Council of the
European Union

Brussels, 25 January 2023

Mr. Juan Fernando Lopez Aguilar
Chair of the Committee on Civil Liberties, Justice and Home Affairs
European Parliament
Bât. Altiero Spinelli – 14G305
60, rue Wiertz, Wiertzstraat 60
B-1047 Brussels

Subject: - Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - 2018/0108 (COD).
- Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings - 2018/0107 (COD).

Dear Mr. Lopez Aguilar,

Following the informal meeting between the representatives of the three institutions, the draft compromise text was agreed today by the Permanent Representatives' Committee.

I am therefore now in a position to confirm that, should the European Parliament adopt its position at first reading, in accordance with Article 294 paragraph 3 of the Treaty, in the form set out in the compromise package contained in the Annex to this letter (subject to finalisation by the legal linguists of the two institutions), the Council would approve the position of the European Parliament and the act shall be adopted in the wording which corresponds to the position of the European Parliament in accordance with Article 294(4) of the TFEU.

On behalf of the Council I also wish to thank you for your close cooperation which should enable us to reach agreement on this dossier at first reading.

Yours faithfully,

L. DANIELSSON
Chairman of the Permanent
Representatives Committee

Copy to: Ms Birgit Sippel, Rapporteur, Member of the European Parliament
Ms. Ilva Johansson, Member of the European Commission
Mr. Didier Reynders, Member of the European Commission

Council of the
European Union

ANNEX 1

Amended proposal for a

REGULATION (EU) 2023/...
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of ...

on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following 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 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[1],

Acting in accordance with the ordinary legislative procedure[2],

[1] OJ C 367, 10.10.2018, p. 88.
[2] Position of the European Parliament of … (not yet published in the Official Journal) and decision of the Council of ….

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) 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 to combat crime, subject to conditions and safeguards to ensure full compliance 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'), in particular the principles of necessity and proportionality, due process, protection of privacy and personal data and confidentiality of communications.

(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[3], 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, in its Resolution on the fight against cybercrime of 3 October 2017[4], underlined the need to find means to secure and obtain electronic evidence more rapidly, as well as the importance of close cooperation between law enforcement authorities, third countries and service providers active on European territory, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[5] and Directive (EU) 2016/680 of the European Parliament and of the Council[6], and existing mutual legal assistance (MLA) agreements, 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, while welcoming the ongoing work of the Commission towards a cooperation platform with a secure communication channel for digital exchanges of European Investigation Orders (EIOs) for electronic evidence and replies between EU judicial authorities.

---

3 JOIN(2017) 450 final.

4 2017/2068(INI).

5 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).

6 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).

(7) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the country where the relevant service is offered. Therefore, 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.

(8) Because of the way network-based services are provided, judicial cooperation requests are often addressed to states which are hosts to a large number of service providers. Furthermore, the number of requests has multiplied in view of increasingly used networked services. Directive 2014/41/EU of the European Parliament and of the Council[7] provides for the possibility of issuing a European Investigation Order (EIO) for the purpose of gathering evidence in another Member State. In addition, 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 also provides for the possibility of requesting evidence from another Member State. However, the procedures and timelines foreseen in the EIO and the Convention 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 subsequent leads might no longer be available. Furthermore, there is no harmonised framework for cooperation with service providers, while certain third-country providers accept direct requests for data other than content data as permitted by their applicable domestic law. As a consequence, all Member States increasingly rely on voluntary direct cooperation channels with service providers where available, applying different national tools, conditions and procedures. For content data, some Member States have taken unilateral action, while others continue to rely on judicial cooperation.

[7] 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).

(9) The fragmented legal framework creates challenges for law enforcement and judicial authorities as well as for service providers seeking to comply with 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 cooperation for preserving and producing electronic evidence, addressing the specific nature of electronic evidence, including an obligation on service providers covered by the scope of the instrument to respond directly to requests stemming from authorities in another Member State. With this, this Regulation complements the existing Union law and clarifies the rules applicable to law enforcement and judicial authorities as well as to service providers in the field of electronic evidence, while ensuring full compliance with fundamental rights.

(10)

(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 of a European Production Order by an enforcing authority 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.

(11) The mechanism of the European Production Order and the European Preservation Order for electronic evidence in criminal proceedings relies on the principle of mutual trust between the Member States and a presumption of compliance by Member States with 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 such orders to service providers.

(11a) 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.

(11b) When implementing this Regulation, Member States should ensure that personal data are protected and processed in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680, as well as Directive 2002/58/EC of the European Parliament and of the Council[8] including in case of further use, transmissions and onward transfers of data obtained.

[8] 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).

(11c) 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 which may be obtained through authentication processes.

(12)

(13)

(14) The procedural rights in criminal proceedings set out in Directives 2010/64/EU[9], 2012/13/EU[10], 2013/48/EU[11], (EU) 2016/343[12], (EU) 2016/800[13] and (EU) 2016/1919[14] 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 also apply.

(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.

---

9 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).

10 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).

11 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).

12 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).

13 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).

14 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 lays down the rules under which, in a criminal proceeding or for the execution of a custodial sentence following criminal proceedings in accordance with this Regulation, 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 is applicable in all cross-border cases where the service provider has its designated establishment or legal representative in another Member State. This Regulation is without prejudice to the powers of national authorities to address service providers established or represented on their territory in order for them to comply with similar national measures.

(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 Regulation. Providers of electronic communication services are defined in Directive (EU) 2018/1972 of the European Parliament and of the Council[15]. 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 providers within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council[16] that do not qualify as electronic communications service 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.

---

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

16 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 (codification) (OJ L 241, 17.9.2015, p. 1).

The categories of service providers included here are, for example, online marketplaces providing consumers and businesses with 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 with 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 or 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 in this Regulation, even if within the definition of information society services pursuant to Directive (EU) 2015/1535.

(17) In many cases, data is no longer stored or processed on a user's device but made available on cloud-based infrastructure enabling 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 service provider's establishment or of the data processing or storage facility.

(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 allow for the identification of an individual or entity behind a web site used in criminal activity, or the victim of criminal activity.

(19) This Regulation should regulate the gathering of data stored by a service provider at the time of receipt of a European Production or Preservation Order only. It should 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. This Regulation also should not authorise interception of data or obtaining data stored at a future point from the receipt of a European production or preservation order.

(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 should not stipulate any obligation for service providers to decrypt data.

(20) This Regulation should cover the data categories subscriber data, traffic data and content data. Such categorisation is in line with the laws of many Member States Union law such as Directive 2002/58/EC and the case law of the Court of Justice, as well as international law, notably the Convention on Cybercrime of the Council of Europe (CETS No.185) ('Budapest Convention').

(21)

(22)

(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 requested from the service provider. In such cases, it is appropriate to apply the same 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, they are generally sought to obtain more privacy-intrusive information, such as the contacts and whereabouts of the user and could serve to establish a comprehensive profile of an individual concerned, while they 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 treated as traffic data and requested under the similar regime as content data, as defined under this Regulation.

(23) All data categories contain personal data and are thus covered by the safeguards under the Union data protection acquis. However, the intensity of the impact on fundamental rights varies between the categories, in particular between subscriber data, and data requested for the sole purpose of identifying the user, as defined in this Regulation, on the one hand and traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data on the other. While subscriber data as well as IP addresses, access numbers and related information, where requested for the sole purpose of identifying the user, could be useful to obtain first leads in an investigation about the identity of a suspect, traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data are often more relevant as probative material. 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 data.

(24) In the framework of criminal proceedings, the European Production Order and the European Preservation Order should only be issued for specific criminal proceedings concerning 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.

(24a) As proceedings for mutual legal assistance might 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 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.

(24b) This Regulation should apply to 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.

(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 it should only be possible to issue the Orders provided for by this Regulation for data pertaining to services offered in the Union. Services offered exclusively outside the Union are not included in the scope of this Regulation, even if the service provider is established in the Union. Therefore, this Regulation should not allow any access to any data beyond data related to the services offered to the user in the Union by those service providers.

(27) Determining whether a service provider offers services in the Union requires an assessment whether the service provider enables natural or legal persons in one or more Member States, to use its services. However, the mere accessibility of an online interface in the Union, such as for instance the accessibility of the website or an e-mail address or other contact details of a service provider or an intermediary, taken in isolation, should be considered insufficient to determine that a service provider offers services in the Union within the meaning of this Regulation.

(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 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. 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 generally 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 Regulation (EU) No 1215/2012 of the European Parliament and of the Council[17]. 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 of the European Parliament and of the Council[18] cannot, 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.

---

17 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).

18 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 60I, 2.3.2018, p. 1).

(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 enforcing authority. Where the disruption or destruction of a critical infrastructure as defined in Council Directive 2008/114/EC[19] 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.

(29) A European Production Order should only be issued if it is necessary, proportionate, adequate and applicable to the case at hand. The issuing authority should take into account the rights of the suspected or accused person in a proceeding relating to a criminal offence and should only issue the Order if it could have been ordered under the same conditions in a similar domestic case. 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.

(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 data requested 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 of data requires review by a judge. As subscriber data and data requested for the sole purpose of identifying the user as defined in this Regulation are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent public prosecutors. In accordance with the right to a fair trial, as protected by the Charter and the European Convention on Human rights, public prosecutors should exercise their responsibilities objectively, taking their decision solely on the basis of the factual elements in the case file and taking into account all incriminatory and exculpatory evidence.

---

[19] 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 345, 23.12.2008, p. 75).

(31) In view of the more sensitive character of traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data, a distinction has to be made regarding the material scope of this Regulation: it should be possible to issue Orders to produce subscriber data and data requested for the sole purpose of identifying the user, as defined in this Regulation, for any criminal offence, whereas access to traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data should be subject to stricter requirements to reflect the more sensitive nature of such data. There should be a threshold allowing for a more proportionate approach, together with a number of other ex ante and ex post conditions and safeguards provided for in this Regulation 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 custodial sentence would limit the scope of the instrument to more serious crimes, without excessively affecting the possibilities of its use by practitioners. It should exclude from its scope a significant number of crimes which are considered less serious by Member States, as expressed in a lower maximum penalty. It would also have the advantage of being easily applicable in practice.

(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 this 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 (EU) 2017/541 of the European Parliament and of the Council[20] 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[21] do not require the minimum maximum threshold of 3 years.

(33)

(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.

[20] 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).

[21] 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).

