AMENDMENTS 001-001
by the Committee on Civil Liberties, Justice and Home Affairs

Report
Birgit Sippel **A9-0256/2020**
Electronic evidence regulation: European production and preservation orders for electronic evidence in criminal matters

Proposal for a regulation (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European Production and Preservation Orders for electronic *information* 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 Article 82(1) thereof,

Having regard to the proposal from the European Commission,

---

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

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,

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 ***information*** are increasingly important to enable criminal investigations and prosecutions across the Union. Effective mechanisms to obtain electronic ***information*** 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) ▌

(4) ▌

(5) ▌

(6) ▌

(7) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the relevant country ***where the service is offered***. ***Therefore***, relevant ***electronic information*** is often stored outside of the investigating State***, creating challenges regarding the gathering of electronic information in criminal proceedings***.

(8) Due to this, 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. As a result, obtaining electronic ***information*** using judicial cooperation channels often takes a long time ***which may cause problems due to the often volatile nature of electronic information***. Furthermore, there is no ***harmonised*** framework for cooperation with service providers, while certain third-country providers accept direct requests for non-content data as permitted by their applicable domestic law. As a consequence, all Member States ***increasingly*** rely on ***voluntary direct*** cooperation channel***s*** with service providers where available, ***applying*** different national tools, conditions and procedures.

[1] OJ C , , p. .

(9) The fragmented legal framework creates challenges for ***law enforcement, judicial authorities and*** 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 ***information, in order to complement the existing EU law and to clarify the rules of the cooperation between law enforcement, judicial authorities and service providers in the field of electronic information, while ensuring full compliance with fundamental rights and principles recognised in Article 6 TEU and the Charter and with the rule of law***.

(9a) Directive 2014/41/EU of the European Parliament and of the Council[1] provides for the acquisition, access and production of evidence in one Member State for criminal investigations and proceedings in another Member State. The procedures and timelines foreseen in the EIO may not be appropriate for electronic information, which is more volatile and could more easily and quickly be deleted. This Regulation therefore provides for specific procedures that address the nature of electronic information. However, in order to avoid a long-term fragmentation of the Union framework for judicial cooperation in criminal matters, in the mid-term, the Commission should assess the functioning of the Regulation in relation with Directive 2014/41/EU.

(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 respect for private and family life, the protection of personal data, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of legality and proportionality, as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence.

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

(11) The mechanism of the European Production Order and the European Preservation Order for electronic ***information*** in criminal ***proceedings*** work***s*** on the ***condition*** of mutual trust between the Member States ***and a presumption of compliance by other Member States with Union law, the rule of law and, in particular, with fundamental***

---

1 ***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).***

rights, which are essential ***elements of the area of freedom, security and justice within the Union. However, if the executing authority has substantial grounds for believing that the execution of a European Production Order would not be compatible with its obligations concerning the protection of fundamental rights recognised in Article 6 TEU and in the Charter, the execution of the European Production Order should be refused. Before deciding to raise one of the grounds for non-recognition or non-execution provided for in this Regulation, the executing authority should consult the issuing authority in order to obtain any necessary additional information. Information regarding a reasoned proposal by the Commission to the Council on the basis of Article 7(1) and 7 (2) TEU, indicating systemic or generalised deficiencies, should be particularly relevant for the purposes of that assessment.***

(11a) If the European Council were to adopt a decision determining, as provided for in Article 7(2) TEU, that there is a serious and persistent breach in the issuing Member State of the principles set out in Article 2 TEU, such as those inherent in the rule of law, the executing judicial authority may decide automatically to raise one of the grounds for non-recognition or non-execution provided for in this Regulation, without having to carry out any specific assessment.

(11b) 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 and Article 16(1) of the TFEU, everyone has the right to respect for his or her private and family life, home and communicatons and to the protection of personal data concerning them. When implementing this Regulation, Member States should ensure that personal data are protected and processed only in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council [1] and Directive (EU) 2016/680 of the European Parliament and of the Council[2], as well as Directive 2002/58/EC of the European Parliament and of the Council[3].

(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

---

1 ***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).***

2 ***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).***

3 ***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).***

purposes of this Regulation, including measures to ensure the security of the data. Service providers should ensure that the same safeguards apply for the transmission of personal data to relevant authorities. Only authorised persons should have access to information containing personal data.

(12) ▌

(13) ▌

(13a) According to the European Court of Justice case-law, a general and indiscriminate data retention by EU national security authorities seriously interferes with the privacy rules enshrined, in particular, in the EU Charter of Fundamental Rights. Therefore, the application of this Regulation should not have the effect of resulting in any general and indiscriminate retention of data, nor should it affect any rights of or obligations incumbent on service providers concerning the security of data, including the right to encryption.

