other media.**~~Whether a second legal framework needs to be taken into account should depend on the strength of the connection of the person whose data is sought to the issuing State. Where the person is residing on the territory of the issuing State, a strong link to the issuing State exists. The applicable legal framework to assess immunities and privileges should therefore be that of the issuing State alone. The same principle applies for rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, and fundamental interests of the enforcing State. By the time a request for content or transactional data is made, authorities will regularly have an indication of where the person resides on the basis of previous investigatory steps. Moreover, statistics show that in a large majority of cases, the person resides in the issuing State. Where that is not the case, for example because the person whose data is sought has taken steps to conceal his or her location, the same principle should be applied.~~[55]

[55] **ES** has noted its strong preference for the general approach. **DE** has noted that it must be made clear that this recital applies only to the normal case, where no specialized infrastructure is being used.

(35a) [Immunities and privileges as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, which protect transactional or content data in the enforcing State should therefore be taken into account where the issuing authority has reasonable grounds to believe the person whose data is sought is not residing on its territory. This is relevant in particular should the law of that~~e~~ Member State provide for a higher protection than the law of the issuing State. The provision also ensures respect for cases where the disclosure of the data may impact fundamental interests of that Member State such as national security and defence. These aspects should be taken into account not only when the Order is issued, but also later, and if an enforcement procedure takes place, by the enforcing authority.][56]

(35b) [Where the issuing authority seeks to obtain transactional data and has reasonable grounds to believe that the person whose data are sought is not residing on its territory and that the data requested is protected by immunities and privileges granted under the law of the enforcing State, or by rules of that Member State on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, or its disclosure may impact fundamental interests of that Member State such as national security and defence, the issuing authority should seek clarification, including through appropriate consultation.] [57]

(35c) [In cases where the European Production Order concerns content data and where the issuing authority has reasonable grounds to believe the person whose data are sought is not residing on its territory, the enforcing State is notified and can as soon as possible, preferably within 10 days, inform the issuing authority of issues that might lead to a withdrawal or adaptation of the Order, such as privileges or immunities of the person whose data are sought or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media. 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 such cases, the issuing Member State should provide a copy of the Certificate to the enforcing State at the same time as the Certificate is provided to the service provider.

---

56 EP has suggested to delete this recital, as the substance is covered by recital 35.

57 EP has suggested to delete this recital, as the substance is covered by recital 35.

In the interest of allowing for a swift check, the issuinig authority should choose one of the languages accepted by the enforcing State if a translation of the Certificate is needed, even where the service provider indicated that it would also accept Certificates in another language than one of the official languages of the enforcing State. Where the notified authority raises issues, it should provide the issuing authority with any relevant information regarding the immunities or privileges as well as the rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media granted to the person under its law or information, or if the Order impacts fundamental interests of that Member State such as national security and defence.]

(35d) **Residency is a stable notion therefore a short visit, a holiday or a similar stay in the issuing State without any further substantial link is not enough to establish a residence in that Member State.** In cases where the person, at the time of issuing the European Production Order, **the residency of the person cannot be determined with reasonable and proportionate efforts, the above procedures do not**[58] **apply.**~~has more than one residency, of which one is on the territory of the issuing State, or in cases where the residency of the person cannot be determined with reasonable and proportionate efforts, the above procedures do not apply. However, a short visit, a holiday or a similar stay in the issuing State without any further substantial link is not enough to establish a residence in that Member State.~~

For the purpose of this Regulation, residence applies where a person is registered as a resident in a Member State, holding an identity card, a residence permit or a registration in an official register [for at least 6 months]. Exceptionally, in the absence of registration, residence may be indicated by a registered vehicle, the registration of a fixed telephone number, or other objective and factual criteria proving residence in a Member State, which should be strictly and narrowly assessed. A short visit, a holiday stay, including in a holiday home, or a similar stay in a Member State without any further substantial link is not enough to establish a residence in that Member State. In cases where, at the time of issuing the European Production Order, the residence of the person cannot be determined with reasonable efforts on the part of the issuing authority, the issuing authority should proceed on the assumption that the person is not residing on its territory.

---

58 **DE** has insisted that the word "not" must be deleted here.

´Residence´ or ´resides´ means situations where a person is registered as a resident in a Member State, by holding an identity card, a residence permit or a registration in an official register for at least 6 months. Exceptionally, in the absence of registration, residence may be indicated by a registered vehicle, the registration of a fixed telephone number, or other objective and factual criteria proving residence in a Member State, which shall be strictly and narrowly assessed. In cases where, at the time of issuing the European Production Order, the residence of the person cannot be determined with reasonable efforts on the part of the issuing authority, the issuing authority shall proceed on the assumption that the person is not residing on its territory.[59]

(35e) In order to provide for a swift procedure, the relevant point in time to determine whether there is a need to notify the authorities of the enforcing State should be the time when the Order is issued or validated. Any subsequent change of residency should not have any impact on the procedure. ~~Where the issuing authority did not have reasonable grounds to believe the person whose data are sought is not residing on its territory at the time of issuing or validating the Order, and it later emerges that this person was in fact not residing on the territory of the issuing Member State no later check or notification should be required. However,~~ The person concerned can invoke his or her **fundamental** rights as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media during the whole criminal proceeding, and the other Member State could also raise its fundamental interests such as national security and defence **or where in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter,** at any time during the criminal proceedings. In addition, these grounds could also be invoked during the enforcement procedure.[60]

---

59 The new text has been proposed by the EP. The EP insists on including objective criteria to determine residence.

60 The new text has been proposed by the EP.

~~(35f) Where data is protected by privileges or immunities or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media granted under the law of the enforcing State, or disclosure of data might impact fundamental interests of that Member State, the issuing State should ensure that these grounds are taken into account in the same way as if they were provided for under its own national law, in order to give effect to them. If, for example, such privileges or immunities are not granted under the law of the issuing Member State, the protection should, to the extent possible, be adapted to the closest equivalent privilege or immunity under the law of the issuing State, taking into account the aims and the interests pursued by the specific protection and the effects attached to it. The legal consequences in its own national law for such similar situations should be applied. For the purposes of determining how to take these grounds into account in the same way as if they were provided for under its national law, the issuing authority may contact the notified authority for further information on the nature and the effects of the protection, either directly or via the European Judicial Network in criminal matters or Eurojust. While the enforcing State may raise any and all objections based on these grounds, the person whose data is sought can only rely on his or her own rights, such as privileges or immunities, and cannot raise objections based on a fundamental interest of the enforcing State.[61]~~

(35g) Where a privilege or immunity prohibits the use of the data but these rights could be lifted and where the issuing authority intends to use the data obtained as evidence or does not withdraw the Order in case the data was not obtained, yet, the issuing Member State should have the possibility to request the competent authority to apply for lifting the privilege or immunity.

(36) The European Preservation Order may be issued for any offence. **It should only be issued if it is necessary and proportionate. It should take into account the rights of the suspected or accused person in a proceeding relating to a criminal offence. It should only be issued if it could have been ordered under the same conditions in a similar domestic case and if its execution seems proportionate, adequate and applicable to the case in hand. The assessment should take into account whether the Order is limited to what is strictly necessary to achieve the legitimate** ~~Its~~ aim ~~is~~ to prevent the removal, deletion or alteration of relevant **and necessary as evidence in an individual case** ~~data~~ in situations where it may take more time to obtain the production of this data~~, for example because judicial cooperation channels will be used~~.

---

61 The EP has suggested the deletion of this recital. This has not yet been discussed in Council.

(36a) In order to ensure full protection of fundamental rights, any validation of European Production or Preservation Orders by judicial authorities should in principle be obtained before the order is issued. Exceptions to this principle can only be made in **valably established emergency**~~exceptional~~ cases when seeking subscriber and ~~access~~ data **requested for the sole purpose of identifying the user in accordance with this Regulation,** ~~where the issuing authority validly establishes an emergency case and~~ where it is not possible to obtain the prior validation by the judicial authority in time, in particular because the validating authority cannot be reached to obtain validation and the threat is so imminent that immediate action has to be taken. However, this only applies where **these authorities could issue the Order in a similar domestic case without prior validation by the judicial authority.**~~this procedure is provided for in a similar domestic case under national law.~~

(37) European Production and Preservation Orders should be addressed **directly to the designated establishment or** to the legal representative designated by the service provider **pursuant to Directive XXXX/XXX. Exceptionally, in emergency cases as defined in this Regulation, where the designated establshment or the legal representative of a service provider does not react to the EPOC or the EPOC-PR within the deadlines, the EPOC or EPOC-PR may** ~~In the absence of a designated legal representative, Orders can~~ be addressed to any **other** establishment **or legal representative** of the service provider in the Union ~~This can be the case where there is no legal obligation for the service provider to nominate a legal representative. In case of non-compliance by the legal representative in emergency situations, the European Production or Preservation Order may also be addressed to the service provider~~ alongside or instead of pursuing enforcement of the original Order according to Article 14. ~~In case of non-compliance by the legal representative in non-emergency situations, but where there are clear risks of loss of data, a European Production or Preservation Order may also be addressed to any establishment of the service provider in the Union.~~ Because of these various possible scenarios, the general term 'addressee' is used in the provisions.[62]

[62] The modifications have been proposed by the EP and have not been discussed in Council.

(38) The European Production and European Preservation Orders should be transmitted to the addressee through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR)~~, which should be translated~~. The Certificates should contain the same mandatory information as the Orders~~, except for the grounds for the necessity and proportionality of the measure or further details about the case to avoid jeopardising the investigations. But as they are part of the Order itself, they allow the suspect to challenge it later during the criminal proceedings.~~ Where necessary, ~~a Certificate needs to~~ **the EPOC or the EPOC-PR should** be translated into (one of) the official language(s) of the **Member State where the designated establishment or the legal representative of the service provider are located**~~enforcing State~~, or into another official language that the **designated establishment or the legal representative of the** service provider has declared it will accept.[63] **Where a notification is required, the EPOC or the EPOC-PR to the notified authority should be translated into an official language of the enforcing State. In this regard, Member States should be allowed, at any time, to state in a declaration submitted to the Commission if and in which official language(s) of the Union in addition to their official language(s), they would accept translations of EPOCs and EPOC-PRs. The Commission should make the declarations available to all Member States and to the European Judicial Network.**[64]

(39) The competent issuing authority or the authority competent for transmission should transmit the EPOC or the EPOC-PR directly to the addressee in a secure and reliable way by any means capable of producing a written record under conditions that allow the service provider to establish authenticity, such as by registered mail, secured email and platforms or other secured channels, including those made available by the service provider, in line with the rules protecting personal data.

---

63 NL opposes the suggestion to allow both the language of the executing state and the language of the service provider.

64 The modifications have been proposed by the EP and have not been discussed in Council

(40) **Where notification is not needed in application of this Regulation, an EPOC for subscriber data, [other] data requested for the sole purpose of identifying the user, as defined in this Regulation, traffic data and for content data, should be addressed directly to the designated establishment of the service provider or, where applicable, its legal representative. Upon receipt of such EPOC, the addressee should ensure that** the requested data **are**~~should be~~ transmitted to the authorities in a secure and reliable way **allowing** ~~that allows to~~ **the** establish**ment of** ~~the~~ authenticity **and integrity directly issuing authority or the law enforcement authoritis as indicated in the EPOC** ~~of the sender and integrity of the data~~ at the latest within 10 days upon receipt of the EPOC. **Where notification is needed in application of this Regulation, an EPOC for traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation and for content data should be addressed directly and simultaneously to the designated establishment of the service provider or, where applicable, its legal representative and the enforcing authority. Upon receipt of the EPOC, the service provider should act expeditiously to preserve the data. Where the enforcing authority has not raised any ground for refusal in accordance with this Regulation within 10 days, the addressee should ensure that the requested data are transmitted in a secure and reliable way allowing the establishment of authenticity and integrity directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the at the end of the 10 days upon receipt of the EPOC.** Shorter time limits should be respected by the **addressee, and where applicable, the enforcing authority** ~~provider~~ in emergency cases **as defined in this Regulation.** and if the issuing authority indicates other reasons to depart from the 10 day deadline. ~~In addition to the imminent danger of the deletion of the requested data, such reasons could include circumstances that are related to an ongoing investigation, for example where the requested data is associated to other urgent investigative measures that cannot be conducted without the missing data or are otherwise dependent on it.~~ **The addressee, and, where applicable, the enforcing authority, should execute the order as soon as possible and at the latest inside the deadlines proscribed in the Regulation, taking as full account as possible of the procedural deadlines and other deadlines indicated by the issuing State.** [65]

65 The modifications have been proposed by the EP and have not been discussed in Council

(40a) Where the addressee considers, based solely on the information contained in the EPOC, that the execution of the EPOC could interfere with immunities or privileges, or rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing State the addressee should inform the competent authorities of the issuing and the enforcing State. Where no notification is made pursuant to this Regulation, the issuing authority should take the information mentioned in the previous sub-paragraph into account, and should decide, on its own initiative or on request of the enforcing authority, whether to withdraw, adapt or maintain the Order. Where a notification is made pursuant to this Regulation, the issuing authority should take the information received from the addressee into account, and decide, whether to withdraw, adapt or maintain the Order. The enforcing authority may also decide to raise the grounds for refusal set out in this Regulation.[66]

(41) In **addition, in** order to allow **the addressse** ~~service providers~~ to address formal problems, it is necessary to set out a procedure for the communication between the **addressee** ~~service provider~~ and the issuing ~~judicial~~[67] authority**, as well as, where a notification took place, the enforcing authority,** in cases where the EPOC might be incomplete or contains manifest errors or not enough information to execute the Order. Moreover, should the **addresse** ~~service provider~~ not provide the information in an exhaustive or timely manner for any other reason, for example because it thinks there is a conflict with an obligation under the law of a third country, or because it thinks the European Production Order has not been issued in accordance with the conditions set out by this Regulation, it should go back to the issuing authorities **as well as, where a notification took place, the enforcing authority,** and provide the opportune justifications. The communication procedure thus should broadly allow for the correction or reconsideration of the ~~EPOC~~ **European Production Order** by the issuing authority at an early stage. To guarantee the availabilty of the data, the **addressee** ~~service provider~~ should preserve the data if they can identify the data sought.[68]

---

66 The modification has been proposed by the EP, to correspond to the agreed text of Article 9(2)b. The text has not yet been discussed in Council.

67 JL suggestion.

68 The modification has been proposed by the EP, with reference to Article 9(3) and 9(5). The text has not yet been discussed in Council.