(34) As a matter of principle, European Production Orders should be addressed to the service provider, acting as controller. However, in some circumstances, the delimitation between the roles of controller and processor can prove particularly challenging, in particular where several service providers are involved in the processing of data or where service providers process the data on behalf of a natural person. The delimitation between the roles of controller and processor with regard to a particular set of data requires not only specialised knowledge of the legal context, but it could also require interpretation of often very complex contractual frameworks providing in a specific case for allocation of different tasks and roles with regard to a particular set of data to various service providers. Where service providers process data on behalf of a natural person, it may be difficult in some cases to determine who the controller is, even where there is only one service provider involved.

It follows that where the data is stored or processed by a service provider and there is no clarity as to who the controller is, despite reasonable efforts on the part of the issuing authority, it should be possible to address a European Production Order directly to that service provider.

Moreover, in some cases, addressing the controller could be detrimental to the investigation, for example because the controller is a suspect or accused or convicted person in the case concerned or there are indications that the controller could be acting in the interest of the person subject to the investigation. Also in those cases, it should be possible to address the European Production Order directly to the service provider processing the data on behalf of the controller. This does not affect the right of the issuing authority to order the service provider to preserve the data.

(34a) In accordance with Regulation (EU) 2016/679, the processor, storing or processing the data on behalf of the controller, should inform the controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the 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 the reasons for the delay and a short justification should also be added in the Certificate.

(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 or European Preservation 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 this Regulation 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.

(35) 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. In case the issuing authority has indications that parallel criminal proceedings may be ongoing in another Member State, it should consult the authorities of that Member State in accordance with Council Framework Decision 2009/948/JHA[22]. In any case, a European Production Order or European Preservation Order should not be issued, where the issuing authority has indications that this would be contrary to the ne bis in idem principle.

---

22 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).

(35a) 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 ifit could have been ordered under the same conditions in a similar domestic case.

There is no common definition of what constitutes an immunity or privilege in Union law, the precise definition of these t erms 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 on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media.

(35b) Where the issuing authority seeks to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or content data by issuing the European Production Order and has reasonable grounds to believe 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, the issuing authority could seek clarification, including through consultation with the competent authorities of the enforcing State concerned, either directly or via Eurojust or the European Judicial Network.

(35c) In view of the more sensitive character of European Production Orders for traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data, it is appropriate to provide for a notification mechanism involving a competent authority of the enforcing State, by transmitting the EPOC to that authority at the same time as the EPOC is transmitted to the addressee. Only European Production Orders for those data categories should be subject to a notification requirement. However, where a European Production Order is issued to obtain electronic evidence in a criminal proceeding with substantial and strong links to the issuing State, no notification should be required. Such links should be assumed where, at the time of issuing the European Production Order, the issuing authority has reasonable grounds to believe that the offence has been committed, is being committed or is likely to be committed in the issuing State, and where the person whose data are sought resides in the issuing State.

(35d) Within the meaning of this Regulation, an offense should be considered as having been committed, being committed or being likely to be committed in the issuing State, in accordance with national laws of the issuing State. In some cases, especially in the cybercrime field, some factual elements, such as the residence of the victim, are usually important indications to consider when determining where the offense has been committed. For instance, ransomware crimes can often be considered as having been committed where the victim of this crime resides, even when the exact localization from where the ransomware has been launched is uncertain. Any determination as to the place of the commitment of the crime should be without prejudice to the rules on jurisdiction over the relevant offenses pursuant to the applicable national law.

(35e) It is for the issuing authority to assess, at the time of issuing the order and on the basis of material before it, whether there are reasonable grounds to believe that the person whose data are sought resides in the issuing State.
In that regard, various objective circumstances that could indicate that the person concerned has established the habitual centre of his or her interests in a particular Member State or has the intention to do so, can be of relevance.

It follows from the need for uniform application of Union law and from the principle of equality that the notion of "residence" in this particular context should be given uniform interpretation throughout the Union. Reasonable grounds to believe that a person resides in an issuing State could exist, in particular, where a person is registered as a resident in an issuing State, by holding an identity card, a residence permit or a registration in an official residence register.

In the absence of registration in the issuing State, residence could be indicated by the fact that a person manifested the intention to settle in that Member State or has acquired, following a stable period of presence in that Member State, certain connections with that State which are of a similar degree as those resulting from establishing a formal residence in that Member State. In order to determine whether, in a specific situation, there are sufficient connections between the person concerned and the issuing State giving rise to reasonable grounds to believe that the person concerned resides in that State, various objective factors characterising the situation of that person could be taken into account, which include, in particular, the length, nature and conditions of her or his presence in the issuing State or the family ties or economic connections which that person has with that Member State. A registered vehicle, a bank account, the fact that the person's stay in the issuing State was uninterrupted or other objective factors may be of relevance to determine that there are reasonable grounds to believe that the person concerned resides in the issuing State. A short visit, a holiday stay, including in a holiday home, 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, at the time of issuing the European Production Order, there are no reasonable grounds to believe that the person whose data are sought resides in the issuing State, the issuing authority should notify the enforcing State.

(35f) 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. Any subsequent change of residence should not have any impact on the procedure. The person concerned should be able to invoke his or her 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 should be able to raise 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. In addition, it should be also possible to invoke these grounds during the enforcement procedure.

(36) It should be possible to issue the European Preservation Order for any criminal offence. 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 where it is necessary, 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 to prevent the removal, deletion or alteration of relevant and necessary data as evidence in an individual case in situations where it may take more time to obtain the production of this data.

(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 validly established emergency cases when seeking the production of subscriber data and data requested for the sole purpose of identifying the user, as defined in this Regulation, 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 under national law without prior validation.

(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 (EU) 2023/XXX of the European Parliament and of the Council* [legal representatives Directive]. Exceptionally, in emergency cases as defined in this Regulation, where the designated establishment or the legal representative of a service provider does not react to the EPOC or the EPOC-PR within the deadlines or has not yet been designated within the deadlines set out in Directive (EU) 2023/XXX [legal representatives Directive], it should be possible to address the EPOC or EPOC-PR to any other establishment or legal representative of the service provider in the Union alongside or instead of pursuing enforcement of the original Order according to this Regulation. Because of these various possible scenarios, the general term 'addressee' is used in the provisions.

(38) The European Production and European Preservation Orders should be transmitted through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). Where necessary, 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, or into another official language that the designated establishment or the legal representative of the service provider declared it will accept. Where a notification is required, the EPOC to the notified authority should be translated into an official language of the enforcing State. In this regard, Member States should be encouraged, 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. The Commission should make the declarations available to all Member States and to the European Judicial Network.

(39)

---

* OJ: Please insert in the text the number of the Directive contained in document PE-CONS XX/XX (2018/0107(COD)) and insert the number, date, title and OJ reference of that Directive in the footnote.

(40) Where notification is not needed in application of this Regulation, upon receipt of the EPOC, the addressee should ensure that the requested data are transmitted 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.
Where notification is needed in application of this Regulation, 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 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. Where the enforcing authority, already before the end of the 10 days, confirms to the issuing authority and the addressee that it will not raise any ground for refusal, the addressee should act as soon as possible upon such confirmation and at the latest at the end of the 10 days. Shorter time limits should be respected by the addressee, and, where applicable, the enforcing authority, in emergency cases as defined in this Regulation. The addressee, and, where applicable, the enforcing authority, should execute the order as soon as possible and at the latest within the deadlines prescribed in this Regulation, taking as full account as possible of the procedural deadlines and other deadlines indicated by the issuing State.

(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 under the law of 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 received from the addressee 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. It should also be possible for the enforcing authority to raise the grounds for refusal set out in this Regulation.

(41) 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 authority, as well as, where a notification took place, the enforcing authority, in cases where the EPOC or 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 Production Order or European Preservation Order has not been issued in accordance with the conditions set out by this Regulation, it should go back to the issuing authority 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 European Production Order by the issuing authority at an early stage. To guarantee the availability of the data, the addressee should preserve the data if they can identify the data sought.

(41a) The addressee should not be obliged to comply with the European Production Order or 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 Production Order or 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 lawfully deleted before receiving the order.

(42) Upon receipt of a EPOC-PR, the addressee should preserve the requested data for a maximum of 60 days unless the issuing authority confirms that a subsequent request 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 this Regulation. Where the issuing authority confirms within the relevant deadline that a subsequent request for production has been issued at its level, the addressee should preserve the data as long as necessary to produce the data once the addressee has received the subsequent request for production. Such a confirmation must be sent to the addressee within the relevant deadline, in one of the official languages of the Member State where the designated establishment or the legal representative of the service provider is located or any other language accepted by the addressee, using the form set out in this Regulation. To prevent the preservation from ceasing it is sufficient that the underlying request for production has been issued and the confirmation has been sent by the 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.

(42a) Notwithstanding the principle of mutual trust, it should be possible for the enforcing authority to 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. Where a notification or enforcement takes place in accordance with this Regulation and where provided by national law of the enforcing State, the execution of the order might require the procedural involvement of a court in the enforcing State.

(42b) Where the enforcing authority is notified of an order for traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, or for content data, it should have the right to assess the information set out in the Order and, where appropriate, refuse a European Production Order, where, based on a mandatory and due analysis of the information contained in the Order and in observance of the applicable rules of primary Union law, in particular the Charter, it reaches the conclusion, that one or more of the grounds for refusal provided for in this Regulation are met. The need to respect the independence of judicial authorities requires that a degree of discretion is granted to these authorities when taking decisions as to the grounds for refusal.

(42c) It should be possible for the enforcing authority, 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 under the law of the enforcing State, or where the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order.

(42d) It should be possible for the enforcing authority to refuse an Order where, in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the European Production 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. In particular, when assessing this ground for refusal, where the enforcing authority has at its disposal 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 was executed, of a serious breach of the fundamental right to an effective remedy and to a fair trial guaranteed by Article 47(2) of the Charter, on account of systemic or generalised deficiencies as concerns the independence of the issuing Member State's judiciary, the enforcing 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 authority, there are substantial grounds for believing that that person will run such a risk of breach of his or her right to a fair trial.

(42e) It should be possible for the enforcing authority to refuse an Order where the execution of the Order would be contrary to the principle of ne bis in idem.

(42f) It should be possible for the enforcing authority, where it is notified according to this Regulation, to refuse an European Production Order in case the conduct for which the EPOC has been issued does not constitute an offence under the law of the enforcing State unless it concerns an offence listed within the categories of offences set out in the Annex of this Regulation, 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.

(43) 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. 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 (EU) 2016/680 are met in which case, the issuing authority should indicate in the case file the reasons for the delay, restriction or omission and add a short justification in the Certificate. 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.