(14) ▌The procedural rights in criminal proceedings set out in Directives 2010/64/EU[1], 2012/13/EU[2], 2013/48/EU[3], 2016/343[4], 2016/800[5] and 2016/1919[6] of the European Parliament and of the Council ***should apply, within the scope of those Directives, to criminal proceedings covered by this Regulation as regards the Member States bound by those Directives. The procedural safeguards under the Charter apply to all proceedings covered by this Regulation.***

(14a) Where the issuing Member State has reason to believe that parallel criminal proceedings may be ongoing in another Member State, it should consult the authorities of the latter Member State in accordance with Council Framework Decision 2009/948/JHA[7].

(15) This instrument lays down the rules under which, ***in a criminal proceeding***, a

---

1 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).

2 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).

3 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).

4 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).

5 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).

6 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).

7 ***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).***

competent judicial authority in the European Union may order a service provider offering services in the Union to produce or preserve electronic ***information that may serve as evidence*** through a European Production or Preservation Order. This Regulation is applicable in all ***cross-border*** cases where the service provider has its main ***establish***ment in another Member State, ***or, where it is not established in the Union, is legally*** represented in another Member State. ***Authorities of the Member States should not issue domestic orders with extraterritorial effects for the production or preservation of electronic information that could be requested on the basis of this Regulation.***

(16) The service providers most relevant for ***gathering electronic information 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***[1] ▌. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. The categories of information society services included ***in this Regulation*** are those for which the storage of data is a defining component of the service provided to the user, and refer in particular to social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and other hosting services, including where the service is provided via cloud computing.

(17) ▌

(18) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries 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.

(18a) Orders under this Regulation should be addressed to the main establishment of the service providers or to legal representatives designated for that purpose as regards service providers not established in one of the Member States bound by this Regulation. As regards a service provider with establishments in more than one Member State, the main establishment should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of data are taken in another establishment of the service provider in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions should be considered to be the main establishment.

(19) This Regulation regulates gathering of ***data*** stored by a service provider at the time of ***the issuing*** of a European Production or Preservation Order ***only***. It does not stipulate a general data retention obligation, nor does it authorise interception of data or

---

[1] ***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).***

obtaining data stored at a future point from the ***issuing*** of a ***European*** production or preservation order.

(20) The categories of data ***which*** this Regulation covers include subscriber data, ***traffic*** data and content data. ***Such categorisations are 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) It is appropriate to single out ***subscriber*** data as a specific data category used in this Regulation. ***Subscriber*** data is pursued to identify the underlying user, and the level of interference with fundamental rights is ***lower than is the case with other, more sensitive data categories***.

(22) ***Traffic*** data, on the other hand, is generally pursued to obtain ***more privacy-intrusive*** information***, such as*** the contacts and whereabouts of the user and may be served to establish a ***comprehensive*** profile of an individual concerned. ***Therefore, as regards its sensitivity, traffic data is comparable to content data***.

(22a) IP addresses can constitute a crucial starting point for criminal investigations in which the identity of a suspect is not known. 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. However, for the purpose of a specific criminal investigation, law enforcement authorities might request an IP address for the sole purpose of identifying the user and, in a subsequent step, the name or address of the subscriber or the registered user. In such cases, it is appropriate to apply the same regime as for subscriber data, as defined under this Regulation.

(22b) Metadata can be processed and analysed more easily than content data, as it is already brought into a structured and standardised format, but, where derived from electronic communications services or protocols, it may also reveal very sensitive and personal information. It is therefore essential that, where metadata of other electronic communications services or protocols are stored, transmitted, distributed or exchanged by using the respective services/by the service providers, they are to be considered content data.

(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 on the one hand and ***traffic*** data and content data on the other. While subscriber data and ***IP addresses*** could be useful to obtain first leads in an investigation about the identity of a suspect, ***traffic*** and content data are ***often more*** relevant as probative material***, which could finally lead to a conviction of the suspect.*** 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) The European Production Order and the European Preservation Order are investigative measures that should be issued only in the framework of specific criminal proceedings ***concerning*** 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.

(25) ▌

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

(27) ***Determining*** whether a service provider offers services in the Union requires an assessment whether ***it is apparent that*** the service provider ***envisages offering services to data subjects, either*** legal or natural persons***,*** in one or more Member States ***in the Union***. However, the mere accessibility of an online interface***,*** as for instance the accessibility of the website or an e**-**mail address ***or*** other contact details ***of a service provider or an intermediary, or the use of a language also used in a Member State, should be considered insufficient to ascertain such intention***.

(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 assessed on the basis of 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 ▌.

(28a) Situations, where there is an imminent threat to life or physical integrity of a person, should be treated as emergency cases and allow for shorter time limits on the service provider and the executing authority. Where the disruption or destruction of a critical infrastructure would directly imply an imminent risk to the life or physical integrity of a person, such a situation should also be treated as an emergency case, in accordance with EU law.