(41a) The addressee should not be obliged to comply with the **European Production** Order in case of de facto impossibility **due to circumstances not attributable to** ~~which was not created by~~ the addressee or, if different, the service provider at the time when the **European Production** Order was received. De facto impossibility should be assumed if the person whose data were sought is not a customer of the service provider or cannot be identified as such even after a request for further information to the issuing authority, or if the data have been deleted lawfully before receiving the order. [69]

(42) Upon receipt of a European Preservation Order Certificate ('EPOC-PR'), the service provider should preserve requested data for a maximum of 60 days unless the issuing authority ~~informs the service provider that it has launched the procedure for issuing a subsequent request for production~~ **confirms that a subsequent requet for production has been issued,** in which case the preservation should be continued. **The issuing authority can extend the duration of the preservation by an additional 30 days, where necessary to allow for the issuing of the subsequent request for production, using the form set out in Annex IV. Where the issuing authority confirms within the relevant deadline that a subsequent request for production has been issued at its level, the service provider should preserve the data as long as necessary to produce the data once the subsequent request for production is served. Such a confirmation must be sent to the service provider [and to the enforcing authority when a notification took place on the EPOC,] within the relevant deadline, in one of the official languages of the Member State where the service provider or its legal representative is located [and of the enforcing State] or any other language accepted by the addressee[s], using the form set out in Annex IV. To prevent the preservation from ceasing it is sufficient that the formal step of issuing the underlying production request has been taken and the confirmation sent by the competent issuing authority; further required formalities for the transmission such as the translation of documents do not need to be completed at this point of time. Where the preservation is no longer necessary, the issuing authority should inform the addressee without undue delay and the preservation for the purpose of the relevant Order should cease.**

---

69 The modification has been proposed by the EP, to correspond to the agreed text of Article 9(2)b. The text has not yet been discussed in Council.

~~The 60 day period is calculated to allow for the launch of an official request. This requires that at least some formal steps have been taken, for example by sending a mutual legal assistance request to translation. Following receipt of that information, the data should be preserved as long as necessary until the data is produced in the framework of a subsequent request for production.~~[70]

(42a) Where the addressee considers, based solely on the information contained in the EPOC-PR, that the execution of the EPOC-PR could interfere with immunities or privileges, or rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing State the addressee should inform the competent authorities of the issuing and the enforcing State. The issuing authority should take the information received from the addressee into account, and decide on its own initiative or on request of the enforcing State, whether to withdraw, adapt or maintain the Order.[71]

(42b) In addition, in order to allow the addressee to address formal problems, it is necessary to set out a procedure for the communication between the addressee and the issuing judicial authority in cases where the EPOC-PR might be incomplete or contains manifest errors or not enough information to execute the Order. Moreover, should the addressee not provide the information in an exhaustive or timely manner for any other reason, for example because it thinks there is a conflict with an obligation under the law of a third country, or because it thinks the European Preservation Order has not been issued in accordance with the conditions set out by this Regulation, it should go back to the issuing authorities and provide the opportune justifications. The communication procedure thus should broadly allow for the correction or reconsideration of the European Preservation Order by the issuing authority at an early stage.

---

70 The modification has been proposed by the EP, to correspond to the agreed text of Article 10(3). The text has not yet been discussed in Council.

71 The recitals in points (a), (b) and (c) have been proposed by EP, based on the provisional agreement on Article 10(3) to 10(6); EP has also suggested that these recitals could possibly be merged with recitals (40a), (41) and (41a)

(42c) The addressee should not be obliged to comply with the European Preservation Order in case of de facto impossibility due to circumstances not attributable to the addressee or, if different, the service provider at the time when the European Preservation Order was received. De facto impossibility should be assumed if the person whose data were sought is not a customer of the service provider or cannot be identified as such even after a request for further information to the issuing authority, or if the data have been deleted lawfully before receiving the order.

(42d) Notwithstanding the principle of mutual trust, the enforcing authority should, where appropriate, raise grounds for refusal of a European Production Order, where a notification took place in accordance with this Regulation, based on a list of grounds for refusal, provided for in this Regulation. [72]

(42e) Where the recognition or execution of such European Production Order would involve the breach of an immunity or privilege in the enforcing State, where the data requested are related to rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, or where, in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter, the enforcing authority should refuse that order.[73]

(42f) The principle of ne bis in idem is a fundamental principle of law in the Union, as recognised by the Charter and developed by the case law of the Court of Justice of the European Union. Therefore, where the enforcing authority assesses the Order, it should refuse the execution of a European Production Order if its execution would be contrary to that principle.

---

72 The recital has been proposed by EP, with reference to the EIO and to Article 10a(1). The text has not yet been discussed in Council.

73 The recital has been proposed by EP, with reference to Article 10a(1) points b-d. The text has not yet been discussed in Council.

(43) ~~Service providers and their legal representatives should ensure confidentiality. Furthermore they should refrain from informing the person whose data is being sought in order to safeguard the investigation of criminal offences, in compliance with Article 23 of Regulation (EU) 2016/679[74], except where requested by the issuing authority to inform the person. In these cases, the issuing authority should also provide the necessary information about the applicable legal remedies to the service provider, so that it can be included in the information to the person. In any case, user information is an essential element in enabling review and judicial redress and should be provided by the authority if the service provider was not asked not to inform the user, as soon as there is no risk of jeopardising ongoing investigations, in accordance with the national measure implementing Article 13 of Directive (EU) 2016/680[75]. The issuing authority may abstain from informing the person whose subscriber or access data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought. This could be the case where an Order concerns subscriber or access data of a third person, in light of the presumption of innocence of the suspect. Where the identity of the person concerned is unknown to the issuing authority, investigations to determine the identity of this person should only be carried out insofar as it seems necessary and proportionate in relation to the invasiveness of the measure and the respective effort associated with establishing their identity.~~ **Since informing the person whose data is sought is an essential element as regards data protection rights and defence rights, in enabling effective review and judicial redress, in accordance with Article 6 TEU and the Charter, the issuing authority should inform the person whose data are being sought without undue delay about the data production.**

---

74 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

75 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

However, the issuing authority may, in accordance with national law, delay, restrict or omit informing the person whose data are being sought, to the extent that, and for as long as the conditions of Directive 2016/680[13] are met, in which case, the issuing authority should indicate [in the case file/order] the reasons for the delay, restriction or omission. The addressees and, if different, the service providers should take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved. [76]

The service provider may claim reimbursement of its costs by the issuing State, if that is provided for by the national law of the issuing State for domestic orders in similar situations, in accordance with that national law provisions. Member States should inform the Commission about their national rules for reimbursement, and the Commission should make them public. [77]

Without prejudice to national laws providing for the imposition of criminal sanctions, Member States should lay down rules on pecuniary sanctions applicable to infringements of this Regulation and should take all necessary measures to ensure that they are implemented. Member States should, without delay notify the Commission of those rules and of those measures and should notify it, without delay, of any subsequent amendment affecting them. Member States should ensure that the pecuniary sanctions provided for by national laws of the Member States are effective, proportionate and dissuasive and that pecuniary sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed. Without prejudice to data protection obligations, service providers should not be held liable in Member States for the consequences resulting from compliance with an EPOC or an EPOC-PR. [78]

---

76 The recital has been proposed by EP, with reference to provisional agreement Article 11(1) and 11(1)a. The text has not yet been discussed in Council.

77 The recital has been proposed by EP, with reference to the provisional agreement in Article 12(1). The text has not yet been discussed in Council.

78 The paragraph has been proposed by EP, with reference to the provisional agreement in Article 13. The text has not yet been discussed in Council.

Where a service provider acts with due diligence, in particular with regards to data protection obligations, and requested clarification or justification from the issuing authority, in accordance with this Regulation, it should not be held liable for the consequences of any delays caused. In addition, sanctions applied to infringements of the obligations of service provider pursuant to this Regulation should be annulled, where an order has been successfully challenged in accordance with this Regulation. [79]

(44) **Where the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority and where the enforcing authority has not invoked any of the grounds for refusal as provided for in this Regulation, the issuing authority may request the competent authority in the enforcing State to enforce the European Production Order or the European Preservation Order. To this end, the issuing authority should transfer the Form filled out by the addressee and any relevant document by any means capable of producing a written record under conditions allowing the enforcing authority to establish authenticity. It should translate the Order and any document transferred into one of the languages accepted by this Member State and should inform the addressee of the transfer. This Member State should enforce it in accordance with its national law. Member States should provide for the imposition of effective, proportionate and deterrent pecuniary sanctions in case of infringements of the obligations set up by this Regulation.** ~~In case of non-compliance by the addressee, the issuing authority may transfer the full Order including the reasoning on necessity and proportionality, accompanied by the Certificate, to the competent authority in the Member State where the addressee of the Certificate resides or is established. This Member State should enforce it in accordance with its national law. Member States should provide for the imposition of effective, proportionate and deterrent pecuniary sanctions in case of infringements of the obligations set up by this Regulation.~~ [80]

[79] The paragraph has been proposed by EP. The text has not yet been discussed in Council.

[80] The changes in this recital have been proposed by the EP and have not been discussed in Council.

(45) The enforcement procedure is a procedure where the addressee can invoke formal grounds against the enforcement based on certain restricted grounds, **provided for in this Regulation, including it not being issued or validated by a competent authority or where the European Production Order does not concern data stored by or on behalf of the service provider at the time of receipt of EPOC**. The enforcing authority can refuse to recognise and enforce the Order based on the same grounds**, or where a notification took place in accordance with this Regulation, based on additional grounds for refusal.** ~~and additionally, in case they have to be taken into account under this Regulation, if immunities and privileges as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media under its national law apply or the disclosure may impact its fundamental interests such as national security and defence.~~ **The enforcing authority can refuse to recognize and enforce the Order based on the same grounds, or, where a notification took place in accordance with this Regulation, based on additional grounds for refusal.** The enforcing authority should consult the issuing authority before refusing to recognise or enforce the order, based on these grounds. In case of non-compliance, authorities can impose sanctions. These sanctions should be proportionate also in view of specific circumstances such as repeated or systemic non-compliance.[81]

(45a) When determining in the individual case the appropriate pecuniary sanction, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence, whether the service provider was held responsible for similar previous breaches and the financial strength of the service provider held liable. In exceptional circumstances, that assessment may lead the enforcing authority to decide to abstain from imposing any pecuinary sanctions. Particular attention should, in this respect, be given to micro enterprises that fail to comply with an Order in an emergency case due to lack of **human**[82]~~personal~~ resources ouside normal buisness hours, if the data is transmitted without undue delay.

---

81 The changes in this recital have been proposed by the EP and have not been discussed in Council.

82 EP suggestion.

(46) **Without prejudice to data protection obligations,** service providers should not be held liable in Member States for **the consequences resulting from** ~~the prejudice to their users or third parties resulting from good faith~~ compliance with an EPOC or an EPOC-PR. The responsibility to ensure the legality of the Order, in particular its necessity and proportionality, should lie with the issuing authority. [83]

(47) In addition to the individuals whose data is ~~requested,~~ **sought, the laws of a third country** ~~the service providers and third countries~~ may be affected by the investigative measure. To ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned and to address conflicting obligations on service providers, this instrument provides a specific mechanism for judicial review where compliance with a European Production Order would prevent service providers from complying with legal obligation deriving from **the law of** a third **country** ~~State's law~~. [84]

(48) To this end, whenever the addressee considers that the European Production Order in the specific case would entail the violation of a legal obligation stemming from the law of a third country, it should inform the issuing authority by way of a reasoned objection, using the forms provided. The issuing authority should then review the European Production Order in light of the reasoned objection **and any input provided by the enforcing State**, taking into account the same criteria that the competent court would have to follow. Where the authority decides to uphold the Order, the procedure should be referred to the competent court, as notified by the relevant Member State, which then reviews the Order. [85]

(49) In determining the existence of a conflicting obligation in the specific circumstances of the case under examination, the competent court may rely on appropriate external expertise where needed, for example on the interpretation of the law of the third country concerned. This could include consulting the central authorities of that country, **taking into account Directive 2016/680**. **Information should in particular be requested from the competent authority of the third country by the issuing State where the conflict concerns fundamental rights of the third country or fundamental interests of the third country related to national security and defence.** [86]

---

83 The changes in this recital have been proposed by the EP and have not been discussed in Council.

84 The changes in this recital have been proposed by the EP and have not been discussed in Council.

85 The changes in this recital have been proposed by the EP and have not been discussed in Council.

86 The changes in this recital have been proposed by the EP and have not been discussed in Council.

(50) Expertise on interpretation could also be provided through expert opinions where available. Information and case law on the interpretation of **the laws of a** third country~~ies' laws~~ and on conflicts procedures in Member States should be made available on a central platform such as the SIRIUS project and/or the European Judicial Network**, with a view to benefitting** ~~. This should allow courts to benefit~~ from experience and expertise gathered by other courts on the same or similar questions. It should not prevent a renewed consultation of the third state where appropriate.[87]

(51) Where conflicting obligations exist, the court should determine whether the conflicting provisions of the third country law applies and if so, whether they prohibit disclosure of the data concerned, ~~Where the court concludes that conflicting provisions of the third country prohibit disclosure of the data.~~ **by weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible consequences for the service provider of having to comply with the Order. Particular importance and weight should be given to the protection of fundamental rights by the third country's provisions and other fundamental interests, such as national security interests of the third country as well as the degree of connection of the criminal case to either of the two jurisdictions when conducting the assessment. Where the court decides to lift the Order, it should inform the issuing authority and the addressee. If the competent court determines that the Order is to be upheld, it should inform the issuing authority and the addressee, who should proceed with the execution of the Order. The issuing authority should inform the enforcement authority about the outcome of the proceedings.**[88]

---

87 The changes in this recital have been proposed by the EP and have not been discussed in Council.

88 The changes in this recital have been proposed by the EP and have not been discussed in Council.

(52) [The court should take its decision on whether to uphold the European Production Order by weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible consequences for the service provider of having to comply with the Order. Importantly for cyber-related offences, the place where the crime was committed covers both the place(s) where the action was taken and the place(s) where the effects of the offence materialised. Particular importance and weight should be given to the protection of fundamental rights by the third country's provisions and other fundamental interests, such as national security interests of the third country as well as the degree of connection of the criminal case to either of the two jurisdictions when conducting the assessment.][89]

(53) The conditions set out in Article 9 [*OR instead of the last four words: "related to the execution fo an EPOC"*] are applicable also where conflicting obligations deriving from the law of a third country occur. During this procedure[90], the data should be preserved. Where the Order is lifted, a new Preservation Order may be issued to permit the issuing authority to seek production of the data through other channels, such as mutual legal assistance.