(43a) It should be possible for the service provider to claim reimbursement of its costs to respond to Orders from 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. Member States should inform the Commission about their national rules for reimbursement, and the Commission should make them public. This should not include costs related to the decentralised IT system, which are addressed in the provisions on the decentralised IT system.

(43b) Without prejudice to national laws providing for the imposition of criminal sanctions, Member States should lay down the 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 pecuniary sanctions provided for by national laws of the Member States are effective, proportionate and dissuasive.

(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 to the enforcing authority. 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.

(45) The enforcement procedure is a procedure where the addressee can invoke 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 recognize and enforce the Order based on the same grounds, and also, in specific cases, for the manifest breach of relevant fundamental rights set out in Article 6 TEU and Charter. The enforcing authority should consult the issuing authority before refusing to recognize 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.

(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 pecuniary 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 resources outside normal business hours, if the data is transmitted without undue delay.

(46) Without prejudice to data protection obligations, service providers should not be held liable in Member States for prejudices to their users or third parties exclusively 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.

(47) Compliance with an Order could conflict with applicable laws of a third country. 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 a law of a third country.

(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.

(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 (EU) 2016/680. The issuing State should in particular request the competent authority of the third country for information where the conflict concerns fundamental rights or other fundamental interests of the third country related to national security and defence.

(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 and on conflict 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 from experience and expertise gathered on the same or similar questions. It should not prevent a renewed consultation of the third state where appropriate.

(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, 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 enforcing authority about the outcome of the proceedings.

(52)

(53) The conditions set out in this Regulation for the execution of an EPOC are applicable also where conflicting obligations deriving from the law of a third country occur. During this judicial review where compliance with a European Production Order would prevent service providers from complying with legal obligation deriving from a law of a third country, 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. In line with this and without prejudice to further legal remedies available in accordance with national law, any persons whose data were sought via a European Production Order should have the right to effective remedies against the European Production 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 about the possibilities under national law for seeking remedies should be provided in due time and it should ensure that they can be exercised effectively.

(55)

(56)

(56a) Appropriate channels should be developed to ensure that all parties can efficiently cooperate in a digital way, through a decentralised information technology (IT) system that allows for the swift, direct, interoperable, sustainable, reliable and secure cross-border electronic exchange of case-related forms, data and information.

(56b) The decentralised IT system should be comprised of IT systems of Member States and the Union agencies and bodies, and interoperable access points, through which they are interconnected. The access points of the decentralised IT system should be based on e-CODEX.

(56c) In order to allow for the efficient and secure written communication between competent authorities and designated establishments or legal representatives of service providers under this Regulation, the latter should be provided with electronic means of access to the national IT systems, part of the decentralised IT system, operated by the Member States.

(56d) Member States could use a software developed by the Commission (reference implementation software) instead of a national IT system. This reference implementation software should be based on a modular setup, meaning that the software is packaged and delivered separately from the e-CODEX components needed to connect it to the decentralised IT system. This setup should enable Member States to reuse or enhance their existing national judicial communication infrastructures for the purpose of cross-border use.

(56e) The Commission should be responsible for the creation, maintenance and development of this reference implementation software. The Commission should design, develop and maintain the reference implementation software in compliance with the data protection requirements and principles laid down in Regulation (EU) 2018/1725 of the European Parliament and of the Council[23], Regulation (EU) 2016/679, and Directive (EU) 2016/680 of the European Parliament and of the Council, in particular the principles of data protection by design and by default as well as high level of cybersecurity. The reference implementation software should also include appropriate technical measures and enable the organisational measures necessary for ensuring an appropriate level of security and interoperability.

---

[23] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(56f) As a rule, all written communication among competent authorities or between competent authorities and designated establishments or legal representatives of service providers should be carried out through the decentralised IT system. Alternative means may be used only where the use of the decentralised IT system is not possible, for example because of specific forensic requirements, because the volume of data to be transferred is hampered by technical capability constraints, or because another establishment not connected to the decentralised IT system has to be addressed in an emergency case. In such cases, the transmission should be carried out by the most appropriate alternative means, taking into account the need to ensure a swift, secure and reliable exchange of information.

(56g) The use of mechanisms to ensure authenticity, as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council[24], should be considered.

(56h) To ensure that the decentralised IT system contains a complete record of written exchanges under this Regulation, any transmission effected by alternative means should be recorded in the decentralised IT system without undue delay.

(56i) Service providers, in particular small and medium size enterprises, should not be exposed to disproportionate costs in relation to the establishment and operation of the decentralised IT system. As part of the creation, maintenance and development of the reference implementation, the Commission therefore should also make available a web-based interface allowing service providers to communicate securely with authorities without having to establish their own dedicated infrastructure in order to access the decentralised IT system.

---

24 Regulation (EU) No 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 (OJ L 257, 28.8.2014, p. 73).

(56j) By the same token, service providers who make use of bespoke IT solutions for the purposes of exchanging information and data related to requests for electronic evidence should enjoy automated means of accessing the decentralised IT systems by means of a common data exchange standard.

(56k) For data exchanges carried out via the decentralised IT system or recorded in the decentralised IT system, Member States may collect statistics to fulfil their monitoring and reporting obligations under this Regulation via their national portals.

(56l) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[25].

(57)

(57a) In order to monitor the outputs, results and impacts of this Regulation, the Commission should publish an annual report on the preceding calendar year, based on data obtained from the Member States. For this purpose, Member States should collect and provide to the Commission comprehensive statistics on different aspects of this Regulation, by type of data requested, the addressees and whether it was an emergency case or not.

(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 added value and should provide the basis for impact assessments of possible further measures. It should 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. Information should be collected regularly in order to inform the evaluation of this Regulation.

---

25 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information under this Regulation, allowing for a quicker and more effective communication 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 of the amendment of forms provided for in 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[26]. 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.

[26] OJ L 123, 12.5.2016, p. 1.

(61) The measures based on this Regulation should 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. Member States' authorities should choose the tool most adapted to the case at hand; they may prefer to use EU and other international instruments, agreements and arrangements when requesting a set of different types of investigative measures including but not limited to the production of electronic evidence from another Member State. Member States should notify the Commission by ... [date of the application of this Regulation] of the existing agreements and arrangements referred to in this Regulation which they will continue to apply. Member States should also notify the Commission within three months of the signing of any new agreement or arrangement referred to in this Regulation.

(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 an evaluation of 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 objective.

(64) In accordance with Article 3 of 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.

(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 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on 6 November 2019[27],

HAVE ADOPTED THIS REGULATION:

[27] EDPS Opinion 7/2019 on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6 November 2019).

Chapter I

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 service providers established or represented on their territory in order for them 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.

Article 2

Definitions

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

(1) 'European Production Order' means a decision, issued or validated by a judicial authority of a Member State in application of Article 4(1), (2), (4) and 5, addressed to a designated establishment or a legal representative of a service provider offering services in the Union located in another Member State bound by this Regulation to produce electronic evidence.

(2) 'European Preservation Order' means a decision, issued or validated by a judicial authority of a Member State in application of Article 4(3) to 4(5), addressed to a designated establishment or a legal representative of a service provider offering services in the Union located in another Member State bound by this Regulation to preserve electronic evidence in view of a subsequent request for production.

(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 of the European Parliament and of the Council[28]:

(a) electronic communications service as defined in Article 2(4) of Directive (EU) 2018/1972;

(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;

[28] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

(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[29] 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 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 persons in a Member State to use the services listed under point (3); 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' means an entity actually pursuing 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

(5a) 'designated establishment' means an establishment with a legal personality 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 Directive (EU) 2023/XXX [legal representatives Directive], for the purpose of Articles 1(1) and 3(1).

[29] 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).

(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 (EU) 2023/XXX [legal representatives Directive], for the purpose of Articles 1(1) and 3(1).

(6) ‘electronic evidence’ means 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 European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).

(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) ‘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) ‘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 including electronic communications metadata and data relating to the commencement and termination of a user access session to a service such as the date and time of use, the log-in to and log-off from the service other than subscriber data.

(10) ‘content data’ means any data in a digital format, such as text, voice, videos, images and sound, other than subscriber or traffic 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[30].

(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 the European Production Order or the European Preservation Order.

(13) ‘enforcing State’ means the Member State in which the designated establishment is established or the legal representative resides and 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 for notification or enforcement of the order in accordance with this Regulation.

[30] 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).

(14) ‘enforcing authority’ means, in accordance with its 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 enforcement of the order in accordance with this Regulation.

(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, 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.

(15a) ‘controller’ means controller as defined in point 7 of Article 4 of Regulation (EU) 2016/679.

(15b) ‘processor’ means processor as defined in point 8 of Article 4 of Regulation (EU) 2016/679.

(15c) ‘decentralised IT system’ means a network of IT systems and interoperable access points, operating under the individual responsibility and management of each Member State, Union agency or body that enables the secure and reliable cross-border exchange of information.

Article 3

Scope

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

1a. This 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 only be issued in the framework and for the purposes of 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 II

European Production Order, European Preservation Order and Certificates

Article 4

Issuing authority

1. A European Production Order for obtaining subscriber data and for obtaining data requested for the sole purpose of identifying the user, as defined in Article 2(8) 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 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.

2. A European Production Order 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 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.

5. In validly established emergency cases, as defined in Article 2(15), the authorities mentioned under paragraphs 1(b) and 3(b) may exceptionally issue the respective Order for subscriber data and, data requested for the sole purpose of identifying the user as defined in Article 2(8), without prior validation, where the validation cannot be obtained in time and where these authorities could issue the Order in a similar domestic case without prior 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 delete or otherwise restrict the use of any data that was obtained.

6. Each Member State may designate one or more central authorities 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 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. It may only be issued if it could have been ordered under the same conditions in a similar domestic case.

3. European Production Orders to produce subscriber data or 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.

4. European Production Orders to produce traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data shall 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[31];

   – offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[32];

[31] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (OJ L 123, 10.5.2019, p. 18).

[32] 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).

– offences as defined in Articles 3 to 8 of Directive 2013/40/EU;

(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[33];

(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, 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;

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

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

(g) in case of emergency, the duly justified reasons for it;

(h) in cases where the European Production Order is directly addressed to the service provider, processing the data on behalf of the controller, a confirmation that the Order is made in accordance with paragraph 6;

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

---

33 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).

(j) a summary description of the case.

6. European Production Orders shall be addressed to service providers, acting as controllers, in accordance with Regulation (EU) 2016/679.