(29) A European Production Order should only be issued if it is necessary and proportionate***, taking into account the rights of the suspected or accused person and the seriousness of the offence***. The assessment should take into account whether ***it could have been ordered under the same conditions in a similar domestic case, whether there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border production of the data and where the requested information is relevant for the investigation. T***he Order ***should be*** 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 ***and should be limited to data of specific persons with a direct link to the specific proceedings***. ***The direct link between the person whose data are sought and the purpose of the specific proceeding must be demonstrable at all times.***

(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*** and content data, the issuing or validation of European Production Orders for production of these categories requires review by a judge. As subscriber data are less sensitive, European Production Orders

for their disclosure can in addition be issued or validated by competent ***public*** prosecutors***, where such a public prosecutor is capable of exercising its responsibilities objectively. Where so provided by national law, the execution of the order might require the procedural involvement of a court in the executing State***.

(30a) The competent issuing authority should be considered independent where it is not exposed to the risk of being subject, directly or indirectly, to external directions or instructions, in particular from the executive, such as a Minister for Justice, in connection with the adoption of a decision. That independence should be considered to exist where, based on the appropriate statutory rules and an institutional framework, the competent issuing authority is capable of exercising his or her responsibilities objectively and acts independently in the execution of his or her responsibilities which are inherent in the issuing of a European Production or Preservation Order, taking into account all incriminatory and exculpatory evidence and without being exposed to the risk that its decision-making power be subject to external directions or instructions.

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

(32) There are specific offences where ***information*** will typically be available exclusively in electronic form, which is particularly fleeting in nature. This is the case for cyber-related crimes, even those which might not be considered serious in and of themselves but which may cause extensive or considerable damage, in particular including cases of low individual impact but high volume and overall damage. For most cases where the offence has been committed by means of an information system, applying the same threshold as for other types of offences would predominantly lead to impunity. This justifies the application of the Regulation also for those offences where the penalty frame is less than 3 years of imprisonment. Additional terrorism related offences as described in Directive 2017/541/EU ***of the European Parliament and of the Council[1] 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***

[1] ***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).***

Council[1] do not require the minimum maximum threshold of 3 years.

(33) ▌

(34) ▌

(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege***, source confidentiality***) ***or rules relating to freedom of the press and freedom of expression in other media***, are referred to in other mutual recognition instruments such as the European Investigation Order. ***There is no common definition of what constitutes an immunity or privilege in Union law. The precise definition of those terms is, therefore, left to national law. This may include protections which apply to medical (such as doctors) and legal professions, clergy or otherwise protected counsellors but also, even though they are not necessarily considered to be forms of privilege or immunity, rules relating to freedom of the press and freedom of expression in other media (such as journalists). Thus,*** the applicable national law should ***already*** be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order ***where it could have been ordered under the same conditions*** in a ***in a similar*** domestic ***case***. In addition to this basic principle, immunities and privileges which protect data in the ***executing*** State should be taken into account as far as possible in the issuing State in the same way as if they were provided for under the national law of the issuing State. This is relevant in particular should the law of the ***executing*** State provide for a higher protection than the law of the issuing State. As an additional safeguard, these aspects should be taken into account not only when the Order is issued, but also later, ***during the notification procedure or*** when assessing the relevance and admissibility of the data concerned at the relevant stage of the criminal proceedings, and if an enforcement procedure takes place, by the ***executing*** authority.

(36) The European Preservation Order may be issued for any ***criminal*** offence***, where it could have been ordered under the same conditions in a similar domestic case in the issuing State, where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border preservation of the data and where the requested information is relevant for that investigation. It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in this Regulation and the direct link between the person whose data are sought and the purpose of the specific processing must be demonstrable at all times***. ***The*** aim ***of European Preservation Orders*** is to prevent the removal, deletion or alteration of relevant data in situations where it may take more time to obtain the production of this data.

(37) European Production and Preservation Orders should be addressed to the ***main establishment of the service provider where the data controller is, or, where not established in the Union or one of the Member States bound by this Regulation, to its*** legal representative designated by the service provider. ***Simultaneously, it should be addressed directly to the executing authority***.