(54) It is essential that all persons whose data are requested in criminal investigations or proceedings have access to an effective legal remedy, in line with Article 47 of the Charter of Fundamental Rights of the European Union. ~~For suspects and accused persons, the right to an effective remedy could be exercised whenever data obtained is used in criminal proceedings against them. This may affect the admissibility, or as the case may be, the weight in the proceedings, of the evidence obtained by such means. In addition, they benefit from all procedural guarantees applicable to them, such as the right to information. Other persons, whose data were sought but who are not suspects or accused persons, should also have a right to an effective remedy. Therefore, as a minimum, the possibility to challenge the legality of a European Production Order, including the necessity and the proportionality of the Order, should be provided. This Regulation should not limit the possible grounds to challenge the legality of the Order. These remedies should be exercised in the issuing State in accordance with national law. Rules on interim relief should be governed by national law.~~

89 EP proposes to delete this recital, which is partly covered by recital 51.

90 JL comment: unclear.

Without prejudice to further legal remedies available in accordance with national law, any persons whose data were sought via a European Production Order or Preservation Order should have the right to effective remedies against the European Production Order or Preservation Order. Where that person is a suspect or accused person, the person should have the right to effective remedies during the criminal proceedings in which the data were being used as evidence. The right to an effective remedy should be exercised before a court in the issuing State in accordance with its national law and should include the possibility to challenge the legality of the measure, including its necessity and proportionality, without prejudice to the guarantees of fundamental rights in the enforcing State, or other additional remedies in accordance with national law. This Regulation should not limit the possible grounds to challenge the legality of the Order. **Remedies mentioned in this Regulation should be without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679. Information should be provided in due time as regards the possibilities under national law for seeking remedies and ensure that they can be exercised effectively.**[91]

(55) [In addition,During the enforcement procedure the enforcing authority may refuse the recognititon and enforcement of a European Production or Preservation Order on a number of limited grounds.]**[92]**

(56) [The protection of natural persons for the processing of personal data is a fundamental right. In accordance with Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the TFEU, everyone has the right to the protection of personal data concerning them. When implementing this Regulation, Member States should ensure that personal data are protected and may only be processed in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680.**[93]**]

---

91 The changes in this recital have been suggested by EP and have not been discussed in Council.

92 EP considers that this is already covered in recitals 11b and 11c above.

93 EP considers this is already covered in recitals 11c and 11d above.

(56a) Transmission and transfer as well as making use of electronic evidence obtained through a European Production Order in other proceedings and for another purpose as for the one for which the Order was issued should be restricted, in particular to criminal offences for which the issuing authority could have also issued a European Production Order. The use, transmission or transfer of electronic evidence should, in addition only be possible where the data are needed to prevent an immediate and serious threat to public security of the respective Member State or third country as well as their essential interests. International transfer of electronic evidence is furthermore subject to conditions as set out in Chapter V of Directive (EU) 2016/680. In cases, where the obtained personal data is used for the prevention of an immediate and serious threat to public security of the respective Member State or third country as well as their essential interests, and such threat may not lead to criminal investigations Regulation (EU) 2016/679 should apply.

(56b) [When making a declaration concerning the language regime, Member States are encouraged to include at least one additional language to their official language(s).][94]

(57) Personal data obtained under this Regulation should only be processed when necessary and proportionate to the purposes of prevention, investigation, detection and prosecution of crime or enforcement of criminal sanctions and the exercise of the rights of defence. In particular, Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers for the purposes of this Regulation, including measures 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.

---

94 EP suggests that this is already covered by recital 38.

(58) The Commission should carry out an evaluation of this Regulation that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU value added and should provide the basis for impact assessments of possible further measures. Information should be collected regularly and in order to inform the evaluation of this Regulation.

(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information between judicial authorities and service providers, allowing them to secure and transmit electronic evidence more quickly and effectively, while also fulfilling the necessary security requirements in a user-friendly manner. They reduce translation costs and contribute to a high quality standard. Response forms similarly should allow for a standardised exchange of information, in particular where service providers are unable to comply because the account does not exist or because no data is available. The forms should also facilitate the gathering of statistics.

(60) In order to effectively address a possible need for improvement regarding the content of the EPOCs and EPOC-PRs and of the form to be used to provide information on the impossibility to execute the EPOC or EPOC-PR, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission **in respect to the amendment of** ~~to amend~~ Annexes I, II, III **and IV** to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[95]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(61) The measures based on this Regulation should not supersede European Investigation Orders in accordance with Directive 2014/41/EU of the European Parliament and of the Council[96] to obtain electronic evidence. Member States' authorities should choose the tool most adapted the case at hand; they may prefer to use the European Investigation Order when requesting a set of different types of investigative measures including but not limited to the production of electronic evidence from another Member State.

---

95 OJ L 123, 12.5.2016, p. 1.

96 Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p.1).

(62) Because of technological developments, new forms of communication tools may prevail in a few years, or gaps may emerge in the application of this Regulation. It is therefore important to provide for a review on its application.

(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic evidence across borders, cannot be sufficiently achieved by the Member States given its cross-border nature, but can rather be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve **that**~~those~~ objectives.

(64) In accordance with Article 3 of ~~the~~ Protocol **No 21** on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation.~~] or [and without prejudice to Article 4 of that Protocol, the United Kingdom/Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.~~

(65) In accordance with Articles 1 and 2 of the Protocol No 22 on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(66) The European Data Protection Supervisor was consulted in accordance with Article ~~28~~**42**(2) of Regulation (**EU**) No **2018/1725**~~45/2001~~ of the European Parliament and of the Council[97] and delivered an opinion on **6 November 2019**[98],

---

97 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

98 OJ C , , p. .

HAVE ADOPTED THIS REGULATION:

Chapter 1: Subject matter, definitions and scope

Article 1

Subject matter

1. This Regulation lays down the rules under which an authority of a Member State**, in a criminal proceeding,** may order a service provider offering services in the Union **and established or, if not established, represented by a legal representative in another Member State**, to produce or preserve electronic evidence, regardless of the location of data. This Regulation is without prejudice to the powers of national authorities to **address**[99] ~~compel~~ service providers established or represented on their territory to comply with similar national measures.

1a. The issuing of a European Production or Preservation Order may also be requested by a suspected or accused person, or by a lawyer on his behalf within the framework of applicable defence rights in accordance with national criminal procedures.

2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined **in the Charter and** in Article 6 of the TEU, and any obligations incumbent on law enforcement or judicial authorities in this respect shall remain unaffected. **It shall apply without prejudice to fundamental principles, in particular the freedom of expression and information, including freedom and pluralism of the media, the respect for private and family life, the protection of personal data, as well as the right for effective judicial protection.** [100]

---

99 **ES** and **BE** would prefer the word "compel"

100 **BE** doesn't see the added value of an enumeration of particular fundamental rights but can conditionally support this approach.

Article 2

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'European Production Order' means a ~~binding~~ decision, **issued or validated** by a~~n~~ ~~issuing~~ **judicial** authority of a Member State **in application of Articles 4(1) to 4(5), addressed to a designated establishment or a legal representative of** ~~compelling~~ a service provider offering services in the Union **located** ~~and established or represented~~ in another Member State **bound by this Regulation** to produce electronic evidence[101];

(2) 'European Preservation Order' means a ~~binding~~ decision**, issued or validated** by a~~n~~ **judicial** ~~issuing~~ authority of a Member State ~~compelling a service provider offering services in the Union~~ **in application of Articles 4(1) to 4(5), addressed to a designated establishment or a legal representive** ~~and established or represented~~ in another Member State **bound by this Regulation** ~~compelling a service provider offering services in the Union and established or represented,~~ to preserve electronic evidence in view of a subsequent request for production;[102]

(3) 'service provider' means any natural or legal person that provides one or more of the following categories of services, with the exception of financial services referred to in Article 2(2)(b) of Directive 2006/123/EC

(a) electronic communications service as defined in Article 2(4) of [Directive establishing the European Electronic Communications Code];

(b) internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and domain name related privacy and proxy services;

(c) other information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[103] that provide:

---

101 **DE** suggests that the substance of Article 5(6) should be moved here, as it regards the definition of ISPs/addressees.

102 **DE** suggests that the wording „legal representative of a service provider offering services in the Union located in another Member State" should be same in para. 1 and 2 of Article 2

103 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

– the ability to its users to communicate with each other; or

– **the ability** to process or store data on behalf of the users to whom the service is provided **for, where the storage of data is a defining component of the service provided to the user**;

(4) 'offering services in the Union' means:

(a) enabling **natural or** legal ~~or natural~~ persons in **a** ~~one or more~~ Member State~~(s)~~ to use the services listed under **point** (3) ~~above~~; and

(b) having a substantial connection based on specific factual criteria to the Member State(s) referred to in point (a)**; such a substantial connection to the Union shall be considered to exist where the service provider has an establishment in the Union, or, in the absence of such an establishment, based on the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States**;

(5) 'establishment' ~~or 'being established'~~ means ~~the actual pusuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or the business is managed~~ **the establishment designated by the service provider in accordance with Directive XXXX/XXXX.**

(5a) '**designated establishment' means an establishment designated in writing by a service provider established in a Member State taking part in a legal instrument referred to in Article 1(2) of the Directive XXXX/XXX, for the purpose of Articles 1(1) and 3(1);**

(5b) '**legal representative' means a natural or legal person, designated in writing by a service provider not established in a Member State taking part in a legal instrument referred to in Article 1(2) of the Directive XXX/XXX, for the purpose of Articles 1(1) and 3(1);**

(6) 'electronic evidence' means ~~evidence~~ **subscriber data, traffic data or content data** stored by or on behalf of a service provider**,** in **an** electronic form**,** at the time of receipt of a **an EPOC or an EPOC-PR, and is requeted for the purpose of proceedings as defined in Article 3(2)** ~~production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data~~;

(7) 'subscriber data' means any data **held by a service provider relating to the subscription to the services,** pertaining to:

(a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone **number**, or email **address**;

(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer **at the moment of initial registration or activation** and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;

(8) ~~'access data' means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (c) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];~~

'[other] data requested for the sole purpose of identifying the user' means IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information where requested by law enforcement authorities for the sole purpose of identifying the user in a specific criminal investigation.

(9) '~~transactional~~**traffic** data' means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression ~~unless such data constitutes access data. This includes~~ **including** electronic communications metadata as defined in point (c) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications] **and data relating to the commencement and termination of a user access session to a service such as the data and time of use, the log-in to and log-off from the service other than subscriber data**;

(10) 'content data' means any ~~stored~~ data in a digital format such as text, voice, videos, images, and sound other than subscriber, ~~access~~ or **traffic**~~transactional~~ data;

(11) 'information system' means information system as defined in point (a) of Article 2 of Directive 2013/40/EU of the European Parliament and of the Council[104];

(12) 'issuing State' means the Member State in which the European Production Order or the European Preservation Order is issued;

(12a) **'issuing authority' means the competent authority in the issuing State, which, in accordance with Article 4, can issue a European Production Order or European Preservation Order;**

(13) 'enforcing State' means the Member State in which the **designated establishment or legal representative is established and to which**~~addressee of~~ the European Production Order **and the European Production Certificate** or the European Preservation Order **and the European Preservation Order Certificate** ~~resides or is established and to which, if necessary, the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate~~ are transmitted for **notification or** enforcement **of the order in accordance with this Regulation**;[105]

(14) 'enforcing authority' means**, in accordance with national law,** the competent authority in the enforcing State to which the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted by the issuing authority for **notification or**[106] enforcement **of the order in accordance with this Regulation**;[107]

---

104 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

105 **PL** would like to have this provision redrafted

106 "and" has been replaced by "or" as suggested or implied by delegations (**ES, IE**).

107 **PL** would like to have this provision redrafted

(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity **or safety** of a person or to a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC[108], **where the disruption or destruction of such critical infrastructure would result in an imminent threat to life or physical integrity or safety of a person, including through a serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State.**

Article 3

Scope

1. This Regulation applies to service providers which offer services in the Union.

1a. The Regulation shall not apply to proceedings initiated by the issuing authority for the purpose of providing mutual legal assistance to another Member State or a third country.

2. The European Production Orders and European Preservation Orders ~~may~~ **shall**[109] only be issued **in the framework and for the purposes of** ~~for~~ criminal proceedings, **[**and for the execution of custodial sentences or detention orders that were not rendered in absentia in case the convict absconded from justice**]**. The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.

3. The Orders provided for by this Regulation may be issued only for data pertaining to services as defined in Article 2(3) offered in the Union.

Chapter 2: European Production Order, European Preservation Order and Certificates

Article 4

Issuing authority

1. A European Production Order for **obtaining** subscriber data **and for obtaining [other] data requested for the sole purpose of identifying the user, as defined in Article 2 (8)** ~~and access data~~ may be issued by:

(a) a judge, a court, an investigating judge or **a public** prosecutor competent in the case concerned; or

---

108 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 34523.12.2008. p 75).

109 JL suggestion.

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a **public** prosecutor in the issuing State[110].

2. A European Production Order for **traffic data,**~~transactional~~ **except for data requested for the sole purpose of identifying the user as defined in Article 2 (8),** and content data may be issued only by:

(a) a judge, a court or an investigating judge competent in the case concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court or an investigating judge in the issuing State.

3. A European Preservation Order **for all data categories** may be issued by:

(a) a judge, a court, an investigating judge or **a public** prosecutor competent in the case concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Preservation Order shall be validated, after examination of its conformity with the conditions for issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a **public** prosecutor in the issuing State.

4. Where the Order has been validated by a judicial authority pursuant to paragraphs 1(b), 2(b) and 3(b), that authority may also be regarded as an issuing authority for the purposes of transmission of the European Production Order Certificate and the European Preservation Order Certificate.

---

110 EP wishes to add a subparagraph here, to allow MS to require the involvement of a judge. **NL** and **BE** note their opposition to such a subparagraph. **DE** questions whether this subparagraph provides sufficient clarity. **HU** can support the additional proposal of EP.

5. In validly established emergency cases **as defined in Art. 2(15),** the authorities mentioned under paragraphs 1(b) and 3(b) may **exceptionally** issue the respective Order for subscriber ~~and access~~ data **and date requested for the sole purpose of identifying the user in accordance with Article 2(8),** without prior validation**,** ~~if~~ **where** the validation cannot be obtained in time and ~~if~~ **where** these authorities could issue the Order in a similar domestic case without validation. The issuing authority shall seek validation ex-post without undue delay, at the latest within 48 hours. Where such ex-post validation is not granted, the issuing authority shall withdraw the Order immediately and shall ~~in accordance with its national law, either~~ delete any data that was obtained**.** ~~or ensure that the data are not used as evidence.~~

6. Each Member State may designate one or more central authority responsible for the administrative transmission of Certificates, Orders and notifications, the receipt of data and notifications as well as transmission of other official correspondence relating to the Certificates or Orders.

Article 5

Conditions for issuing a European Production Order

1. An issuing authority may only issue a European Production Order where the conditions set out in this Article are fulfilled.