As an exception, the European Production Order may be directly addressed to the service provider, processing the data on behalf of the controller, where:

– the controller cannot be identified despite reasonable efforts on the part of the issuing authority, or

– addressing the controller might be detrimental to the investigation.

6a. In accordance with Regulation (EU) 2016/679, the processor, storing or processing the data on behalf of the controller, shall inform the controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the 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 the reasons for the delay. A short justification shall also be added in the Certificate.

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 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 may only be issued:

– where the privileged professional resides in the issuing State, or

– where addressing the privileged professional might be detrimental to the investigation, or

– where the privileges were waived in accordance with the applicable law.

7. If the issuing authority has reasons to believe that traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, 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, the issuing authority may seek clarification before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. Where the issuing authority finds that the requested traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data is 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, the issuing authority shall not issue the European Production Order.

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 paragraph 6b shall apply mutatis mutandis.

2. It may be issued provided it is 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. 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 sought;

(d) the requested data category as defined in Article 2 paragraphs 7 to 10;

(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 6(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 the designated establishment or to the legal representative designated by the service provider pursuant to Directive (EU) 2023/XXX [legal representatives Directive].

2. Exceptionally, in emergency cases as defined in Article 2(15), where the designated establishment or the legal representative of a service provider does not react to the EPOC within the deadlines, the EPOC may be addressed to any other establishment or legal representative of the service provider in the Union.

Article 7a

Notification

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 the EPOC to that authority at the same time as the EPOC is transmitted to the addressee in accordance with Articles 7 and 8(2).

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

   (b) the person whose data are sought resides in the issuing State.

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

4. The notification shall have a suspensive effect on the obligations of the addressee as outlined in Article 9 except for emergency cases defined in Article 2(15) of this Regulation.

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 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 competent authority in the enforcing State when necessary.

   Where a notification is required, the EPOC to the notified authority shall contain the information listed in Article 5(5) (a) to (j).

3. 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.

4. 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 the legal representative of the service provider are located. Where a notification is required, the EPOC to the notified authority shall be translated into an official language of the enforcing State or into another official languages of the Union accepted by that State.

Article 9

Execution of an EPOC

1. Upon receipt of the EPOC, the addressee shall act expeditiously to preserve the data.

1a. Where a notification is needed in accordance with Article 7a and the enforcing authority has not raised any ground for refusal in accordance with Article 10a within 10 days, the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the end of the 10 days upon receipt of the EPOC. Where the enforcing authority, already before the end of the 10 days, confirms to the issuing authority and the addressee that it will not raise any ground for refusal, the addressee shall act as soon as possible upon such confirmation and at the latest at the end of the 10 days.

1b. Where notification is not needed in accordance with Article 7a, upon receipt of an EPOC, the addressee shall ensure that the requested data are transmitted 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 hours upon receipt of the EPOC. Where the order is subject to a notification pursuant to Article 7a, the enforcing authority may, without delay and at the latest within 96 hours after the receipt of the notification, notify the issuing authority and the addressee, based on one of the grounds provided for in Article 10a(1), that it objects to the use of the data or that the data may only be used under conditions which it shall specify. In cases where a ground for refusal is raised by the enforcing authority, if the data has already been transmitted by the addressee to the issuing authority, the issuing authority shall delete or otherwise restrict the use of the data or, in case of conditions, comply with those conditions when using the data.

2a. 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 competent authorities of the issuing and the enforcing State.

Where no notification is made pursuant to Article 7a, the issuing authority shall take the information mentioned in the previous sub-paragraph into account, and shall 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 Article 7a, the issuing authority shall take the information mentioned in the first subparagraph 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 Article 10a.

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 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, 1 a, 1 b and 2. The obligations set out in paragraphs 1, 1 a, 1 b 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 to the addressee, the addressee shall inform the issuing authority as well as, where a notification took place, the enforcing authority referred to 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 addressee, and, where a notification took place in accordance with Article 10a, the enforcing authority, 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, 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 1a, 1 b 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 and if necessary, set a new deadline for the addressee 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. During the procedure referred to in paragraphs 1 to 5, the addressee shall preserve the data requested, where possible. The preservation shall be upheld until the data is produced or until the EPOC is withdrawn.

   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 addressee without 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 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 V.

2. Where within the time period set out in paragraph 1 the issuing authority confirms that the subsequent request for production has been issued, the addressee shall preserve the data as long as necessary to produce the data once the subsequent request for production is received.

3. 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.

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.

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, whether to withdraw, adapt or maintain the Order.

4. Where the addressee cannot comply with its obligation because the EPOC-PR 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, for the addressee, to fulfil its obligations 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 ofde facto impossibility due to circumstances not attributable to the addressee, the addressee shall inform the issuing authority referred to 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 addressee that the EPOC-PR no longer needs to be executed.

6. In all cases where the addressee does not preserve the requested information, for other reasons listed in the Form of Annex III, it 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 addressee.

Article 10a

Grounds for refusal for European Production Orders

1. Where the issuing authority has notified the competent authority of the enforcing State in accordance with Article 7a, and without prejudice to Article 1(2), the enforcing authority shall, as soon as possible but at the latest within 10 days of the receipt of the notification, or, in emergency cases, within 96 hours, assess the information set out in the Order and, where appropriate, raise one or more of the following grounds for refusing the Order provided that:

   (a) The data requested is protected by immunities and privileges granted under the law of the enforcing State, or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order, or;

   (b) 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

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

   (d) the conduct for which the EPOC has been issued does not constitute an offence under the law of the enforcing 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.

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 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 the transfer of all data requested in the order or whether the data may only be partly transferred or used under conditions specified by the enforcing authority.

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 without delay. 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. The issuing authority shall inform the person whose data are being sought without undue delay about the data production.

2. 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 in Article 13(3) of Directive (EU) 2016/680 are met, in which case, the issuing authority shall indicate in the case file the reasons for the delay, restriction or omission. A short justification shall also be added in the Certificate.

3. The addressees and, if different, the service providers 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.

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

Article 12

Reimbursement of costs

1. 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 shall inform the Commission about their national rules for reimbursement, and the Commission shall make them public.

2. This Article does not apply to the reimbursement of costs of the decentralised IT system as referred to in Article 18g of this Regulation.

Chapter III

Sanctions and enforcement

Article 13

Sanctions

1. Without prejudice to national laws providing for the imposition of criminal sanctions, Member States shall lay down rules on pecuniary sanctions applicable to infringements of Articles 9, 10 and 11(3) of this Regulation in accordance with Article 14 (10) and shall take all necessary measures to ensure that they are implemented. 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. Member States shall ensure that the pecuniary sanctions provided for by national laws of the Member States are effective, proportionate and dissuasive. 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.

2. Without prejudice to data protection obligations, service providers shall not be held liable in Member States for the prejudices to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR.

Article 14

Procedure for enforcement

1. 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 Article 10 a 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 shall transfer the Form set out in Annex III 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 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 applies; or

   (b) a European Preservation Order, unless the enforcing authority considers that one of the grounds provided for in paragraph 5 applies.

   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.

3. The enforcing authority shall formally require the addressees to comply with the relevant obligation, informing the addressees of the possibility to oppose the execution by invoking grounds listed in paragraphs 4 points (a) to (f) or 5 points (a) to (e), as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.

4. Enforcement of the European Production Order 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;

(b) the European Production Order has not been issued for an 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) the data requested is protected by immunities and privileges granted under the law of the enforcing State, or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order;

(g) based on the sole information contained in the EPOC, 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.

5. The enforcement of the European Preservation order 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;

(b) the addressee could not comply with the EPOC-PR because of de facto 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) the data requested is protected by immunities and privileges granted under the law of the enforcing State, or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order;

(f) 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.

6. In case of an objection by the addressee, 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.

7. Before deciding not to recognise or enforce the Order in accordance with paragraphs 2 and 6, the enforcing authority shall consult the issuing authority by any appropriate means. 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. The enforcing authority shall notify all decisions immediately to the issuing authority and to the addressee.

9. If the enforcing authority obtains the data from the addressee, it shall transmit it to the issuing authority without undue delay.

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. An effective judicial remedy shall be available against the decision to impose a fine.

Chapter IV
Conflicts of law and remedies

Article 15

Article 16

Review procedure in case of conflicting obligations

1. Where the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country, it shall 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 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. It shall be filed no later than 10 days after the date on which the addressee received 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.

5. Where the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. Where 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 fundamental 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.

5a. The court may seek information from the competent authority of the third country taking into account Directive (EU) 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 or other 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 persons whose data were 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 in which the data were being used. Remedies mentioned in this paragraph shall be without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

2. The 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.

3. When applying Article 11(1) of this Regulation, information shall be provided in due time about the possibilities under national law for seeking remedies 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, the issuing State and any other Member State to which the electronic evidence has been transmitted, 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.

Article 18

Chapter IVa

Decentralised IT system

Article 18a

Secure digital communication and data exchange between competent authorities and service providers and between competent authorities

1. Written communication between competent authorities and designated establishments or legal representatives of service providers under this Regulation, including the exchange of forms established by this Regulation and the requested data, shall be carried out through a secure and reliable decentralised IT system.

2. Member States shall ensure that the designated establishments or legal representatives of service providers located in their Member State are provided with access to the decentralised IT system via their respective national IT system.

3. Service providers shall ensure that their designated establishments or legal representatives can use the decentralised IT system via the respective national IT system in order to receive EPOCs and EPOCs-PR, send the requested data to the issuing authority and communicate in any other way with the issuing and enforcing authority, as provided for under this Regulation.

4. Written communication between competent authorities under this Regulation, including the exchange of forms established by this Regulation, and the requested data under the procedure for enforcement as provided for in Article 14, as well as written communication with competent Union agencies or bodies, shall be carried out through the decentralised IT system referred to in paragraph 1.

5. Where electronic communication in accordance with paragraph 1 or 4 is not possible due to for instance the disruption of the decentralised IT system, the nature of the transmitted material, technical limitations, such as data size, legal constraints relating to the admissibility as evidence of the requested data or to forensic requirements applicable to the requested data, or exceptional circumstances, the transmission shall be carried out by the most appropriate alternative means, taking into account the need to ensure a swift, secure and reliable exchange of information.

6. Where transmission is effected by alternative means as provided for in paragraph 5, the originator of the transmission shall record the transmission, including, as appropriate, date and time of transmission, sender and recipient, file name and size, in the decentralised IT system without undue delay.

Article 18b

Legal effects of electronic documents

Documents transmitted as part of electronic communication shall not be denied legal effect or be considered inadmissible in the context of cross-border judicial procedures under this Regulation solely on the ground that they are in electronic form.

Article 18c

Electronic signatures and seals

1. The general legal framework for the use of trust services set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council[34] shall apply to the electronic communication under this Regulation.

2. Where a document transmitted as part of the electronic communication under Article 18a(1) and 18a(4) of this Regulation requires a seal or a signature in accordance with this Regulation, the document shall feature a qualified electronic seal or qualified electronic signature as defined in Regulation (EU) No 910/2014.

Article 18d

Implementing acts

1. The Commission shall adopt implementing acts establishing the decentralised IT system for the purposes of this Regulation, setting out the following:

   – the technical specifications defining the methods of communication by electronic means for the purposes of the decentralised IT system,

   – the technical specifications for communication protocols,

   – the information security objectives and relevant technical measures ensuring minimum information security standards and a high level of cybersecurity for the processing and communication of information within the decentralised IT system,

   – the minimum availability objectives and possible related technical requirements for the services provided by the decentralised IT system.

2. The implementing act referred to in paragraph 1 of this Article shall be adopted in accordance with the examination procedure referred to in Article 18e.

---

34 Regulation (EU) No 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 (*OJ L 257, 28.8.2014, p. 73).*

3. The implementing acts referred to in paragraph 1 of this Article shall be adopted by 2 years after the entry into force of this Regulation.

Article 18e

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 18f

Reference implementation

1. The Commission shall be responsible for the creation, maintenance and development of reference implementation software which Member States may choose to apply as their back-end system instead of a national IT system. The creation, maintenance and development of the reference implementation software shall be financed from the general budget of the Union.

2. The Commission shall provide, maintain and support on a free-of-charge basis the reference implementation software.

Article 18g

Costs of the decentralised IT system

1. Each Member State shall bear the costs of the installation, operation and maintenance of the decentralised IT system's access points for which they are responsible.

2. Each Member State shall bear the costs of establishing and adjusting its relevant national IT systems to make them interoperable with the access points, and shall bear the costs of administering, operating and maintaining those systems.

3. Union agencies and bodies shall bear the costs of the installation, operation and maintenance of the components comprising the decentralised IT system under their responsibility.

4. Union agencies and bodies shall bear the costs of establishing and adjusting their case-management systems to make them interoperable with the access points, and shall bear the costs of administering, operating and maintaining those systems.

5. Service providers shall bear all necessary costs in order for them to successfully integrate and/or otherwise interact with the decentralised IT system.

Article 18h

Transition period

Before the obligation referred to in Article 18a becomes applicable, the written communication between competent authorities and designated establishments or legal representatives of service providers under this Regulation shall take place by the most appropriate alternative means, taking into account the need to ensure a swift, secure and reliable exchange of information. 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 EPOC or EPOC-PR via these channels to designated establishments or legal representatives of service providers.

Chapter V

Final provisions

Article 18i

Language

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 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.

2. In any event, as of the date of application of this Regulation, Member States shall collect 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 include:

   (a) the number of EPOCs and EPOC-PRs issued by the type of data requested, the addressees and the situation (emergency case or not);

   (aa) the number of EPOCs issued under emergency case derogations;

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

(ba) the number of notifications, and the number of EPOCs that were refused, by the type of data requested, the addressees, the situation (emergency case or not) and the ground for refusal raised;

(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 addressees 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 addressees;

(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 addressees and the situation (emergency case or not) and the number thereof fulfilled;

(e) the number of legal remedies used against European Production 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. As of the date of application of this Regulation, for the data exchanges carried out via the decentralised IT system pursuant to Article 18a(1), the statistics referred to in paragraph 2 may be programmatically collected by national portals. The reference implementation software referred to in Article 18f shall be technically equipped to provide for this functionality.

4. Service providers may collect, maintain and publish statistics, 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, the Member State 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 State 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);

   d) 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.

5. As of one year after the date of application of this Regulation, 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, IV and V 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[35].

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

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

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.

Article 22

Notifications

1. By ... [12 months 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 Article 4 to issue, validate and/or transmit European Production Orders and European Preservation Orders or the notifications thereof;

   (b) the authority or authorities which are competent, in accordance with Article 7a, to receive 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 competent authorities to deal with reasoned objections by addressees in accordance with Article 16;

   (d) the 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 18 i.

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[36].

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 this 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.

Article 24

Evaluation

By 3 years from the date of application of this Regulation at the latest, the Commission shall carry out an evaluation of this Regulation. The Commission shall transmit this report to the European Parliament, the Council, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights. This overall evaluation 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. 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.

[36] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).

Article 25

Entry into force

1. 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 36 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.

2. The obligation for competent authorities and service providers to use the decentralised system established in Article 18a for written communication under this Regulation will apply from 1 year after adoption of the implementing acts referred to in Article 18d.

Done at Strasbourg,

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

ANNEX I

EUROPEAN PRODUCTION ORDER CERTIFICATE (EPOC) FOR THE PRODUCTION OF ELECTRONIC EVIDENCE

Under Regulation (EU)….[37] the addressee of this European Production Order Certificate (EPOC) must execute this EPOC and must transmit the requested data in accordance with the deadline(s) specified in Section C to the competent authority indicated under point (i) of Section L of the EPOC.

In every case, the addressee must, upon receipt of the EPOC, act expeditiously to preserve the data requested, unless the information in the EPOC does not allow it to identify this data. Preservation shall be upheld until the data is produced or until the issuing authority or, where applicable, the enforcing authority, indicates that it is no longer necessary to preserve and produce data.

The addressee must take the necessary measures to ensure the confidentiality, secrecy and integrity of the EPOC and of the data produced or preserved.

SECTION A: Issuing/validating authority

Issuing State: ……..

Issuing authority: ……..……..

Validating authority (where applicable): ……..…….

NB: details of issuing and validating authority to be provided at the end (Sections I and J)

File number of the issuing authority: …….

File number of the validating authority: …….

[37] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L …).

Council of the
European Union

SECTION B: Addressee

Addressee:……..……...…….

□ Designated establishment

□ Legal Representative

□ This order is issued in an emergency case to the specified addressee because the designated establishment or the legal representative of a service provider did not react to the EPOC within the deadlines or has not yet been designated within the deadlines set out in Directive XXXX

Address:……..

Tel. No/Fax No/email(if known):……

Contact person (if known): ……..……

File number of the addressee (if known):……..……..…

Service provider concerned (if different from addressee):……

Any other relevant information:……..…..

SECTION C: Deadlines (tick the appropriate box and complete, if necessary)

Upon receipt of the EPOC, the data requested must be produced:

□ as soon as possible and at the latest within 10 days (no notification)

□ in case of notification: at the end of the 10 days, where the enforcing authority has not raised a ground for refusal within that time period, or upon confirmation by the enforcing authority before the end of the 10 days that it will not raise a ground for refusal, as soon as possible and at the latest at the end of the 10 days

□ without undue delay and at the latest within 8 hours in an emergency case involving:

□ an imminent threat to life or physical integrity or safety of a person

□ an imminent threat to a critical infrastructure as defined in Art. 2(a) of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures, 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.

Please indicate whether there are any procedural or other deadlines which should be taken into account for the execution of this EPOC:……

Please provide additional information where relevant: ……..

SECTION D: Relation to a previous production/preservation request (tick and complete if applicable and available)

□ The requested data was totally/partially preserved in accordance with an earlier request for preservation

issued by…….……. (indicate the authority, and the file number)

on ….……(indicate the date of issuance of request)

and transmitted on ..... (indicate the date of transmission of request)

to ……..…… (indicate the service provider/ legal representative/ designated establishment/competent authority to which it was transmitted and, if available, the file number given by the addressee).

□ The requested data is related to an earlier request for production

issued by…….……..…… (indicate the authority, and the file number)

on ….……(indicate the date of issuance of request)

and transmitted on ..... (indicate the date of transmission of request)

to ……..…… (indicate the service provider/ legal representative/ designated establishment/competent authority to which it was transmitted and, if available, the file number given by the addressee).

Any other relevant information:……..

SECTION E: Information to support identification of the requested data (complete to the extent this information is known and necessary to identify the data)

IP address(es) and timestamps (incl. date and time zone):……..…….

Tel No.:……

Email address(es):…….

IMEI number(s):……

MAC address(es):……..……

The user(s) or other unique identifier(s) such as user name(s), login ID(s) or account name(s):…….……..

Name(s) of the relevant service(s): ……..

Other: …….

If applicable, the time range requested to be produced:

……

□ Additional information if needed:……

SECTION F: Electronic evidence to be produced

This EPOC concerns (tick the relevant box(es)):

□ subscriber data:

□ name, date of birth, postal or geographic address, contact information (email address, phone number) and other relevant information pertaining to the identity of the user/subscription holder

□ date and time of initial registration, type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber

□ type of service and its duration, including identifier(s) used by or provided to the subscriber at the moment of initial registration or activation (e.g. phone number, SIM-card number, MAC address) and associated device(s)

□ profile information (e.g. user name, screen name, profile photo)

□ data on the validation of the use of service, such as an alternative email address provided by the user/subscription holder

□ debit or credit card information (provided by the user for billing purposes) including other means of payment

□ PUK-codes

□ other:…….

□ data requested for the sole purpose of identifying the user as defined in Article 2(8) of the Regulation:

□ IP connection records such as IP addresses / logs / access numbers together with other technical identifiers, such as source ports and time stamps or equivalent, the user ID and the interface used, in the context of the use of the service, please specify, if necessary: ……..

□ time range (if different from section E):……

□ other:…….

□ traffic data:

(a) for (mobile) telephony:

□ outgoing (A) and incoming (B) identifiers (phone number, IMSI, IMEI)

□ time and duration of connection(s)

□ call attempt(s)

□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection

□ bearer / teleservice used (e.g. UMTS, GPRS)

□ other:…….

(b) for internet:

□ routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID)

□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection(s)

□ volume of data

□ date and time of connection(s)

□ duration of connection or access session(s)

□ other:…….

(c) for hosting:

□ logfiles

□ tickets

□ other:…….

(d) Other

□ purchase history

□ prepaid balance charging history

□ other:…….

□ content data:

□ (web)mailbox dump

□ online storage dump (user generated data)

□ pagedump

□ message log/backup

□ voicemail dump

□ server contents

□ device backup

□ contact list

□ other:…….