2. The European Production Order shall **only be issued if it is**[111] ~~be~~ necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2**), taking into account the rights of the suspected or accused person**[112]**. It** ~~and~~ may only be issued if **it could have been ordered under the same conditions in** a similar ~~measure would be available for the same criminal offence in a comparable~~ domestic **case**~~situation in the issuing State~~.

3. European Production Orders to produce subscriber data or ~~access~~ data **requested for the sole purpose of identifying the user as defined in Article 2(8)** may be issued for all criminal offences [and for the execution of a custodial sentence or a detention order of at least 4 months].

---

111 JL suggestion.

112 **PL** has questioned why the rights of victims are omitted here and has suggested to go back to the general approach, or to refer to the "rights of the data subject and, in particular, to the rights of the victim…"

4. European Production Orders to produce **traffic** ~~transactional~~ data, **except for data requested for the sole purpose of identifying the user as defined in Article 2(8)** or content data may only be issued:

(a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or

(b) for the following offences, if they are wholly or partly committed by means of an information system:

– offences as defined in Articles 3, 4, 5, **6, 7 and 8 of the Directive (EU) 2019/713 of the European Parliament and of the Council** ~~of the Council Framework Decision 2001/413/JHA~~;

– offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[113];

– offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[114].

(d) for the execution of a custodial sentence or a detention order of at least four months imposed for criminal offences pursuant to point (a), (b) and (c) of this paragraph;

5. The European Production Order shall include the following information:

(a) the issuing and, where applicable, the validating authority;

(b) the addressee of the European Production Order as referred to in Article 7;

(c) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, ID or account name to determine the data that are being sought;

(d) the requested data category **as defined in Article 2 paragraphs 7 to10** (~~subscriber data access data, transactional data or content data);~~

(e) if applicable, the time range requested to be produced;

(f) the applicable provisions of the criminal law of the issuing State;

---

113 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

114 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).

(g) in case of emergency or request for earlier disclosure, the reasons for it**[115]**;

(h) in cases where the **European Production Order is directly addressed to the service provider, processing the data on behalf of the data controller,** [116]~~data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons,~~ a confirmation that the Order is made in accordance with paragraph 6**[117]**;

(i) the grounds for the necessity and proportionality of the measure **in application of Article 5(2);**

(j) **a summary description of the case.**[118]

6. ~~In cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.~~ **European Production Orders shall be addressed to service providers, acting as data controllers, in accordance with Regulation (EU) 2016/679.**

As an exception, where the data is stored or processed as part of an infrastructure provided by a service provider to a data controller other than natural persons, the European Production Order may be directly addressed to the service provider, processing the data on behalf of the controller, where:

- **the data controller cannot be identified despite reasonable efforts on the part of the issuing authority, or**
- **addressing the data controller might be detrimental to the investigation**[119]**.**

---

115 Not agreed by the EP.

116 **ES** is opposed to build provisions based on the concepts of "data controller" and "data processor".

117 ES, BE and SI object to the method to build provisions based on the concepts of data controllers and data processor (se also Articles 5(6) and 5(6)a).

118 **ES** objects to this point. **BE** could accept it if the description is only shared with the enforcing state, not the addressee. **BG** suggested that point "j" can be implemented in point "i".

119 **ES** is opposed to build provisions based on the concepts of "data controller" and "data processor", **BE** is concerned regarding these two notions. **DE** considers that the mechanism described here and in the following paragraphs should be defined in Article 2 instead. **SI** does not support the current wording of the paragraph.

6a. **In accordance with Regulation (EU) 2016/679, the data processor, storing or processing the data on behalf of the controller, shall inform the data controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the data controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. In this case, the issuing authority shall indicate in the case [file/order]**[120] **the reasons for the delay.**
[121]

~~6a. A European Production Order to produce data stored or processed as part of an infrastructure provided by a service provider to a public authority may only be issued if the public authority for which the data is stored or processed is in the issuing State.~~

6b. **Where the data is stored or processed as part of an infrastructure provided by a service provider to a public authority, a European Production Order shall**[122] ~~may~~ only be issued where the public authority for which the data is stored or processed is in the issuing State.

6c. **In cases where the data is stored or processed by a service provider as part of an infrastructure, provided to professionals protected by professional privilege, in their business capacity, which stores data protected by a professional privilege under the law of the issuing State, a European Production Order to produce traffic data except for data requested for the sole purpose of identifying the user as defined in Article 2(8) and content data shall only be issued:**

- **where the privileged professional resides in the issuing State, or**
- **where address*ing* the privileged professional might be detrimental to the investigation, or**
- **where the privileges were waived in accordance with the applicable law**[123]**.**

---

120 The EP insist on referring to case order here.

121 **ES** is opposed to build provisions based on the concepts of "data controller" and "data processor". **SI** does not support the current wording of the paragraph.

122 JL suggestion, see also paragraph 6c below.

123 **ES** and **NL** wishes to see a reformulation of this provision. **PL** wishes to indicate which State's law is applicable. **DE** considers the exception too large; it should only concern proceedings being conducted against the professionals themselves. **BG** has raised concerned about this provision and suggested that consultation with the enforcing state is a better option. **SI** notes that the professional secrecy in the enforcing state requires equal protection.

~~7. In cases where the Order concerns transactional data and where the issuing authority has reasonable grounds to believe that~~

~~a) the person whose data are sought is not residing on the territory of the issuing State, and~~

~~b) the data requested is protected by immunities and privileges granted under the law of the enforcing State or it is subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media its disclosure may impact fundamental interests of the enforcing State such as national security and defence, the issuing authority shall seek clarification on the circumstances referred to in point b) before issuing the European Production Order, including by consulting the competent authorities of the enforcing Member State concerned, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested transactional data are protected by such immunities and privileges or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media or its disclosure would impact fundamental interests of the other Member State such as national security and defence, it shall take these circumstances into account in the same way as if they were provided for under its national law and it shall not issue or shall adapt the European Production Order where necessary to give effect to these grounds.~~

~~8. Where the power to waive the privilege or immunity lies with an authority of the enforcing State, the issuing authority may request the enforcing authority to contact the competent authority to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.~~

Article 6

Conditions for issuing a European Preservation Order

1. An issuing authority may only issue a European Preservation Order where the conditions set out in this Article are fulfilled. Article 5 ~~(~~6**ba**[124]~~)~~ shall apply mutatis mutandis.

124 **DE** has questioned why this provision does not refer to Article 5(6) in its entirety.

2. It may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order**, taking into account the rights of the suspected or accused person**[125]**.** European Preservation Orders to preserve data may be issued for all criminal offences, **provided that it could have been ordered under the same conditions in a similar domestic case**, and for the execution of a custodial sentence or a detention order of at least 4 months.

3. The European Preservation Order shall include the following information:

   (a) the issuing and, where applicable, the validating authority;

   (b) the addressee of the European Preservation Order as referred to in Article 7;

   (c) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, **login** ID or account name to determine the data that are ~~being~~ sought;

   (d) the **requested** data category **as defined in Article 2 paragraphs 7 to 10;** ~~to be preserved (subscriber data, access data, transactional data or content data);~~

   (e) if applicable, the time range requested to be preserved;

   (f) the applicable provisions of the criminal law of the issuing State;

   (g) the grounds for the necessity and proportionality of the measure **in application of Article 5(2)**.

Article 7

Addressee of a European Production Order and a European Preservation Order

1. The European Production Order and the European Preservation Order shall be addressed directly to a legal representative designated by the service provider **pursuant to Directive XXX/XXXX**~~for the purpose of gathering evidence in criminal proceedings~~.

~~2. If no 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.~~

[125] **PL** has questioned why the rights of victims are omitted here and has suggested to go back to the general approach, or to refer to the "rights of the data subject and, in particular, to the rights of the victim…"

2. **Exceptionally, in emergency cases as defined in Article 2(15), w**here the **designated establishment or the** legal representative **of a servcie provider** does not **reply to the** ~~comply with an~~ EPOC **within the deadlines,** ~~in an emergency case pursuant to Article 9(2),~~ the EPOC~~uropean Production Order~~ may be addressed to any **other** establishment **or legal representative** of the service provider in the Union.

~~4. Where the legal representative does not comply with its obligations under Articles 9 or 10 and the issuing authority considers that there is a serious risk of loss of data, the European Production Order or the European Preservation Order may be addressed to any establishment of the service provider in the Union.~~

Article 7a

Notification[126]

1. **Where a European Production Order is issued for the production of traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8) and of content data, the issuing authority shall notify the competent authority of the enforcing State by transmitting a copy of the EPOC to that authority** at the same time as the EPOC is ~~trans~~**submitted** to the addressee in accordance with Article 7.~~In cases where the European Production Order concerns content data, and the issuing authority has reasonable grounds to believe that the person whose data are sought is not residing on its own territory, the issuing authority shall submit a copy of the EPOC to the competent authority of the enforcing State~~

2. **Paragraph 1 of this Article does not apply if, at the time of issuing the Order, there are reasonable grounds to believe that:**

   (a) **the offence has been committed, is being committed or is likely to be committed in the issuing State, and**[127]**;**

   (b) **the person whose data are sought resides**[128] **in the issuing State.**

---

126 **ES** has a number of substantial objections against aspects of the notifications mechanism now proposed. **IE** also has concerns.

127 **BG, PT, SI** object and wish to clarify the formulation of this criterion. **BE** suggests to add "wholly or partly" after "committed".

128 EP insists on a more clear criterion for residence. Many MS oppose a too rigid definition here.

~~The notified authority may as soon as possible inform the issuing authority of any circumstances pursuant to Article 5 (7) (b) and shall endeavour to do so within 10 days. The issuing authority shall take these circumstances into account in the same way as if they were provided for under its national law and shall withdraw or adapt the Order where necessary to give effect to these grounds if the data were not provided yet. In case of withdrawal the issuing authority shall immediately inform the addressee.~~

3. When transmitting the copy referred to in paragraph 1 to the competent authority of the enforcing State, the issuing authority shall add any additional information that may be needed for the evaluation of the possibility to raise a ground for refusal[129]**.**

~~Where power to waive the privilege or immunity lies with an authority of the enforcing State, the issuing authority may request the notified authority to contact the competent authority to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.~~

~~4.~~ The notification shall ~~not~~ have a suspensive effect[130] on the obligations of the addressee ~~under~~ **as outlined in Article 9 except for emergency cases defined in Article 2(15) of** this Regulation**.**

---

129 **IE** wishes to clarify the wording to limit the scope of the "evaluation". **DE** has proposed a rewording of the last part of the provision to clarify that the scrutiny is mandatory.

130 The legislators are still discussing the issue of suspensive effect. EP insists that the suspensive effect shall apply also to emergency cases, which many MS (**ES, FR, NL, BE, PT, HU, IE**…) strongly oppose. **BG** opposes a suspensive effect in all cases. **DE** has stated that the duration of the suspensive effect must be spelled out explicitly.

Article 7b

Common European exchange system[131]

[…]

Article 8

European Production and Preservation Order Certificate

1. A European Production or Preservation Order shall be transmitted to the addressee as defined in Article 7 through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).
   The issuing or validating authority shall complete the EPOC set out in Annex I or the EPOC-PR set out in Annex II, shall sign it and shall certify its content as being accurate and correct.

~~2. The EPOC or the EPOC-PR shall be transmitted by or on behalf of the issuing authority in a secure and reliable way allowing the addressee to produce a written record and to establish the authenticity of the Certificate.~~
   ~~Where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities, the issuing authority may also choose to transmit the Certificate via these channels.~~

3. The EPOC shall contain the information listed in Article 5(5) (a) to (h), including sufficient information to allow the addressee to identify and contact the issuing authority **and the enforcing authority when necessary**. ~~The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.~~
   Where a notification in accordance with Article [7a] is required, the EPOC to the enforcing authority shall contain the information listed in Article 5(5) (a) to (j).[132]

4. The EPOC-PR shall contain the information listed in Article 6(3) (a) to (f), including sufficient information to allow the addressee to identify and contact the issuing authority.
   ~~The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.~~

---

131 The Article is under discussion and will be presented in a separate document. **BE** has underlined that the setting up of such a system shall neither interfere nor preclude the entering into force of this instrument

132 **ES** objects. **SI** suggests that it would be sufficient with a possibility for the enforcing authority to request additional information from the issuing authority.

5. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the Union accepted by the addressee. Where no language has been specified **by the service provider**, the EPOC or the EPOC-PR shall be translated into one of the official languages of the Member State where the **designated establishment or** legal representative **of the service provider are located**. **Where a notification in accordance with Article [7a] is required, the EPOC to the enforced authority shall be translated into an official language of the enforcing State**~~resides or is established~~[133].

Article 9

Execution of an EPOC

1. **Where needed in application of Article 7a, an EPOC for traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8) and for content data shall be addressed directly and simultaneously to:**

(a) the designated establishment of the service provider or, where applicable, its legal representative and

(b) the enforcing authority[134].

1a. Upon receipt of the EPOC, the service provider shall act expeditiously to preserve the data.

1b. Where the enforcing authority has not raised any ground for refusal in accordance with Article 7b within 10 days, the addressee shall ensure that the requested data are transmitted in a secure and reliable way allowing the establishment of authenticity and integrity directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the at the end of the 10 days[135] **upon receipt of the EPOC.**

---

133 **BE** suggests to add "or into another official languages of the Union accepted by that state" at the end of the phrase. The last phrase has been slightly redrafted to ensure coherence (JL remarks).

134 **SI** notes that this provision and parts of the rules in point -1c rather fits in Article 7(1)

135 **BE** and **SI** questions this 10 days rule and has suggested a flexible rule that makes it possible to transmit data also before, when it has been established that no ground for refusal is at hand.

1c. **Where notification is not needed in application of Article 7a, an EPOC for subscriber data, [other] data requested for the sole purpose of identifying the user, as defined in Article 2(8), traffic data and for content data, shall be addressed directly to the designated establishment of the service provider or, where applicable, its legal representative.** Upon receipt of such EPOC, the addressee shall ensure that the requested data are transmitted in a secure and reliable way allowing the establishment of authenticity and integrity directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days upon receipt of the EPOC.

2. In emergency cases the addressee shall transmit the requested data without undue delay, at the latest within **8** ~~6~~hours upon receipt of the EPOC. [136]

2b. **Where the addressee considers, based solely on the information contained in the EPOC, that the execution of the EPOC could interfere with immunities or privileges, or rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing State the addressee shall inform the issuing and the enforcing authority**[137]**.**

Where no notification is made pursuant to Article 7a, the issuing authority shall decide, on its own initiative or on request of the enforcing authority, taking into account the information referred to in the first subparagraph, whether to withdraw, adapt or maintain the Order.

Where a notification is made pursuant to Article 7a, the issuing authority shall decide, taking into account the information mentioned in the first subparagraph, whether to withdraw, adapt or maintain the Order. The enforcing authority may also decide to raise the grounds for refusal set out in Article 7b[138]**.**

---

136 The EP does not agree with this provision and wishes that this provision makes a clear reference to a suspensive effect. An alternative wording has been proposed. **BE** and **NL** consider that 8 hours is too long a time.

137 **ES** and **PL** question this provision as it gives the addressee specific rights. **SI** wishes to enlarge the scope of the provision.

138 The order of the wording of the last paragraphs follows suggestions from JL.

3. If the addressee cannot comply with its obligation because the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC, the addressee shall inform the issuing authority**, and, where a notification took place, the enforcing authority,** referred to in the EPOC without undue delay and ask for clarification, using the Form set out in Annex III. **At the same time, the addressee** ~~It~~ shall inform the issuing authority whether an identification and preservation was possible as set out in paragraph 6. The issuing authority shall react expeditiously and within 5 days **of the receipt of the form** at the latest. **The addressee shall ensure that the needed clarification or any correction provided by the issuing authority can be received in order, for the addressee, to fulfil its obligations set out in paragraphs 1 and 2. In the absence of a reaction from the issuing authority, the service provider shall be exempt from the obligations under paragraphs 1 and 2.** The **obligations** ~~deadlines~~ set out in paragraphs 1 and 2 shall not apply until the clarification is provided.

4. **Where** the addressee cannot comply with its obligations because of de facto impossibility due to circumstances **not attributable** ~~not created by~~ to the addressee, the addressee shall inform the issuing authority **as well as, where a notification took place, the enforcing authority referred to**~~set out~~ in the EPOC**,** without undue delay explaining the reasons, using the Form set out in Annex III. **Where these conditions are fulfilled, the issuing authority shall inform the addressees** that the EPOC does no longer need to be executed.

5. In all cases where the addressee does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons ~~listed in the Form of Annex III,~~ it shall inform the issuing authority **as well as, where a notification took place, the enforcing authority referred to in the EPOC** without undue delay and at the latest within the deadlines set out in paragraphs 1 and 2 of the reasons for this using the Form in Annex III. The issuing authority shall review the order in light of the information provided by the **addressee** ~~service provider~~ and if necessary, set a new deadline for the **addressee**~~service provider~~ to produce the data.

6. **The preservation shall be upheld until the data is produced, whether it is on the basis of the clarified European Production Order and its Certificate or through other channels, such as mutual legal assistance**[139]**. During the procedure referred to in paragraphs 1 to 5, t**he addressee shall preserve the data requested, **where possible**~~. if it does not produce it immediately, unless the information in the EPOC does not allow it to identify the data requested, in which case it shall seek clarification in accordance with paragraph 3.~~ The preservation shall be upheld until the data is produced **or until the EPOC is withdrawn.**~~, whether it is on the basis of the clarified European Production Order and its Certificate or through other channels, such as mutual legal assistance~~. **Where** the production of data and its preservation is no longer necessary, the issuing authority and where applicable pursuant to Article 14(8) the enforcing authority shall inform the addresseewithout undue delay.

Article 10

Execution of an EPOC-PR

1. Upon receipt of the EPOC-PR, the addressee shall, without undue delay, preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been ~~launched~~ **issued**, **using the form set out in Annex IV. Within the 60 days, the issuing authority can extend the duration of the preservation by an additional 30 days, where necessary, to allow for the issuing of the subsequent request for production, using the form set out in Annex IV.**
2. ~~If this issuing authority confirms~~**Where** within the time period set out in paragraph 1 the issuing authority confirms that the subsequent request for production has been **issued**~~launched~~, the addressee shall preserve the data as long as necessary to produce the data once the subsequent request for production **has been**[140]~~is~~ served.
3. ~~If~~**Where** the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay **and the preservation for the purpose of the relevant order shall cease**.

---

139 **PL** considers that the EIO should also be mentioned here.

140 JL suggestion. JL have also suggested, for the sake of linguistic coherence, not to use the term “served”, but to rather use a construction with the term “received”.

3a. Where the addressee considers, based solely on the information contained in the EPOC-PR, that the execution of the EPOC-PR could interfere with immunities or privileges, or rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing State, the addressee shall inform the competent authorities of the issuing and the enforcing state[141].
The issuing authority shall take the information mentioned in previous sub-paragraph into account, and shall decide, on its own initiative or on request of the enforcing State, taking into account the information referred to in the first subparagraph, whether to withdraw, adapt or maintain the order.

4. **Where** the addressee cannot comply with its obligation because the Certificate is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC-PR, the addressee shall inform the issuing authority set out in the EPOC-PR without undue delay and ask for clarification, using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The addressee shall ensure that **the needed clarification or any correction provided by the issuing authority can be received in order** ~~on its side the needed clarificationcan be received in order to~~ to fulfil its obligation**s** set out in paragraphs 1**, 2 and 3**. **In the absence of a reaction from the issuing authority, the service provider shall be exempt from the obligations under paragraphs 1 and 2.**
5. **Where** the addressee cannot comply with its obligations because of de facto impossibility due to circumstances **not attributable** ~~not created by~~ to the addressee, the addressee shall inform the issuing authority **set out** in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. **Where these conditions are fulfilled, the issuing authority shall inform the adressee that the EPOC-PR does not longer need to be executed.**
6. In all cases where the addressee does not preserve the requested information, for other reasons, **it**~~the addressee~~ shall inform the issuing authority without undue delay of the reasons for this in the Form set out in Annex III. The issuing authority shall review the Order in light of the justification provided by the service provider.

---

141 **ES** and **PL** question this provision.

Article 10a

Grounds for refusal for European Production Orders[142]

1. Where the issuing authority has notified the enforcing authority in accordance with Article 7a, the enforcing authority shall[143] **as soon as possible but at the latest within 10 days of the receipt of the notification, or, in emergency cases, within 8 hours, where appropriate, on the basis of all the elements**[144] **available to it, raise grounds for refusal of the Order provided that**[145]**:**[146]

(a) The data requested is protected by immunities and privileges granted under the law of the enforcing State, or;

(b) the data requested are related to rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, or;

(c) in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter, or;

(d) the execution of the Order would be contrary to the principle of ne bis in idem, or;

(e) the conduct for which the EPOC has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex IIIa, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years;

---

142 **PL** considers the draft of this provision unacceptable; it must be clarified that the grounds are to be defined narrowly and that they are optional.

143 **BE** and **PT** insist on replacing "shall" with "may".

144 **IE** wishes to analyse some of the elements of this provision in detail.

145 **NL** wishes to replace "provided with" with "in case".

146 Another possible way of formulating this provision that could be considered would be to say "Where the issuing authority has notified the competent authority of the enforcing State in accordance with Article 7a, after assessment/examination of the order, the enforcing authority shall decide, as soon as possible but at the latest within 10 days of the receipt of the notification, or, in emergency cases, within 8 hours, whether or not to raise grounds for refusal of the Order provided that…"

2. Where the enforcing authority raises a ground for refusal pursuant to paragraph 1, it shall inform the addressee and the issuing authority. The addressee shall stop the execution[147] of the Order and not transfer the data and the issuing authority shall withdraw the order.

3. Before deciding to raise a ground for refusal, the notified authority shall contact the issuing authority by any appropriate means in order to discuss the appropriate measures to take. On that basis, the issuing authority may decide to adapt or withdraw the Order. Where, following such discussions, no solution is reached, the notified authority may decide to raise grounds for refusal of the Order and inform the issuing authority as well as the addressee accordingly.

4. Where the enforcing authority decides to raise grounds for refusal of the Order pursuant to paragraph 1, it may indicate whether it objects to all use of data obtained pursuant to the order or whether the data may only be used under conditions specified by the enforcing authority[148].

5. Where power to waive the privilege or immunity as set out in paragraph (1)(a) lies with an authority of the enforcing State, the issuing authority may request the notified authority to contact the competent authority to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.

Article 11

User information and confidentiality

~~1. Addressees and, if different, service providers shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and shall refrain from informing the person whose data is being sought in order to avoid obstructing the relevant criminal proceedings. They shall only inform the person whose data are being sought if expicitly requested by the issuing authority. In this case the issuing authority shall also provide information pursuant to paragraph 4 of this Article to the addressee or, if different, to the service provider.~~

147 **DE** has noted that this wording could create confusion, as the addressee could not have started an execution if there is a suspensive effect.

148 Paragraph 4 would only be relevant if there is no suspensive effect in emergency cases. The EP thus finds this wording, as suggested by PRES, unacceptable. **NL** explicitly supports the paragraph.

~~2~~**1**. **The issuing authority shall inform the person whose data is being sought by the EPOC without undue delay about the data production**[149]**.** ~~Where the issuing authority did not request the service provider to inform the person whose data were sought in accordance with paragraph 1, the issuing authority shall inform this person.~~

2. The issuing authority may**, in accordance with national law,** delay**, restrict or omit** informing the person whose data were sought**, to the extent that,** as long as **the conditions in Article 13(3) of Directive 2016/680 are met, in which case the issuing authority shall indicate in the case file/order**[150] **the reasons for the delay, restriction or omission.** ~~it constitutes a necessary and proportionate measure to avoid obstructing criminal proceedings Theis issuing authority may delay informing the person whose data were sought as long as it constitutes a necessary and proportionate measure.~~

2a. The addresses and, if different, the service provides shall take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.

~~3. The issuing authority may abstain from informing the person whose subscriber **data** or access for the sole purpose of identifying the user, IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers, data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought.~~

4. **When informing the person, the issuing authority shall include** information about available remedies pursuant to Article 17~~shall be included~~.

Article 12

Reimbursement of costs

The service provider may claim reimbursement of **its** ~~their~~ cost~~s~~ by the issuing State, if **that**~~this~~ is provided by the national law of the issuing State for domestic orders in similar situations, in accordance with th**atese** national **law** provisions. Member States shall inform the Commission about **their national** rules for reimbursement **and the Commission** ~~who~~ shall make them public.

---

149 JL has noted that it must be clarified from which point the "undue delay" applies, from reception or from production.

150 The Presidency insists on „case file".

~~*Article 12a*~~

~~*Limitations to the use of data obtained*~~

~~1. In case the person whose data are sought is not residing on the territory of the issuing State, and transactional or content data has been obtained by the European Production Order and the issuing authority receives information that these data are protected by privileges or immunities granted under the law of the enforcing State, or is subject, in the enforcing State, to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, or if invoked by that Member State, disclosure of these data would impact its fundamental interests such as national security and defence, the competent authorities in the issuing State shall ensure during the criminal proceedings that these grounds are taken into account in the same way as if they were provided for under their national law. The competent authorities may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust.~~

~~2. Where power to waive the privilege or immunity lies with an authority of the enforcing State, the competent authority in the issuing State may request the enforcing or notified authority to contact the competent authority of the enforcing State to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the competent authority in the issuing State may request the authority concerned to exercise that power.~~

Article 12b

Speciality principle[151]

1. Electronic evidence shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except:
   a) for the purpose of proceedings for which a European Production Order could have been issued in accordance with Article 5(3) and (4); or
   b) for preventing an immediate and serious threat to public security of the issuing State or its essential interests.
2. Electronic evidence obtained in accordance with this Regulation may only be transmitted to another Member State:
   a) for the purpose of proceedings for which a European Production Order could have been issued in accordance with Article 5(3) and (4); or

151 The EP still wishes to discuss this Article.

b) for preventing an immediate and serious threat to public security of that Member State or its essential interests.

3. Electronic evidence obtained in accordance with this Regulation may only be transferred to a third country or to an international organisation pursuant to conditions of paragraph 2, points a) and b) of this Article and Chapter V of the Directive (EU) 2016/680.

Chapter 3: Sanctions and enforcement

Article 13

Sanctions

1. Without prejudice to national laws which provide for the imposition of criminal sanctions, Member States shall lay down the rules on pecuniary sanctions applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 (~~1~~**3**) **and in accordance with Article 14(10)** of this Regulation and shall take all **measures** necessary ~~measures~~ to ensure that they are implemented. **The sanctions provided for shall be effective, proportionate and dissuasive.** Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. ~~The Member States shall ensure that **the** pecuniary sanctions provided for **by national laws of Member States** are effective, proportionate and dissuasive.~~[152]

   Member States shall ensure that pecuniary sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed.

1a. Without prejudice to data protection obligations, service providers shall not be held liable in Member States for the consequences resulting from compliance with an EPOC or an EPOC-PR.

[152] The wording of the two first paragraphs has been adapted to the joint handbook. The meaning should not have changed.

Article 14

Procedure for enforcement

1. **Where** ~~If~~ the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority **and where the enforcing authority has not invoked any of the grounds for refusal as provided for in Article 7b**, the issuing authority may **request** ~~transfer to~~ the competent authority in the enforcing State **to enforce** the European Production Order ~~with the EPOC~~ or the European Preservation Order ~~with the EPOC-PR.~~ ~~with a view to its enforcement by any means capable of producing a written record under conditions allowing the enforcing authority to establish authenticity~~. To this end, the issuing authority shall translate the ~~Order, the~~ Form set out in Annex III filled out by the addressee and any relevant documents **by any means capable of producing a written record under conditions allowing the enforcing authority to establish authenticity. It shall translate the Order and any document transferred** into one of the languages accepted by this Member State and shall inform the addressee of the transfer.
2. Upon receipt, the enforcing authority shall without further formalities recognise and take the necessary measures for enforcement of
   (a) a European Production Order unless the enforcing authority considers that one of the grounds provided for in paragraph 4 apply, or
   (b) a European Preservation Order unless the enforcing authority considers that one of the grounds provided for in paragraph 5 apply.

   The enforcing authority shall take the decision to recognise the Order without undue delay and no later than 5 working days after the receipt of the Order.

~~2a. Article 5(8) shall apply mutatis mutandis.~~

3. ~~Where~~ **T**he enforcing authority ~~recognises the Order, it~~ shall formally require the addressee to comply with the relevant obligation, informing the addressee of the possibility to oppose the enforcement by invoking the grounds listed in paragraphs **[below]** ~~4 point (a) to (e) or paragraph 5~~, as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition[153].
4. ~~Recognition or~~**Enforcement** of the European Production Order **shall** ~~may~~ only be denied on the basis of the following grounds:
   (a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;

[153] **ES** calls for the inclusion of a reference to the possibility of adopting coercive measures to preserve or obtain the data requested, where technically possible.

(b) the European Production Order has not been issued for criminal offence provided for by Article 5(4);

(c) the addressee could not comply with the EPOC because of de facto impossibility **due to circumstances not attributable to the addressee** or because the EPOC contains manifest errors;

(d) the European Production Order does not concern data stored by or on behalf of the service provider at the time of receipt of EPOC;

(e) the service is not covered by this Regulation;

(f) **based on the sole information contained in the EPOC, it is apparent that in exceptional situations, there are substantial grounds to believe on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter** ~~one of the grounds referred to in Article 12a (1) apply~~[154].