□ Additional information in case necessary to (further) specify or limit the range of the requested data:……

SECTION G: Information on the underlying conditions

(i) This EPOC concerns (tick the relevant box(es)):

□ criminal proceedings in respect of a criminal offence(s);

□ execution of a custodial sentence(s) or a detention order(s) of at least 4 months following criminal proceedings, that was not rendered in absentia and where the convict absconded from justice.

(ii) Nature and legal classification of the offence(s) in relation to which the EPOC is issued and the applicable statutory provision/code[38]:

……..…….……

(iii) ☐ This EPOC is issued for traffic data, which is not requested for the sole purpose of identifying the user, and / or content data, and concerns (tick the relevant box(es), if applicable):

□ criminal offence(s) punishable in the issuing State by a custodial sentence of a maximum of at least 3 years;

□ one or several of the following offence(s), if wholly or partly committed by means of an information system:

□ offence(s) as defined in Articles 3 to 8 of Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment;

□ offence(s) as defined in Articles 3 to 7 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography;

□ offence(s) as defined in Articles 3 to 8 of Directive 2013/40/EU on attacks against information systems;

□ criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 on combating terrorism.

(iv) Controller/processor:

European Production Orders shall be addressed to service providers, acting as controllers. As an exception, the European Production Order may be directly addressed to the service provider, processing the data on behalf of the controller.

[38] For execution of a custodial sentence or detention order for traffic data, which is not required for the sole purpose of identifying the user, or content data please indicate in (ii) and (iii) the offence for which the sentence was imposed.

Tick where appropriate:

□ This EPOC is addressed to the service provider, acting as controller.

□ This EPOC is addressed to the service provider who is or, in case of situations where the controller cannot be identified, possibly is processing the data on behalf of the controller, because:

□ the controller cannot be identified despite reasonable efforts on the part of the issuing authority

□ addressing the controller might be detrimental to the investigation

If the current EPOC is addressed to the service provider processing data on behalf of the controller:

□ the processor shall inform the controller about the data production

□ the processor shall not inform the controller about the data production until further notice, as it would be detrimental to the investigation. Please provide a short justification[39]: ……

(v) Any other relevant information:……..…

SECTION H: Information to the user

The addressee shall always refrain from informing the person whose data is being sought. It is the responsibility of the issuing authority to inform this person without undue delay about the data production.

Please note that (tick where appropriate):

□ the issuing authority will delay informing the person whose data are being sought, for as long as one or several of the following conditions are met:

□ to avoid obstructing official or legal inquiries, investigations or procedures;

□ to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

□ to protect public security;

□ to protect national security;

□ to protect the rights and freedoms of others.

[39] The issuing authority shall indicate the reasons for the delay in the case file, only a short justification shall be added in the EPOC

SECTION I: Details of the issuing authority

The type of issuing authority (tick the relevant box/boxes):

□ judge, court, or investigating judge

□ public prosecutor

□ other competent authority as defined by the issuing State

If validation is necessary, please fill in also Section J.

Please note that (tick if applicable):

□ This EPOC was issued for subscriber data and/or data requested for the sole purpose of identifying the user in a validly established emergency case without prior validation, because the validation could not have been obtained in time. The issuing authority confirms that it could issue an order in a similar domestic case without validation, and that ex-post validation will be sought without undue delay, at the latest within 48 hours (please note that the addressee will not be informed).

Details of the issuing authority and/or its representative certifying the content of the EPOC as accurate and correct:

Name of authority:……..……

Name of its representative:……..……...……

Post held (title/grade):……...……

File number:…..……..……

Address:……..……

Tel. No: (country code) (area/city code)……..……

Fax No: (country code) (area/city code)……..……....

Email:……..……

Language(s) spoken:……

If different from above, authority/contact point (e.g. central authority) which can be contacted for any question related to the execution of the EPOC:

Name of the authority/name:…….

Address: .....…….……

Tel. No: (country code) (area/city code)……..……

Fax No: (country code) (area/city code)……..……....

Email:……..……
Signature of the issuing authority or its representative certifying the content of the EPOC as accurate and correct:
Date: ……..……
Signature[40]:……...……

[40] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

SECTION J: Details of the validating authority (complete if applicable)

The type of validating authority

□ judge, court or investigating judge

□ public prosecutor

Details of the validating authority and/or its representative certifying the content of the EPOC as accurate and correct:

Name of the authority:……

Name of its representative:……...……

Post held (title/grade):……..……

File number:…….……..……

Address: ……...……..……..

Tel. No: (country code) (area/city code)…….……..……....

Fax No: (country code) (area/city code)…….……..

Email:…….…….

Language(s) spoken:……

Date: …….…….

Signature[41]:……..……

SECTION K: Notification and details of the notified authority (if applicable)

□ This EPOC is notified to the following enforcing authority: ……

Please provide contact details of the notified authority (if available):

Name of the authority:……

Address: .....…….……

Tel. No: (country code) (area/city code)……..……

Fax No: (country code) (area/city code)……..……....

Email:……..……

[41] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

SECTION L: Transfer of data

(i) Authority to whom the data has to be transferred

- □ issuing authority,
- □ validating authority
- □ other competent authority (e.g. central authority)

  Name and contact details:.....

(ii) Preferred format or means in which the data has to be transferred (if applicable):……..……

SECTION M: Further information to be included in the European Production Order (**not to be sent to the addressee** - to be provided to the enforcing authority in case notification is required)

The grounds for necessity and proportionality:

……

A summary description of the case:

……

Is the offence for which the European Production Order is being issued punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years and included in the list of offences set out below (tick the relevant box/boxes)?

☐ participation in a criminal organisation;

☐ terrorism;

☐ trafficking in human beings;

☐ sexual exploitation of children and child pornography;

☐ illicit trafficking in narcotic drugs and psychotropic substances;

☐ illicit trafficking in weapons, munitions and explosives;

☐ corruption;

☐ fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council ;

☐ laundering of the proceeds of crime;

☐ counterfeiting currency, including the euro;

☐ computer-related crime;

☐ environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties;

☐ facilitation of unauthorised entry and residence;

☐ murder or grievous bodily injury;

☐ illicit trade in human organs and tissue;

☐ kidnapping, illegal restraint or hostage-taking;

☐ racism and xenophobia;

☐ organised or armed robbery;

☐ illicit trafficking in cultural goods, including antiques and works of art;

☐ swindling;

☐ racketeering and extortion;

☐ counterfeiting and piracy of products;

☐ forgery of administrative documents and trafficking therein;

☐ forgery of means of payment;

☐ illicit trafficking in hormonal substances and other growth promoters;

☐ illicit trafficking in nuclear or radioactive materials;

☐ trafficking in stolen vehicles;

☐ rape;

☐ arson;

☐ crimes within the jurisdiction of the International Criminal Court;

☐ unlawful seizure of aircraft or ships;

☐ sabotage.

Where appropriate, please add any additional information that the enforcing authority may need to evaluate the possibility to raise grounds for refusals:

……..…

Council of the
European Union

ANNEX II

EUROPEAN PRESERVATION ORDER CERTIFICATE (EPOC-PR) FOR THE PRESERVATION OF ELECTRONIC EVIDENCE

Under Regulation (EU) ...[42] the addressee of this European Preservation Order Certificate (EPOC-PR) shall, without undue delay after receiving the EPOC-PR preserve the data requested. The preservation will cease after 60 days, unless extended by the issuing authority by an additional 30 days, or the issuing authority confirms that a subsequent request for production has been issued. If the issuing authority confirms within those time periods that a subsequent request for production has been issued, the addressee shall preserve the data for as long as necessary to produce the data once the subsequent request for production is received.

The addressee must take necessary measures to ensure the confidentiality, secrecy and integrity of the EPOC-PR and of the data preserved.

SECTION A: Issuing/validating authority:

Issuing State: ……

Issuing authority: ……

Validating authority (where applicable): ……

NB: details of issuing and validating authority to be provided at the end (Sections F and G)

File number of the issuing authority: …….

File number of the validating authority:…….

[42] Ref.

Council of the
European Union

SECTION B: Addressee

Addressee:……..…….……..…

□ Designated establishment

□ Legal Representative

□ This order is issued in an emergency case to the specified addressee because the designated establishment or the legal representative of a service provider did not react to the EPOC-PR within the deadlines or has not yet been designated within the deadlines set out in Directive XXXX

Address: ……..…….……

Tel. No/Fax No/email (if known):……..……

Contact person (if known): ……..……

File number of the addressee (if known) :……..……

Service provider concerned (if different from addressee): ……

Any other relevant information…….…….……..

SECTION C: Information to support identification **of** the data requested to be preserved (complete to the extent this information is known and necessary to identify the data)

□ IP address(es) and timestamps (incl. date and time zone):……..

□ Tel. No:……

□ Email address(es):……..

□ IMEI number(s):…….

□ MAC address(es):……

□ The user(s) or other unique identifier(s) such as user name(s), login ID(s) or account name(s) …….……..

□ Name(s) of the relevant service(s): ……..

□ Other: …….

If applicable, the time range requested to be preserved:

……..……

□ Additional information if needed:……..……..

SECTION D: Electronic evidence to be preserved

(i) The EPOC-PR concerns (tick the relevant box(es)):

□ subscriber data:

□ name, date of birth, postal or geographic address, contact information (email address, phone number) and other relevant information pertaining to the identity of the user/subscription holder

□ date and time of initial registration, type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber

□ type of service and its duration, including identifier(s) used by or provided to the subscriber at the moment of initial registration or activation (e.g. phone number, SIM-card number, MAC-address) and associated device(s)

□ profile information (e.g. user name, screen name, profile photo)

□ data on the validation of the use of service, such as an alternative email address provided by the user/subscription holder

□ debit or credit card information (provided by the user for billing purposes) including other means of payment

□ PUK-codes

□ other:…….

□ data requested for the sole purpose of identifying the user as defined in Article 2(8) of the Regulation:

□ IP connection records such as IP addresses / logs / access numbers together with other identifiers , such as source ports and time stamps or equivalent, the user ID and the interface used in the context of the use of the service strictly necessary for identification purposes; please specify, if necessary: ……..

□ time range (if different from section C): ……

□ other: ……

□ traffic data:

(a) for (mobile) telephony:

□ outgoing (A) and incoming (B) identifiers (phone number, IMSI, IMEI)

□ time and duration of connection(s)

□ call attempt(s)

□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection

□ bearer / teleservice used (e.g. UMTS, GPRS)

□ other:…….