5. ~~Recognition or~~ **The** enforcement of the European Preservation Order **shall** ~~may~~ only be denied on the basis of the following grounds:

(a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4[155];

(b) the **addressee** ~~service provider~~ could not comply with the EPOC-PR because of de facto impossibility impossibility **due to circumstances not attributable to the addressee** or because the EPOC-PR contains manifest errors;

(c) the European Preservation Order does not concern data stored by or on behalf of the service provider at the time of the EPOC-PR;

(d) the service is not covered by the scope of the present Regulation

(e) **based on the sole information contained in the EPOC-PR, it is apparent that it in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter.**[156]

---

154 **SE** proposes to add ground for refusal relating to immunity, privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the executing State here. **SI** wishes to see a references to national constitutional law here.

155 **DE** notes that this provision compared with Article 4(1)(b) could lead to uncertainty as regards which authority is competent.

156 **SI** wishes to see a references to national constitutional law here.

6. In case of an objection by the addressee[157] pursuant to paragraphs 4 ~~point (a) to (e)~~ and 5, the enforcing authority shall decide whether **or not** to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority in accordance with paragraph 7. **The enforcing authority shall notify its decision without undue delay to the addressee and the issuing authority.**
7. Before deciding not to ~~recognise or~~ enforce the Order in accordance with paragraph ~~2 and~~ 6, the enforcing authority shall consult the issuing authority by any appropriate means[158]. Where appropriate, it shall request further information from the issuing authority. The issuing authority shall reply to any such request within 5 working days.
8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.
9. If the enforcing authority obtains the data from the addressee, it shall transmit it to the issuing authority **without undue delay.** ~~within 2 working days, unless the data concerned is protected by an immunity or privilege or by rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media under its own domestic law or it impacts its fundamental interests such as national security and defence. In such case, it shall inform the issuing authority of the reasons for not transmitting the data.~~
10. In case the addressee does not comply with its obligations under a recognised Order whose enforceability has been confirmed by the enforcing authority, that authority shall impose a pecuniary sanction in accordance with **Article 13**~~its national law~~[159]. An effective judicial remedy shall be available against the decision to impose a fine.

---

157 **ES, FR** and **PL** note its opposition to the possibility for the service providers to object to the enforcement of orders.

158 **DE** questions if the consultation obligation should not also apply in other cases, where it is considered not to enforce and order.

159 **ES** calls for the inclusion of a reference to the possibility of adopting coercive measures to preserve or obtain the data requested, where technically possible.

Chapter 4: Remedies

[…]

Article 16

Review procedure in case of conflicting obligations

1. ~~If~~ **Where** the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country, it shall**, by way of reasoned objection**[160]**,** inform the issuing authority **and the enforcing authority** of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5) and (6).
2. The reasoned objection **shall** ~~must~~ include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country. **The reasoned objection**~~It~~ shall be filed no later than 10 days after the date on which the addressee was served with the EPOC. Time limits shall be calculated in accordance with the national law of the issuing authority.
3. The issuing authority shall review the European Production Order on the basis of the reasoned objection **and any input provided by the enforcing state**. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.
4. The competent court shall first assess whether a conflict exists, based on an examination of whether
   (a) the third country law applies based on the specific circumstances of the case in question and if so,
   (b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned[161].

---

160 Suggestion by JL.

161 **BG** has noted some hesitations against the regime described in this provision and the subsequent points 5 and 5b.

5. **Where**~~If~~ the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. **Where**~~If~~ the competent court establishes that the third country law, when applied to the specific circumstances of the case under examination, prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or lift the Order. That assessment shall in particular be based on the following factors while giving particular weight to the factors referred to in points (a) and (b):

(a) the interest protected by the relevant law of the third country, including fundamental rights as well as other interests preventing disclosure of the data in particular national security interests of the third country;

(b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated *inter alia* by:

– the location, nationality and residence of the person whose data is being sought and/or of the victim(s),

– the place where the criminal offence in question was committed;

(c) the degree of connection between the service provider and the third country in question; in this context, the data storage location by itself does not suffice in establishing a substantial degree of connection;

(d) the interests of the investigating State in obtaining the evidence concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner;

(e) the possible consequences for the addressee or the service provider of complying with the European Production Order, including the sanctions that may be incurred.

5b. The court may seek information from the competent authority of the third country taking into account Directive 2016/680, in particular its Chapter V and to the extent that such the transmission does not obstruct the relevant criminal proceedings. **Information shall in particular be requested from the competent authority of the third country by the issuing State where the conflict concerns fundamental rights *of the third country* or fundamental interests of *the* third country related to national security and defence.**

6. If the competent court decides to lift the Order, it shall inform the issuing authority and the addressee. If the competent court determines that the Order is to be upheld, it shall inform the issuing authority and the addressee, who shall proceed with the execution of the Order.

6a. The issuing authority shall inform the enforcement authority about the outcome of the proceedings.

Article 17

Effective remedies

1. Without prejudice to further legal remedies available in accordance with national law, any person~~s~~ whose data w**ere**~~as~~ sought via a European Production Order shall have the right to effective remedies against the European Production Order. Where that person is a suspect or accused person, the person shall have the right to effective remedies during the criminal proceedings ~~for~~ in which the data were being used. Such remedies shall be without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679[162].

3. **The** ~~Such~~ right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality, **without prejudice to the guarantees of fundamental rights in the enforcing State**[163]**.**

4. **When applying** ~~Without prejudice to~~ Article 11**(1) of this Regulation**, ~~the issuing authority shall take the appropriate measures to ensure that~~ information ~~is~~ **shall be** provided about the possibilities under national law **and this Regulation** for seeking remedies**, including about when such remedies apply,** and ensure that they can be exercised effectively.

~~5. The same time-limits or other conditions for seeking a remedy in similar domestic cases shall apply here and in a way that guarantees effective exercise of these remedies for the persons concerned.~~

6. Without prejudice to national procedural rules, ~~Member States shall ensure that in criminal proceedings in~~ the issuing State **and any other Member State the electronic evidence has been transmitted to or from** shall ensure that the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the European Production Order.

---

162 **DE** has demanded to explicitly provide in the Regulation itself for remedies against preservation orders.

163 **DE** has demanded to explicitly provide in the Regulation itself for remedies in the executing state.

Chapter 5: Final provisions

Article 18a

Language

~~Each Member State shall indicate, if and which language(s) in addition to their official language(s) they will accept for the transmission of the EPOC or EPOC-PR, and/or of a European Production Order and a European Preservation Order in case of enforcement.~~

Member States may decide, at any time, that they will accept translations of EPOCs and EPOC-PRs in one or more official language(s) of the Union in addition to their official language(s) and shall indicate such a decision in a written declaration submitted to the Commission. The Commission shall make the declarations available to all Member States and to the European Judicial Network.

Article 19

Monitoring and reporting

1. By *[date of application of this Regulation]* at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the means by which and the intervals at which the data and other necessary evidence will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence.
2. In any event, Member States shall collect[164] and maintain comprehensive statistics from the relevant authorities. The data collected shall be sent to the Commission each year by 31 March for the preceding calendar year and shall, as far as possible, include:
   (a) the number of EPOCs and EPOC-PRs issued by **the** type of data requested, ~~service providers~~ **the** addresse**s** and **the** situation (emergency case or not~~, ex-post validation~~);
   (aa) the number of EPOCS issued under emergency case derogations[165]**;**
   (b) the number of fulfilled and non-fulfilled EPOCs **and EPOC-PRs** by **the** type of data requested, **the** ~~service providers~~ addresse**s** and **the** situation (emergency case or not);
   (c) for fulfilled EPOCs, the average duration for obtaining the requested data from the moment the EPOC is issued to the moment it is obtained, by **the** type of data requested, **the**~~service provider~~ addresse**e** and **the** situation (emergency case or not);

---

164 **ES** considers that parts of this obligation will be extremely difficult and burdensome.

165 **BE** wishes to clarify the difference between points a) and aa).

(ca) for fulfilled EPOC-PRs, the average duration for the respective subsequent request for production following the EPOC-PR, from the moment the EPOC-PR is issued to the moment the request for production is issued, by the type of data requested and the addressees[166]**;**

(d) the number of European Production Orders **or European Preservation Orders** transmitted and received for enforcement to an enforcing State by **the** type of data requested, **the** ~~service providers~~ addresse**s** and **the** situation (emergency case or not) and the number thereof fulfilled;

(e) the number of legal remedies **used** against European Production Orders [**or European Preservation Orders**] in the issuing State and in the enforcing State by **the** type of data requested;

(f) the number of cases where no ex-post validation was granted.

(g) **an overview of the costs claimed by service providers related to the execution of the EPOC or the EPOC-PR and the costs reimbursed by the issuing authorities.**

3. Service providers may collect, maintain and publish statistics if any such data were collected**, in accordance with existing data protection principles. If any such data were collected,** they may be sent to the Commission by 31 March for the preceding calendar year and may, as far as possible, include:

(a) the number of EPOCs and EPOC-PRs received by **the** type of data requested, Member States and situation (emergency case or not);

(b) the number of fulfilled and non-fulfilled EPOCs **and EPOC-PRs** by **the** type of data requested, **the** Member States and **the** situation (emergency case or not);

(c) for fulfilled EPOCs, the average duration for providing of the requested data from the moment the EPOC is received to the moment it is provided, by **the** type of data requested, **the** Member State and **the** situation (emergency case or not).

(ca) for fulfilled EPOC-PRs, the average duration for the respective subsequent request for production following the EPOC-PR, from the moment the EPOC-PR is issued to the moment the request for production is issued, by the type of data requested and the Member State;

---

166 **PL** opposes this provision.

3a. The Commission shall, by [30 June] of each year, publish a report containing the data referred to in paragraphs 2 and 3 in a compiled form, subdivided into Member States and type of service provider.

Article 20

Amendments to the Certificates and the Forms

The Commission shall adopt delegated acts in accordance with Article 21 to amend Annexes I, II, III **and IV** in order to effectively address a possible need for improvements regarding the content of EPOC and EPOC-PR forms and of forms to be used to provide information on the impossibility to execute the EPOC or EPOC-PR.

Article 21

Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 20 shall be conferred for an indeterminate period of time from *[date of application of this Regulation]*.
3. The delegation of powers referred to in Article 20 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[167].
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 20 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or of the Council.

[167] OJ L 123, 12.5.2016, p. 13.

Article 22

Notifications

1. By ***[12 months***[168] ***before the*** *date of application of this Regulation]* each Member State shall notify the Commission of the following:
   (a) the authorities which, in accordance with its national law, are competent in accordance with to Article 4 to issue, validate, transmit and/or receive European Production Orders and European Preservation Orders or the notifications thereof;
   (b) the ~~enforcing~~ authority or authorities which are competent, **in accordance with Article 7a, for the notification, and, in accordance with Article 14,** to enforce European Production Orders and European Preservation Orders on behalf of another Member State;
   (c) the ~~courts~~ competent **authorities** to deal with reasoned objections by addressees in accordance with Article 16;
   (d) languages accepted for the **notification and the** transmission of the EPOC or EPOC-PR and/or a European Production Order and a European Preservation Order, in case of enforcement in accordance with Article 18a.
2. The Commission shall make the information received under this Article publicly available, either on a dedicated website or on the website of the European Judicial Network **in criminal matters** referred to in Article 9 of the Council Decision 2008/976/JHA.

Article 23

Relationship to other instruments, agreements and arrangements

1. 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 this Regulation.
2. **Member States shall notify the Commission by ... [date of the application of the Regulation] of the existing agreements and arrangements referred to in paragraph 1 which they will continue to apply. Member States shall also notify the Commission within three months of the signing of any new agreement or arrangement referred to in paragraph 1.**

[168] **IE** opposes the 12 month time period.

Article 24

Evaluation

By *[**X** years from the date of application of this Regulation]* at the latest, the Commission shall carry out an evaluation of the Regulation**. The Commission shall transmit this** ~~and present a~~ report to the European Parliament ~~and to~~ the Council**, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights. This overall evaluation** ~~on the functioning of this Regulation, which~~ shall include an assessment of the **application of this Regulation and of the results that have been achieved with regard to the objectives that were set and of the impact on fundamental rights.** ~~need to enlarge its scope. If necessary, the report shall be accompanied by legislative proposals.~~ The evaluation shall be conducted according to the Commission's better regulation guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

Article 25

Entry into force

This Regulation shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

It shall apply from *[~~24~~**X**[169] months after its entry into force]*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg,

For the European Parliament *For the Council*

The President *The President*

---

169 **IE** would only agree to the 24 months timeline of the General Approach.

ANNEX 2

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 53 and 62 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[170],

Acting in accordance with the ordinary legislative procedure,

Whereas**:**

(1) Network-based services can in principle be provided from anywhere and do not require a physical infrastructure, **premisess** ~~corporate presence,~~ or staff in the **relevant** country where the service~~s are~~ **is** offered, nor in the internal market itself. As a consequence, it can be difficult to apply and enforce obligations laid down in national and Union law which apply to the service providers concerned, in particular the obligation to comply with an order or a decision by a judicial authority. This is the case in particular in criminal law, where Member States' authorities face difficulties with serving, ensuring compliance and enforcing their decisions, in particular where relevant services are provided from outside their territory.[171]

[170] OJ C , , p. .

[171] Modifications proposed by the EP.

(2) Against that background, Member States have taken a variety of disparate measures to more effectively apply and enforce their legislation. This includes measures for addressing service providers to obtain electronic evidence that is of relevance to criminal proceedings.

(3) To that end, some Member States have adopted, or are considering adopting, legislation imposing mandatory legal representation within their own territory, for a number of service providers offering services in that territory. Such requirements create obstacles to the free provision of services within the internal market.

(4) There is a significant risk that**, in the absence of a Union-wide approach,** ~~other~~ Member States will try to overcome existing shortcomings related to gathering **electronic** evidence in criminal proceedings by means of imposing disparate national obligations in the absence of a Union-wide approach. This is bound to create further obstacles to the free provision of services within the internal market. [172]

(5) ~~Under the current circumstances, the resulting~~ **The absence of a Union-wide approach results in** legal uncertainty affect**ing** both service providers and national authorities. Disparate and possibly conflicting obligations are set out for service providers established or offering services in different Member States, which also subject them to different sanction regimes in case of violations. This divergence in the framework of criminal proceedings will likely further expand because of the growing importance of communication and information society services in our daily lives and societies. The foregoing not only represents an obstacle to the proper functioning of the internal market but also entails problems for the establishment and correct functioning of the Union's area of freedom, security and justice.[173]

[172] Modifications proposed by the EP.
[173] Modifications proposed by the EP.

(6) To avoid such fragmentation and to ensure that undertakings active in the internal market are subject to the same or similar obligations, the Union has adopted a number of legal acts in related fields such as data protection[174]. To increase the level of protection for the data subjects, the rules of the General Data Protection Regulation[175] provide for the designation of a legal representative in the Union by controllers or processors not established in the Union but offering goods or services to individuals in the Union or monitoring their behaviour if their behaviour takes place within the Union, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, 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 if the controller is a public authority or body. **For service providers established in the Union, the General Data Protection Regulation[3] further provides for the determination of those establishments where the decisions on the purposes and means of the processing of personal data are taken.** [176]

---

174 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

175 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 (OJ L 119, 4.5.2016, p. 1).

176 Modifications proposed by the EP.

(7) By setting out harmonised rules on the **designation of establishments and the appointment of** legal **representatives** of certain service providers in the Union for receipt of, compliance with and enforcement of decisions issued by competent authorities in the Member States for the purposes of gathering **electronic** evidence in criminal proceedings, the existing obstacles to the free provision of services should be removed, as well as the future imposition of divergent national approaches in that regard should be prevented. Level playing field for service providers should be established. This should not affect obligations on service providers deriving from other EU legislation. Moreover, more effective criminal law enforcement in the common area of freedom, security and justice should be facilitated.[177]

(8) The legal **designated establishment and** representative at issue should serve as an addressee for **decisions and** orders ~~and decisions and for orders and decisions pursuant to Union legal instruments falling within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union~~ for **the purpose of** gathering **electronic** evidence **on the basis of Regulation XXX/XXX Directive 2014/41/EU, the Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of the Union,** including where those orders and decisions are transmitted in form of a certificate **without prejudice to the powers of national authorities in accordance with Union and national law to address directly service providers via a designated establishment or legal representative on their territory, for the purposes of gathering electronic evidence in criminal proceedings**. ~~This includes both instruments that permit the direct serving of orders in cross-border situations on the service provider or its legal representative, such as the [Regulation on European Production and Preservation Orders for electronic evidence in criminal matters ("Regulation")[178]], and other instruments for judicial cooperation applicable between the Member States, notably those falling within the scope of Title V, Chapter 4, such as the Directive on the European Investigation Order[179] and the 2000 Mutual Legal Assistance Convention[180].~~

---

177 Modifications proposed by the EP.

178 Regulation of the European Parliament and of the Council on European Production and preservation orders for electronic evidence in criminal matters

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

180 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the

Recourse to the **designated establishment or** legal representative should be in accordance with the procedures-set out in the instruments and legislation applicable to the judicial proceedings. The competent authorities of the Member State where **the designated establishment is established** or the legal representative resides or is established should act in accordance with the role set out for them in the respective instrument if and where an involvement is foreseen. [181]

(9) **Depending on whether service providers are established in the Union, are established in Member States not taking part in a legal instrument referred to in this Directive or are not established in the Union,** Member States should ensure that service providers have the obligation to designate **at least one establishment or** legal representative by [6 months from the transposition deadline of this Directive] or from the moment service providers start offering services in the Union for those service providers that will start offering services after [6 months from the transposition deadline of this Directive]. [182]

(10) The obligation to designate **an establishment or** a legal representative should apply to service providers that offer services in the Union, meaning in one or more Member States. Situations where a service provider is established on the territory of a Member State and offers services exclusively on the territory of that Member State, should not be covered by this Directive. [183]

(11) ~~Notwithstanding the designation of a legal representative,~~ **For the purpose of gathering electronic evidence in criminal proceedings,** Member States should be able to continue addressing service providers[184] ~~established~~ on their territory, ~~be it in~~ **for** purely domestic situations **in accordance with their respective national laws or**, ~~be it~~ after receipt of a request for assistance under legal instruments on mutual legal assistance and on mutual recognition in criminal matters.

Member States of the European Union, OJ C 197, 12.7.2000, p. 1 and its Protocol, OJ C 326, 21.11.2001, p. 2.

181 Modifications proposed by the EP, with reference made to Article 1 in the Directive.

182 Modifications proposed by the EP.

183 Modifications proposed by the EP.

184 EP wishes to add the words "a designated establishment or a legal representative" here. Commission services don't agree with this proposal as well as **AT, DE, IE** and **FR. BE** cannot accept the mention of "designated" establishment (mainly referring to proposal to Art. 1). **HU** supports the position of COM but is flexible. **BG** believes that proposed solution is acceptable compromise. The Presidency intends to oppose the addition of "*a designated establishment or a legal representative*".

~~Likewise~~ Member States should **also** be able to continue addressing the Member States where service providers are established with instruments falling within the scope of Title V, Chapter 4, **TFEU** such as the Directive on the European Investigation Order and **the Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of Draft agreement the Union**~~the 2000 Mutual Legal Assistance Convention~~.[185] **Member States should not circumvent the principles set out in this Directive and in Regulation XXXX/XXX**[186].

(12) ~~The~~ Determin**ingation** ~~-~~whether a service provider offers services in the Union requires an assessment whether **it is apparent that** the service provider **envisages offering services to data subjects, either** ~~enables~~ legal or natural persons in **one or more Member States in** the Union ~~to use its services~~. However, the mere accessibility of an online interface**, as** for instance the accessibility of the **website or an e-mail address or other contact details of a** service provider~~'s~~ or an intermediary~~'s website or of an email address and of other contact details)~~ **, or the use of a language also used in a Member States,** ~~taken in isolation~~ should **be consider insufficient to ascertain such intention** ~~not be a sufficient condition~~ for the application of this Directive. [187]

(13) A substantial connection to the Union should also be relevant to determine the ambit of application of th**e present** Directive. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be based on specific factual criteria such as **the existence** of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States **should** be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services.

---

185 EP wishes to add „The possibilities currently provided by domestic law to address service providers on their own territory". PRES suggests to not include this text. According to **IE** the effect of the leaving out this text is unclear and suggests to add „Notwithstanding" at the begging of the sentence.

186 The text is based on a Presidency proposal from June this year. It has been pointed out that this recital must be redrafted and clarified. The EP has suggested some additional wording.

187 Modifications proposed by the EP.

The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing **a** customer service in the language generally used in that Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302[188] cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union. The same considerations should apply to determine whether a service provider offers services in a Member State. [189]

(14) Service providers obliged to designate a legal representative should be able to choose to that effect an existing establishment in a Member State, be it a corporate body or a branch, agency, office or a main seat or headquarters, and also more than one legal representative. This legal representative could also be a third party, which could be shared between several service providers, in particular small and medium-sized enterprises. Nevertheless, a corporate group should not be forced to designate multiple representatives, one for each undertaking part of that group, but can designate one legal representative for the group. Different instruments falling within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union apply in the relationships between Member States when gathering evidence in criminal proceedings. As a consequence of this 'variable geometry' that exists in the common area of criminal law, there is a need to ensure that the Directive does not facilitate the creation of further disparities or obstacles to the provision of services in the internal market by allowing service providers offering services on their territory to designate legal representatives within Member States that do not take part in relevant legal instruments, which would fall short of addressing the problem.

---

188 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (OJ L 601, 2.3.2018, p. 1).

189 Modifications proposed by EP, which refers to the Regulation and notes that some parts of the recital will need to be discussed again.

Therefore, at least one representative should be designated in a Member State that participates in the relevant Union legal instruments to avoid the risk of weakening the effectiveness of the designation provided for in this Directive and to make use of the synergies of having a legal representative for the receipt of, compliance with and enforcement of decisions and orders issued in the context of gathering evidence in criminal proceedings, including under the [Regulation], the Directive on the European Investigation Order or the 2000 Mutual Legal Assistance Convention. In addition, designating a legal representative, which could also be utilised to ensure compliance with national legal obligations, makes use of the synergies of having a clear point of access to address the service providers for the purpose of gathering evidence in criminal matters[190]. [191]

(15) Service providers should be free to choose in which Member State they designate their **designated establishment or, where applicable,** legal representative, and Member States may not restrict this free choice, e.g. by imposing an obligation to designate **the designated establishment or** the legal representative on their territory. However, the Directive also contains certain restrictions with regard to this free choice of service providers, notably that the **designated establishment** ~~legal representative~~ should be established **or where applicable, the legal representative residing** in a Member State where the service provider provides services or is established, as well as the obligation to designate a **designated establishment or** legal representative in one of the Member States **a legal instrument referred to in this Directive** ~~participating in judicial cooperation instruments falling within Title V of the Treaty.~~ The sole designation of a legal representative should not be considered to constitute an establishment of the service provider. [192]

(16) The service providers most relevant for gathering evidence in criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Directive. Providers of electronic communication services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services.

---

[190] **NL** we would like to keep the possibility for service providers established in the Union to designate a legal representative collectively as it is important for SMEs. The Presidency intends to clarify this possibility in a recital.

[191] EP has suggested to delete recital 14 altogether.

[192] Modifications proposed by EP, which refers to the Regulation.

This Directive should also be applicable to other information society service~~s~~ providers within the meaning of Directive (EU) 2015/1535 that do not qualify as electronic communications service~~s~~ providers, but offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf. This should be in line with the terms used in the Budapest Convention on Cybercrime. Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, i.e. technical operations to produce or alter data by means of computer processing power.

(16) The categories of service providers included here are, for example online marketplaces providing consumers ~~or~~ and businesses the ability to communicate with each other and other hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms. Where an information society service provider does not provide its users the ability to communicate with each other, but only with the service provider, or does not provide the ability to process or to store data, or where the ability to store/process data is not an essential part of the service provided to users, such as legal, architectural engineering and accounting services provided online at a distance, it would not fall within the scope of the definition, even if within the definition of information society services pursuant to Directive (EU) 2015/1535.[193]

(17) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and privacy and proxy service providers or regional internet registries for internet protocol ('IP') addresses, are of particular relevance when it comes to the identification of actors behind malicious or compromised web sites. They hold data that **could** ~~is of particular relevance for criminal investigations as it can~~ allow for the identification of an individual or entity behind a web site used in **a** criminal activity, or the victim of **a** criminal activity ~~in the case of a compromised web site that has been hijacked by criminals~~. [194]

---

193 The EP has indicated that looks forward to suggestions from Council on how to reformulate this recital.

194 Modifications proposed by EP.

(18) ~~The legal representative should be able to comply with decisions and orders addressed to them by Member States' authorities on behalf of the service provider, which should take the appropriate measures to ensure this result, including sufficient resources and powers.~~ **Member States should ensure that service providers established or offering services on their territory provide their designated establishments and legal representatives with the necessary powers and resources to comply with those decisions and orders received from any Member State. Member States should also verify that the designated establishments or legal representatives residing on their territory have received from the service providers the necessary powers and resources to comply with decisions and orders received from any Member State and that they cooperate with the competent authorities when receiving those decisions and orders, in accordance with the applicable legal framework.** The absence of such measures or their shortcomings should not serve as grounds to justify non-compliance with decisions or orders falling into the ambit of application of by this Directive~~, neither for the service provider nor its legal representative~~. ~~Neither should service providers be able to exculpate themselves due to missing or ineffective internal procedure, as they are responsible for providing the necessary resources and powers to guarantee compliance with orders and national decisions. Nor should the legal representative be able to exculpate himself by claiming for example he is not empowered to deliver data. The service provider and its legal representative(s) should remain free to allocate among themselves the tasks of identifying and accessing the requested evidence as long as decisions and orders addressed to them are complied with.~~**To this end, Member States should ensure that both the designated establishment or the legal representative and the service provider can be held jointly and severally liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders falling within the scope of this Directive, with the effect that each of the designated establishment or the legal representative and the service provider may be sanctioned for non-compliance. In particular, the lack of appropriate internal procedures between the service provider and the designated establishment or the legal representative cannot be used by either side as a justification for non-compliance with those obligations. Joint and several liability should not apply for actions or omissions of either the service provider or the legal representative or the designated establishment which constitute a criminal offence in the Member State applying the sanction.** [195]

---

195 Modifications proposed by EP, which notes that the recital can be shortened and also refers

(19) **Member States should ensure that each s**ervice provider **established or offering services in their territory notifies in writing the central authority of** the Member State **where its designated establishment is established or where its legal representative resides, their** contact details **and any changes thereof**.

The notification should also provide information about the languages in which **the designated establishment or** the legal representative can be addressed, which should include one or more of the official languages in accordance with the national law of the Member State where **the designated establishment is established or** the legal representative resides, but may include other official languages of the Union, such as the language of its headquarters.

When the service provider designates **several designated establishments or legal reprentatives in accordance with this Directive, Member States should ensure that such service providers indicate, for each designated establishment or legal representative, the precise territorial scope of its designation. The territory of all the Member States taking part in the instruments within the scope of this Directive should be covered. Member States should ensure that their respective competent authorities address all their decisions and orders in application of this Directive to the indicated designated establishment or legal representative of this service provider.**

Member States should ensure that the information notified to them in accordance with this Article is publicly available on a dedicated internet page of the European Judicial Network in criminal matters. Member States should ensure that this information is regularly updated. This information may be further disseminated to facilitate access by competent authorities.

Member States should ensure that the information notified to them in accordance with this Directive is publicly available on a dedicated internet page of the European Judicial Network in criminal matters to facilitate coordination between Member States and use of the designated establishments or legal representative by authorities from another Member State. Member States should ensure that this information is regularly updated. The data may also be further disseminated to facilitate access to this data by competent authorities, such as via dedicated intranet sites or forums and platforms. [196]

---

to Article 3(4) and 3(8).

196 Modifications proposed by EP, which also refers to Article 4.

~~**or** more than one legal representative, it may also notify considerations to determine which one should be addressed.These considerations should be followed except where the competent authorities consider it is necessary to depart from those considerations on a case-by-cases basis e.g. when the legal representative is unavailable or uncooperative. Where the competent authorities, by way of exception, depart from these considerations they should only address a legal representative established in a Member State participating in the respective instrument., Member States should publish and keep up-to-date the relevant information for their country on a dedicated internet page of the European Judicial Network in criminal matters to facilitate coordination between Member States and use of the legal representative by authorities from another Member State. The data may also be further disseminated to facilitate access to this data by competent authorities, such as via dedicated intranet sites or forums and platforms.~~

(20) The service provider should be subject to effective, proportionate and dissuasive sanctions for the infringement of its obligations **deriving from this Directive. To this end, Member States should, by the date set out in this Directive, notify the Commission of those rules and of those measures and should notify it, without delay, of any subsequent amendment affecting them. Member States should also inform the Commission on an annual basis about non-compliant service providers, relevant enforcement action taken against them and the sanctions imposed.** ~~to designate a legal representative, to entrust the legal representative with the necessary powers and resources to comply with decisions and orders, establish the appropiate procedures and to notify the information related thereto. The service provider and the legal representative should be subject to effective, proportionate and dissuasive sanctions for the systematic infringement by the legal representative of the obligation to cooperate with the competent authorities when receiving decisions and orders. Member States should ensure that both the designated legal representative and the service provider can be held jointly and severally liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders. Jointly and severally liable means that either the legal representative or the service provider may be sanctioned for non-compliance by either of them with any of the obligations under this Directive. Joint and several liability should not apply for actions or omissions of either the service provider or the legal representative which constitute a criminal offence under the law of the Member State imposing the sanction.~~

Under no circumstances should the sanctions determine a ban, permanent or temporary, of service provision. Member States should coordinate their enforcement action where a service provider offers services in several Member States. Central authorities should coordinate to ensure a coherent and proportionate approach.