(b) for internet:

□ routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID)

□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection(s)

□ volume of data

□ date and time of connection(s)

□ duration of connection or access session(s)

□ other:…….

(c) for hosting:

□ logfiles

□ tickets

□ other:…….

(d) Other

□ purchase history

□ prepaid balance charging history

□ other:…….

□ content data:

□ (web)mailbox dump

□ online storage dump (user generated data)

□ pagedump

□ message log/backup

□ voicemail dump

□ server contents

□ device backup

□ contact list

□ other:…….

□ Additional information in case necessary to (further) specify or limit the range of the requested data:……

SECTION E: Information on the underlying conditions

(i) This EPOC-PR concerns (tick the relevant box(es)):

□ criminal proceedings in respect of a criminal offence;

□ execution of a custodial sentence or a detention order of at least 4 months following criminal proceedings, that was not rendered in absentia and where the convict absconded from justice.

(ii) Nature and legal classification of the offence(s) for which the EPOC-PR is issued and the applicable statutory provision/code[43]:

……..…….……

SECTION F: Details of the issuing authority

The type of issuing authority (tick the relevant box/boxes):

□ judge, court, or investigating judge

□ public prosecutor

□ other competent authority as defined by the law of the issuing State

If validation is necessary, please fill in also section G.

Please note that (tick if applicable):

□ This EPOC-PR was issued for subscriber data and/or data requested for the sole purpose of identifying the user in a validly established emergency case without prior validation, because the validation could not have been obtained in time. The issuing authority confirms that it could issue an order in a similar domestic case without validation, and that ex-post validation will be sought without undue delay, at the latest within 48 hours (please note that the addressee will not be informed).

[43] For execution of a custodial sentence or detention order please indicate the offence for which the sentence was imposed.

This emergency case refers to an imminent threat to life or physical integrity or safety of a person or an imminent threat to a critical infrastructure as defined in Art. 2(a) of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures, 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.

Details of the issuing authority and/or its representative certifying the content of the EPOC-PR as accurate and correct:

Name of authority:……

Name of its representative:……..……

Post held (title/grade):…….……

File number:.…….……

Address:.…….……..

Tel. No: (country code) (area/city code)…….…….

Fax No: (country code) (area/city code)…….…….....

Email:…….…….

Language(s) spoken: ……

If different from above, authority/contact point (e.g. central authority) which can be contacted for any question related to the execution of the EPOC-PR:

Name of authority/name:…….

Address: .....……

Tel. No: (country code) (area/city code)……..……

Fax No: (country code) (area/city code)……..……....

Email:……..……

Signature of the issuing authority or its representative certifying the content of the EPOC-PR as accurate and correct:

Date: ……

Signature[44]:……...……

[44] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

SECTION G: Details of validating authority

The type of validating authority:

□ judge, court or investigating judge

□ public prosecutor

Details of the validating authority and/or its representative certifying the content of the EPOC-PR as accurate and correct:

Name of authority:……..…

Name of its representative:……..……

Post held (title/grade):…….……

File number:……..……

Address: …….

Tel. No: (country code) (area/city code)……..

Fax No: (country code) (area/city code)……..……

Email:……..……

Language(s) spoken:……

Date: ……..

Signature [45]:……...……

[45] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

Council of the
European Union

ANNEX III

INFORMATION ON THE IMPOSSIBILITY TO EXECUTE THE EPOC / EPOC-PR

In case the addressee cannot comply with its obligation to preserve the requested data under an EPOC-PR or to produce it under an EPOC, cannot respect the specified deadline or does not provide the data exhaustively, this form should be completed by the addressee and sent back to the issuing authority as well as, where a notification took place, to the enforcing authority referred to in the EPOC, without undue delay.

Where possible the addressee shall preserve the data requested even where additional information is needed to identify it precisely, unless the information in the EPOC/EPOC-PR is insufficient for that purpose. If clarifications by the issuing authority are needed, the addressee shall seek it without undue delay using this form.

SECTION A**:**

The following information concerns:

- □ a European Production Order Certificate (EPOC)
- □ a European Preservation Order Certificate (EPOC-PR)

SECTION B: Relevant authority(ies)

Issuing authority: ……

File number of the issuing authority: ……

If applicable, validating authority: ……

If applicable, file number of the validating authority:…….……

Date of issue of the EPOC / EPOC-PR: ……...……

Date of receipt of the EPOC / EPOC-PR: ……...……

If applicable, enforcing authority:…….

If available, file number of the enforcing authority:…….

SECTION C: Addressee of the EPOC/EPOC-PR

Addressee of the EPOC / EPOC-PR: ……..……..

File number of the addressee: …….

SECTION D: Reasons for non-execution

(i) The EPOC / EPOC-PR cannot be executed or cannot be executed within the requested deadline for the following reason(s):

□ it is incomplete

□ it contains manifest errors

□ it does not contain sufficient information

□ it does not concern data stored by or on behalf of the service provider at the time of receipt of the EPOC / EPOC-PR

□ other reasons of de facto impossibility due to circumstances not attributable to the addressee or the service provider at the time the EPOC / EPOC-PR was received

□ the European Production Order / European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4 of Regulation (EU).

□ the European Production Order to produce traffic data which is not requested for the sole purpose of identifying the user as defined in Article 2(8) of the Regulation (EU), or content data has not been issued for an offence provided for by Article 5(4) of Regulation (EU).

□ the service is not covered by the Regulation (EU).

□ the data requested is protected by immunities and privileges granted under the law of the enforcing State, or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution of the European Production Order / European Preservation Order.

□ compliance with the European Production Order would conflict with the applicable law(s) of a third country. Please complete also Section E.

(ii) Please explain further the reasons for non-execution in this case referred to in point (i), and, where necessary, indicate and explain-any other reasons not listed under point (i) of this Section:

…….

SECTION E: Conflicting obligations, arising from a third country law

In case of conflicting obligations arising from a third country law, please include the following information:

- title of the law(s) of the third country:

……..……

- applicable statutory provision(s) and text of the relevant provision(s):

……..……..……

- nature of the conflicting obligation, including the interest protected by the law of the third country:

□ fundamental rights of individuals (please specify):

……..……..

□ fundamental interests of the third country related to national security and defense (please specify):

……

□ other interests (please specify):

……..…….

- explain why the law is applicable in this case:

……..……..……

- explain why you consider there is a conflict in this case:

……..……

- explain the link between the service provider and the third country in question:

……..……

- possible consequences for the addressee of complying with the European Production Order, including the sanctions that may be incurred:

……...……..…

Please add any relevant additional information:……

SECTION F: Request for additional information/clarification (complete, if applicable)

Further information is required from the issuing authority for the EPOC/ EPOC-PR to be executed:

……..……

SECTION G: Preservation of data

The requested data (tick the relevant box and complete):

□ is being preserved until the data is produced or until the issuing authority, or where applicable, the enforcing authority, informs that it is no longer necessary to preserve and produce data or until the necessary information is provided by the issuing authority to allow to narrow down the data to be preserved/produced

□ is not being preserved (this should only be the case exceptionally, e.g. if the service provider does not have the data upon receipt of the request or cannot identify the requested data sufficiently)

SECTION H: Contact details of the designated establishment/ legal representative of the service provider

Name of the designated establishment / legal representative of the service provider:….……..……

Name of the contact person: ……..…….……..……

Post held:……..…….……

Address:..…….……..

Tel. No: (country code) (area/city code)…….…….

Fax No: (country code) (area/city code)…….…….....

Email:…….…….

Name of the authorised person:……

Date……..

Signature[46]:……..

[46] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

ANNEX IIIa

CATEGORIES OF OFFENSES REFERRED TO IN ARTICLE 10a(1)(d)

(1) participation in a criminal organisation;
(2) terrorism;
(3) trafficking in human beings;
(4) sexual exploitation of children and child pornography;
(5) illicit trafficking in narcotic drugs and psychotropic substances;
(6) illicit trafficking in weapons, munitions and explosives;
(7) corruption;
(8) fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council[47];
(9) laundering of the proceeds of crime;
(10) counterfeiting currency, including the euro;
(11) computer-related crime;
(12) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties;
(13) facilitation of unauthorised entry and residence;
(14) murder or grievous bodily injury;
(15) illicit trade in human organs and tissue;
(16) kidnapping, illegal restraint or hostage-taking;
(17) racism and xenophobia;
(18) organised or armed robbery;
(19) illicit trafficking in cultural goods, including antiques and works of art;
(20) swindling;
(21) racketeering and extortion;
(22) counterfeiting and piracy of products;
(23) forgery of administrative documents and trafficking therein;
(24) forgery of means of payment;
(25) illicit trafficking in hormonal substances and other growth promoters;
(26) illicit trafficking in nuclear or radioactive materials;
(27) trafficking in stolen vehicles;
(28) rape;

[47] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29).

(29) arson;
(30) crimes within the jurisdiction of the International Criminal Court;
(31) unlawful seizure of aircraft or ships;
(32) sabotage;

Council of the
European Union

ANNEX IV

CONFIRMATION OF ISSUANCE OF REQUEST FOR PRODUCTION FOLLOWING A EUROPEAN PRESERVATION ORDER

Under Regulation (EU)….[48], upon receipt of the European Preservation Order Certificate (EPOC-PR) the addressee shall, without undue delay, preserve the data requested. The preservation shall cease after 60 days, unless extended by the issuing authority by an additional 30 days, or the issuing authority confirms that the subsequent request for production has been issued, using the form set out in this Annex.

Following this confirmation, the addressee shall preserve the data for as long as necessary to produce the data once the subsequent request for production is received.

SECTION A: Issuing authority of the EPOC-PR

Issuing State: ……..

Issuing authority: ……..……..

If different from the contact point indicated in the EPOC-PR, authority/contact point which can be contacted for any question related to the execution of the EPOC-PR:

Name and contact details:.....…….……

SECTION B: Addressee of the EPOC-PR

Addressee:……..……...

Address:……

Phone/fax/email (if known):……

Contact person (if known): ……..……

File number of the addressee (if known):……..……..…

Service provider concerned (if different from addressee):……

Any other relevant information:……..…

[48] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*OJ L …*).

SECTION C: Information about the EPOC-PR

The data is preserved in accordance with the EPOC-PR issued on ……(indicate the date of issuance of request) and transmitted on ……. (indicate the date of transmission of request) with the file number ……(indicate file number).

□ It was extended by 30 days by the issuing authority…., file number…. on ….. (tick the box and indicate, if applicable).