The Commission could facilitate such coordination if necessary, but needs to be informed of cases of infringement. This Directive does not govern the contractual arrangements for transfer or shifting of financial consequences between service providers**, designated establishments** and legal representatives of sanctions imposed upon them. [197]

(20a) When determining ~~in the individual case~~ the appropriate ~~and proportionate~~ sanction~~, the competent authorities should also take into account the financial capacity of the service provider.~~**applicable to infringements of service providers, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence and whether the service provider was held responsible for similar previous breaches. Particular attention should, in this respect, be given to micro enterprises.** [198]

(21) This Directive is without prejudice to the investigative powers of authorities in civil or administrative proceedings, including where such proceedings can lead to sanctions.

(22) In order to ensure the application of the Directive in a consistent manner, additional mechanisms for the coordination between Member States should be put in place. For that purpose, Member States should designate **one or more** central authorit**ies** that can provide central authorities in other Member States with information and assistance in the application of the Directive, in particular where enforcement actions under the Directive are considered. This coordination mechanism should ensure that relevant Member States are informed of the intent of a Member State to undertake an enforcement action. In addition, Member States should ensure that central authorities can provide each other any relevant information and with assistance in those circumstances, and cooperate with each other where relevant. Cooperation amongst central authorities in the case of an enforcement action may entail the coordination of an enforcement action between competent authorities in different Member States.

---

197 Modifications proposed by EP, which notes that the recital can be shortened and also refers to recital 18 and Articles 5(1) and 5(2).

198 Modifications proposed by EP, which refers to the Regulation.

It should aim to avoid positive or negative conflicts of competence. For the coordination of an enforcement action, central authorities should also involve the Commission where relevant. The ~~existence of the~~ obligation of these authorities to cooperate does not prejudice the right of an individual Member State to impose sanctions on service providers that fail to comply with their obligations under the Directive.

The designation and publication of information about central authorities will facilitate the notification by service providers of the designation and contact details of its **designated establishment or** legal representative to the Member State where its **designated establishment is established or** legal representative resides **and its** ~~or is established of the designation and~~ contact details. **To this end, Member States should inform the Commission of their designated central authority, or central authorities and the Commission should forward a list of designated central authorities to the Member States and make it publicly available.**[199]

(23) Since the objective of this Directive, namely to remove obstacles to the free provision of services in the framework of gathering **electronic**[200] evidence in criminal proceedings, cannot be sufficiently achieved by the Member States, but can rather, by reason of the borderless nature of such services, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(24) The European Data Protection Supervisor was consulted in accordance with ~~Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council~~ Article **42(2) of Regulation (EU) 2018/1725** of the European Parliament and of the Council and delivered an opinion on **6 November 2019.**

(25) The Commission should carry out an evaluation of this Directive that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU value added and should provide the basis for impact assessments of possible further measures. The evaluation should be completed 5[201] years after entry into application, to allow for the gathering of sufficient data on its practical implementation. Information should be collected regularly and in order to inform the evaluation of this Directive.

---

199 Modifications proposed by EP, which refers to Articles 6(1) and 6(2).
200 EP suggestion.
201 EP suggests to put an ”X” here instead of “5”.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive lays down rules on the **designation of establishments and the appointment of legal representatives** of certain service providers **offering services in the Union** ~~legal representation in the Union~~ for receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings.

1a. This Directive applies to decisions and orders for the purpose of gathering electronic evidence on the basis of Regulation XXXX/XXX [e-Evidence Regulation], Directive 2014/41/EU, the Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of the Union [***and to domestic orders addressed by Member States to legal representatives or designated establishments of service providers on their territory***]**.**[202]

1b. This Directive is without prejudice to the powers of national authorities in accordance with Union and national law to address directly service providers ***[via a designated establishment or legal representative]***[203] **on their territory, for the purposes of gathering electronic evidence in criminal proceedings.**

2. Member States shall not impose additional obligations to those deriving from this Directive on service providers **in particular with regard to the designation of establishments or the appointment of legal representatives** ~~covered by this Directive~~ for the purposes set out in paragraph 1.

~~3. This Directive is without prejudice to the powers of national authorities in accordance with Union and national law to address **directly** service providers established on their territory for the purposes referred to in in paragraph 1.~~

---

202 The text in brackets is an EP wish. The Presidency suggests to keep this sentence.

203 **FR, DE, BE** and **IE** have noted that they strongly oppose the inclusion of these words in the text. **ES** and **PL** also question the current text. The Presidency intends to propose to the EP the deletion of „*designated establishment or legal representative"* in Article 1 (3) and in the connected recital.

4. This Directive shall apply to the service providers defined in Article 2(2) offering their services in the Union. It shall not apply where those service providers are established on the territory of a single Member State and offer services exclusively on the territory of that Member State.

Article 2

Definitions

For the purpose of this Directive, the following definitions apply:

(1) 'legal representative' means a **natural or** legal ~~or natural~~ person, designated in writing by a service provider **not established in a Member State taking part in a legal instrument referred to in Article 1(2) of this Directive** for the purpose of Articles 1(1) **and** 3(1)~~, 3(2) and 3(3)~~;

(2) 'service provider' means any natural or legal person that provides one or more of the following categories of services, with the exception of financial services referred to in Article 2(2)(b) of Directive 2006/123/EC:

(a) electronic communications service as defined in Article 2(4) of ~~[~~Directive (EU) 2018/1972 establishing the European Electronic Communications Code[204]~~]~~;

(b) internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and **domain name** related privacy and proxy services;

(c) other information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[205] that provide:

the ability to its users to communicate with each other; or

the ability to process or store data on behalf of the users to whom the service isprovided **for, where the storage of data is a defining component of the service provided to the user[206];**

---

204 **Directive (EU) 2018/1972 of the European Parliament and Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36**.)

205 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

206 ES prefers the wording of the general approach as much clearer.

(3) 'offering services in a Member State' means:

(a) enabling **natural or** legal ~~or natural~~ persons in a Member State to use the services referred to in point (2); and

(b) having a substantial connection based on specific factual criteria to the Member State referred to in point (a); **such a substantial connection to the Union shall be considered to exist where the service provider has an establishment in the Union, or, in the absence of such an establishment, based on the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States;**

(4) 'establishment' ~~or 'being established'~~ means the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or the business is managed;

(4a) 'designated establishment' means an establishment designated in writing by a service provider established in a Member State taking part in a legal instrument referred to in Article 1(2) of this Directive, for the purpose of Articles 1(1) and 3(1);

(5) 'group' means a group as defined in Article 3(15) of Directive (EU) 2015/849 of the European Parliament and of the Council[207].

Article 3

Legal representative

1. Member States ~~where a~~ **shall ensure that** service providers offering services in the Union ~~is established shall ensure that it~~ designates at least one **addressee** ~~legal representative in the Union~~ for the receipt of, compliance with and enforcement of decisions and orders **falling within the scope of Article 1(2) of this Directive** issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings:

(a) For service providers established in the Union, the Member States where the service providers are established shall ensure that such service providers designate the establishment(s) responsible for the activities described in this paragraph;

---

207 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

(b) **For service providers that are not established in the Union,** Member States shall ensure that such service providers offering services on their territory designate **at least one legal representative, responsible for the activities described in this paragraph, in Member States taking part to the instruments referred to in Article 1(2) of this Directive;**

(c) **For service providers established in Member States not taking part in a legal instrument referred to in Article 1(2), the Member States taking part in those instruments shall ensure that such service providers offering services on their territory designate the legal representatives, responsible for the activities described in this paragraph, in Member States taking part in such instruments.**

~~Where a service provider is not established in the Union, Member States shall ensure that such service provider offering services on their territory designates at least one legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.~~

~~3. As regards the receipt of, compliance with and enforcement of decisions and orders issued by the competent authorities of Member States under Union legal instruments adopted falling within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal proceedings, the Member States taking part in those legal instruments shall ensure that service providers offering services on their territory designate at least one representative in one of them. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.~~

~~4. Service providers shall be free to may designate additional legal representatives, resident or established in other Member States, including those where the service providers are estalished or offer their services. Service providers which are part of a group shall be allowed to collectively designate one legal representative.~~[208]

[208] **ES** and **NL** wish to reintroduce this provision. The Presidency intends to clarify in the recitals, that it should be possible for the service providers to designate a legal representative collectively (the current text does not prohibit this, but it would be better to explain the situation in a recital).

5. Member States shall ensure that the **addresses defined in paragraph1:** ~~decisions and orders by the their competent authorities for evidence gathering in criminal proceedings are addressed to the legal representative designated by the service provider to that effect. That legal representative shall be entrusted with the receipt, of and compliance with and enforcement of those decisions and orders on behalf of the service provider concerned, and can be subject to enforcement measures.~~

(a) reside in a Member State where the service providers offer the services; and

(b) can be subject to enforcement procedures.

[6]. Member States shall ensure that the decisions and orders issued by the competent authorities for evidence gathering in criminal proceedings are addressed to the designated establishment or legal representative designated by the service provider in accordance with paragraph (1) to that effect.

[…]

[7]. Member States shall ensure that service providers established or offering services ~~i~~**o**n their territory provide their legal representative with the necessary powers and resources to comply with decisions and orders received from any Member State. **Member States shall also verify that the designated establishments or legal representatives residing on their territory have received from the service providers the necessary powers and resources to comply with decisions and orders received from any Member State and that they cooperate with the competent authorities when receiving those decisions and orders, in accordance with the applicable legal framework.**

~~7. The Member States where the legal representatives are residing or are established shall verify that the said legal representatives have received from the service providers the necessary powers and resources to comply with decisions and orders received from any Member State and that they cooperates with the competent authorities when receiving those decisions and orders, in accordance with the applicable legal framework.~~

[8]. Member States shall ensure that both the designated **establishment or the** legal representative and the service provider can be held jointly and severally liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders **falling within the scope of Article 1(2) of this Directive**, with the effect that each of the **designated establishment or the** legal representative and service provider may be sanctioned for non-compliance ~~of either of them~~. In particular, the lack of appropriate internal procedures between the service provider and **the designated establishment or** the legal representatives cannot be used by either side as a justification for non-compliance with those obligations. Joint and several liability shall not apply for actions or omissions of either the service provider or the legal representative **or the designated establishment** which constitute a criminal offence in the Member State applying the sanction.

9. Member States shall ensure that the obligation to designate a legal representative is fulfilled by [6 months from the date of transposition set out in Article 7] for service providers that offer services in the Union at that date, or from the moment service providers start offering services in the Union for those service providers that will start offering services after that date.

Article 4

Notifications and languages

1. Member States shall ensure that~~, upon designation of its legal representative in accordance with Article 3(1), (2), (3) and (4),~~ each service provider established or offering services in their territory notifies in writing the central authority of the Member State where its **designated establishment is established or where its** legal representative resides, **their contact details and** ~~or is established of the designation and contact details of its legal representative as well as~~ any changes thereof.

2. The notification shall specify the official language(s) of the Union, as referred to in Regulation 1/58, in which the legal representative can be addressed. This shall include, ~~at least,~~ one or more of the official languages in accordance with the national law of the Member State where the legal representative resides or **designed establishment** is established.

3. When a service provider designates several **designated establishements or legal** representatives **in accordance with Article 3(1). Member States shall ensure that such service provider indicates the precise territorial scope of the designation for the designated establishment or legal representatives.** The notification shall specify the official language(s) of the Union or Member States covered by each of them. ~~and any other considerations to determine the appropriate legal representative to be addressed. Competent authorities may depart from those considerations on a case-by-case basis; where necessary Member States shall ensure that in such cases, the addressed legal representative has to comply with these orders and decisions.~~

4. Member States shall ensure that the information notified to them in accordance with this Article is publicly available on a dedicated internet page of the European Judicial Network in criminal matters. Member States shall ensure that this information is regularly updated. This information may be further disseminated to facilitate access by competent authorities.

Article 5

Sanctions

1. Member States shall lay down rules on sanctions applicable to infringements of national provisions adopted pursuant to **Article 3 and 4** and shall take all measures necessary to ensure that they are implemented. The sanctions provided for shall be effective, proportionate and dissuasive.

2. Member States shall, by the date set out in Article 7, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. Member States shall also inform the Commission on an annual basis about non-compliant service providers**,** ~~and~~ relevant enforcement action taken against them **and the sanctions imposed**.

Article 6

Central authorities

1. In accordance with their legal systems, Member States shall designate one or more ~~a~~ central authorities, to ensure the application of this Directive in a consistent and proportionate manner.

2. Member States shall inform the Commission of their designated central authority, or central authorities, referred to in paragraph 1. The Commission shall forward a list of designated central authorities to the Member States **and make it publically available**. ~~The Commission will also make publicly available a list of designated central authorities to facilitate the notifications by a service provider to the Member States where its legal representative resides or is established.~~

3. Member States shall ensure that their central authorities coordinate and cooperate with each other and, where relevant, with the Commission, and provide any appropriate information and assistance to each other in order to apply this Directive in a consistent and proportionate manner. The coordination, cooperation and provisioning of information and assistance shall cover, in particular, enforcement actions.

Article 7

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by **18**[209] months after entry into force. They shall immediately inform the Commission thereof.

2. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

3. Member States shall communicate to the Commission the text of the measures of national law which they adopt in the field covered by this Directive.

Article 8

Evaluation

By [*X years from the date of application of this Directive*] at the latest, the Commission shall carry out an evaluation of the Directive. **The Commission shall transmit this** ~~and present a~~ report to the European Parliament and to the Council ~~on the application of this Directive, which shall include an assessment of the need to enlarge its scope. Where appropriate, the report shall be accompanied by a proposal for the amendment of this Directive.~~ The evaluation shall be conducted according to the Commission's Better Regulation Guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

209 The EP has not agreed to this timeline.

Article 9

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 10

Addressees

This Directive is addressed to the Member States **in accordance with the Treaties**.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*