SECTION D: Confirmation

This confirms that the following request for production has been issued (tick the appropriate box and complete, if necessary)

□ EPOC issued by…….…… (indicate the authority) on ……(indicate the date of issuance of request) and transmitted on …….. (indicate the date of transmission of request) with the file number ……(indicate file number) and transmitted to ……..…… (indicate the service provider/ designated establishment/ legal representative/ competent authority to which it was transmitted and, if available, the file number given by the addressee).

□ EIO request issued by…….…… (indicate the authority) on ……(indicate the date of issuance of request) and transmitted on …… (indicate the date of transmission of request) with the file number ……(indicate file number) and transmitted to ……..…… (indicate the State and competent authority to which it was transmitted and, if available, the file number given by the requested authorities).

□ MLA request issued by…….…… (indicate the authority) on ……(indicate the date of issuance of request) and transmitted on …….. (indicate the date of transmission of request) with the file number ……(indicate file number) and transmitted to ……..…… (indicate the State and competent authority to which it was transmitted and, if available, the file number given by the requested authorities).

Signature of the issuing authority and/or its representative

Name:…….

Date: ……

Signature[49]: ……..

[49] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

Council of the
European Union

ANNEX V

EXTENSION OF THE PRESERVATION OF ELECTRONIC EVIDENCE

Under Regulation (EU) ...[50], upon receipt of the European Preservation Order Certificate (EPOC-PR) the addressee shall, without undue delay, preserve the data requested. The preservation will cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been issued. 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 this Annex.

SECTION A: Issuing authority of the EPOC-PR

Issuing State: ……

Issuing authority: ……

File number of the issuing authority: …….

If different from the EPOC-PR, authority/contact point which can be contacted for any question related to the execution of the EPOC-PR:

Name and contact details:.....…….……

SECTION B: Addressee of the EPOC-PR

Addressee:……..……..……..…

Address: ……..……..……

Phone/fax/email (if known): ……..……

Contact person (if known): ……..……

File number of the addressee (if known) :……..……

Service provider concerned (if different from addressee): ……

Any other relevant information:……..……..……..

[50] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*OJ L …*).

SECTION C: Information on prior EPOC-PR

The data is preserved in accordance with the EPOC-PR issued on ……(indicate the date of issuance of request) and transmitted on …… (indicate the date of transmission of request) with the file number ……(indicate file number) and transmitted to ……..…….

SECTION D: Extension of the prior preservation order

The obligation to preserve data under the EPOC-PR as specified in Section C is hereby extended by an additional 30 days.

Signature of the issuing authority and/or its representative

Name: ……

Date:……

Signature[51]:……..

[51] If the decentralised IT system is not used, please also add an official stamp, electronic seal or equivalent authentication.

ANNEX 2

DIRECTIVE (EU) 2023/...
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of ...

laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic 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[1],

Acting in accordance with the ordinary legislative procedure[2],

[1] OJ C 367, 10.10.2018, p. 88.
[2] Position of the European Parliament of … (not yet published in the Official Journal) and decision of the Council of ….

Whereas:

(1) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the country where the relevant service 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.

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

(5) The absence of a Union-wide approach results in legal uncertainty affecting 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.

(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[3]. To increase the level of protection for the data subjects, the rules of Regulation (EU) 2016/679 of the European Parliament and of the Council[4] 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.

(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.

---

3 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).

4 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).

(8) The designated establishment and legal representative at issue should serve as an addressee for decisions and orders for the purpose of gathering electronic evidence on the basis of Regulation (EU) 2023/XXX of the European Parliament and of the Council[5] [e-Evidence Regulation], Directive 2014/41/EU[6], 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[7], including where those orders and decisions are transmitted in the form of a certificate. Recourse to the designated establishment or the legal representative should be in accordance with the procedures set out in the instruments and legislation applicable to the judicial proceedings, including whether the instrument permits the direct serving of orders in cross-border situations on the designated establishment or legal representative of the service provider, or is based on cooperation between competent judicial authorities. The competent authorities of the Member State where the designated establishment is established or the legal representative resides should act in accordance with the role set out for them in the respective instrument where an involvement is foreseen. Member States may also address decisions and orders for the purpose of gathering electronic evidence on the basis of national law to a natural or legal person acting as legal representative or designated establishment of a service provider on their territory.

---

5 Regulation (EU) 2023/XXX of the European Parliament and of the Council on European Production and preservation orders for electronic evidence in criminal matters.

6 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.

7 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 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.

(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. Without prejudice to data protection safeguards, such designated establishment or legal representative could be shared between several service providers, in particular by small and medium-sized enterprises.

(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.

(11) For the purpose of gathering electronic evidence in criminal proceedings, Member States should be able to continue addressing service providers established on their territory for purely domestic situations in accordance with Union law and their respective national laws. Notwithstanding the possibilities currently provided for by domestic law to address service providers on their own territory, Member States should not circumvent the principles set out in this Directive and in Regulation (EU) 2023/XXX [e-Evidence Regulation].

(12) Determining whether a service provider offers services in the Union requires an assessment whether the service provider enables either natural or legal persons, in one or more Member States, to use its services. However, the mere accessibility of an online interface in the Union, such as for instance the accessibility of the website or an e-mail address or other contact details of a service provider or an intermediary, taken in isolation, should be considered insufficient to determine that a service provider offers services in the Union within the meaning of this Directive.

(13) A substantial connection to the Union should also be relevant to determine the ambit of application of this 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. 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 generally 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 Regulation (EU) No 1215/2012 of the European Parliament and of the Council[8]. 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 of the European Parliament and of the Council[9] cannot, 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.

---

8 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

9 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 60I, 2.3.2018, p. 1).

(14) 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 this 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 designated establishments or legal representatives within Member States that do not take part in relevant legal instruments, which would fall short of addressing the problem. Therefore, at least one designated establishment or legal 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 designated establishment or legal representative for the receipt of, compliance with and enforcement of decisions and orders issued in the context of gathering electronic evidence in criminal proceedings, including under Regulation (EU) 2023/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. In addition, designating a designated establishment or 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.

(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 legal representative on their territory. However, this Directive also contains certain restrictions with regard to this free choice of service providers, notably that the designated establishment should be established in, or where applicable, the legal representative should reside in a Member State where the service provider provides services or is established, as well as the obligation to designate a designated establishment or a legal representative in one of the Member States participating in a legal instrument referred to in this Directive. The sole designation of a legal representative should not be considered to constitute an establishment of the service provider.

(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 Directive (EU) 2018/1972 of the European Parliament and of the Council[10]. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. This Directive should also be applicable to other information society service providers within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council[11] that do not qualify as electronic communications service 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. 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.

---

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

11 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).

(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 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.

(18) 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 this Directive. Neither should service providers be able to exculpate themselves due to missing or ineffective internal procedures, as they are responsible for providing the necessary resources and powers to guarantee compliance with orders and national decisions. Nor should designated establishments or legal representatives be able to exculpate themselves by claiming, for example, that they are not empowered to deliver data. 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 by either of them. 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.

(19) Member States should ensure that 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, the respective 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. Where a service provider designates several designated establishments or legal representatives in accordance with this Directive, Member States should ensure that such service provider indicates, 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 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 information may also be further disseminated to facilitate access to this information by competent authorities, such as via dedicated intranet sites or forums and platforms.

(20) Service providers should be subject to effective, proportionate and dissuasive sanctions for the infringement of its obligations deriving from this Directive. Member States should, by the date set out in this Directive, notify the Commission of their rules and of measures regarding such sanctions 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. 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 should 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.

(20a) When determining the appropriate sanction applicable to infringements by service providers, the competent authorities should take into account all relevant circumstances, such as the financial capacity of the service provider, 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.

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

(22) In order to ensure the application of this 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 authorities that can provide central authorities in other Member States with information and assistance in the application of this Directive, in particular where enforcement actions under this 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. 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 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 this Directive. The designation and publication of information about central authorities will facilitate the notification by service providers of the designation and contact details of their designated establishment or legal representative to the Member State where their designated establishment is established or legal representative resides. 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.

(23) Since the objective of this Directive, namely to remove obstacles to the free provision of services in the framework of gathering electronic 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 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[12] and delivered an opinion on 6 November 2019[13],

(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 3 years and 6 months 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.

HAVE ADOPTED THIS DIRECTIVE:

[12] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[13] OJ C 32, 31.1.2020, p.11.

Article 1

Subject matter and scope

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

2. This Directive applies to decisions and orders for the purpose of gathering electronic evidence on the basis of Regulation (EU) 2023/XXX [e-Evidence Regulation], Directive 2014/41/EU 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 the Union. This Directive equally applies to decisions and orders for the purpose of gathering electronic evidence on the basis of national law addressed by a Member State to a natural or legal person acting as legal representative or designated establishment of a service provider on the territory of that Member State.

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 of gathering electronic evidence in criminal proceedings.

4. 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 for the purposes set out in paragraph 1.

5. 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 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);

(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 of the European Parliament and of the Council[14]:

(a) electronic communications service as defined in Article 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council[15];

(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[16] 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 is provided, where the storage of data is a defining component of the service provided to the user;

---

14 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

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

16 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).

(3) ‘offering services in a Member State’ means:

(a) enabling natural or legal 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(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;

(4) ‘establishment’ means an entity actually pursuing 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 with a legal personality 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);

Article 3

Designated establishment and legal representative

1. Member States shall ensure that service providers offering services in the Union designate at least one addressee 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 with legal personality, 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 in accordance with Article 2(4a);

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

(c) For service providers established in Member States not taking part in the instruments 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.

2. Member States shall ensure that the addressees defined in paragraph 1:

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

(b) can be subject to enforcement procedures.

3. 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.

4. Member States shall 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 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.

5. 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 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 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.

6. Member States shall ensure that the obligation to designate designated establishments or legal representatives 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 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, the respective contact details and any changes thereof.

2. The notification shall specify the official language(s) of the Union, as referred to in Council Regulation No 1[17], in which the legal representative or designated establishment can be addressed. This shall include one or more of the official languages in accordance with the national law of the Member State where the legal representative resides or designated establishment is established.

[17] Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385).

3. When a service provider designates several designated establishments 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.

4. Member States shall ensure that the information notified to them in accordance with this Article is publicly available on a dedicated 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, 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 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 publicly available.

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 30 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 [3 years and 6 months from the date of application of this Directive] at the latest, the Commission shall carry out an evaluation of this Directive. The Commission shall transmit this report to the European Parliament and the Council. 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 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
The President

For the Council
The President