---

[1] ***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).***

(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). The Certificates should contain the same mandatory information as the Orders. Where necessary, a Certificate ***should*** be translated into (one of) the official language(s) of the ***executing*** State ***and the service provider***, or into another official language that the ***Member State or the*** service provider ***have*** declared ***they*** will accept. ***In this regard, Member States should be allowed, at any time, to state in a declaration submitted to the Commission that they would accept translations of EPOCs and EPOC-PRs in one or more official languages of the Union other than the official language or languages of that Member State. The Commission should make the declarations available to all Member States and to the European Judicial Network in criminal matters.***

(39) The competent issuing authority should transmit the EPOC or the EPOC-PR directly to the addressee***s, via a common European digital exchange system established by the Commission by [date of application of this Regulation]. This system should allow for secure channels for the handling of authorised cross-border communication, authentication and transmission of the Orders and of the requested data between the competent authorities and service providers, by guaranteeing an effective, reliable and smooth exchange of the relevant information and a high level of security, confidentiality and integrity as well as the necessary protection of privacy and personal data in line with Regulation (EU) 2018/1725 of the European Parliament and of the Council [1], Regulation (EU) 2016/679, Directive (EU) 2016/680, and Directive 2002/58/EC. To this end, open and commonly used state-of-the-art electronic signature and encryption technology should be applied. The system should also allow the addressees to*** produc***e*** a written record under conditions that allow the ***addressees*** to establish authenticity ***of the Order and of the issuing authority***, in line with the rules protecting personal data.

(39a) Where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, it should be possible to interconnect such systems or channels with this common European digital exchange system.

(40) ***Upon receipt of an EPOC for subscriber data or IP addresses for the sole purpose of identifying a person, the service provider*** should ***ensure that the requested data is*** transmitted to the ***issuing authority*** at the latest within 10 days upon receipt of the EPOC ***and within 16 hours in emergency cases***. ***Where the executing authority decides to invoke any of the grounds listed for non-recognition or non-execution provided for in this Regulation within the time periods, it should immediately inform the issuing authority and the service provider of its decision. The issuing authority should erase the data. Where the requested data has not yet been transmitted to the issuing authority, the addressed service provider may not transmit the data.***

(40a) Upon receipt of an EPOC for traffic or content data, the service provider should act expeditiously to preserve the requested data. Where the executing authority has

---

[1] ***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).***

invoked any of the grounds listed for non-recognition or non-execution provided for in this Regulation within the time periods, it should immediately inform the issuing authority and the service provider of its decision. Where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) TEU, the service provider should transmit the requested data only after receiving the explicit written approval of the executing authority. Without prejudice to this special provision, where the executing authority has not invoked any of the grounds listed in this Regulation within the time periods, the service provider should ensure that the requested data is immediately transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC.

(41) ▌

(42) Upon receipt of a European Preservation Order Certificate ('EPOC-PR'), the service provider should ***act expeditiously to*** preserve ***the*** requested data for a maximum of 60 days***. The 60 day period is calculated to allow for the launch of an official request for production. It may only be extended by additional 30 days, where necessary to allow further assessment of the relevance of the data in the ongoing investigations in order to prevent that potentially relevant data is lost before the European Preservation Order ends. Where*** the issuing authority ***submits the subsequent European Production Order to*** the ***addressees within these time periods, the service provider*** should continue ***to preserve the data as long as necessary for the execution of the European Production Order***.

(42a) In order to allow the service provider to address problems, in cases where the EPOC or EPOC-PR might be incomplete, in form or content, contain manifest errors or not enough information to execute the Order, it is necessary to set out a procedure for the communication, to ask for clarification or, where necessary, correction from the issuing authority. Moreover, there might be cases where the service provider cannot provide the information in cases of force majeure or of a de facto impossibility not attributable to the service provider, or cannot provide it in an exhaustive or timely manner for any other reason. Such reasons could be technical or operational (e.g. operational limitations of small and medium-sized enterprises). In these cases, the service provider also should go back to the issuing authorities and provide the opportune justifications, as well as where it considers the Order to be manifestly abusive or excessive For example, an Order requesting the production of data pertaining to an undefined class of people in a geographical area or with no link to concrete criminal proceedings would ignore in a manifest way the conditions for issuing a European Production or Preservation Order. The communication procedure thus should broadly allow for the correction or reconsideration of the EPOC or EPOC-PR by the issuing authority at an early stage. Where clarification or correction is needed, the issuing authority should react expeditiously and within 5 days at the latest. In the absence of a reaction from the issuing authority, the order should be considered null and void. Where the relevant conditions are fulfilled, the issuing authority should set a new deadline or withdraw the order. To guarantee the availability of the data, the service provider should preserve the requested data during this procedure, where possible.

(42b) Notwithstanding the principle of mutual trust, the executing authority should be able to refuse the recognition of execution of a European Production Order, where such refusal is based on the fact that the conditions for issuing a European Production Order as laid down this Regulation are not fulfilled or based on further

specific grounds as listed in this Regulation.

(42c) 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. Therefore, where the executing authority assesses the Order, it should refuse the execution of a European Production Order if its execution would be contrary to that principle.

(42d) Furthermore, where the executing authority assesses the Order and there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter, the executing authority should refuse the execution of a European Production Order.

(42e) In addition, where the recognition or execution of a European Production Order would involve the breach of an immunity or privilege in the executing State, the executing authority should refuse that order in cases where it is assessed by the executing authority.

(42f) Due to the more intrusive character of European Production Orders for traffic and content data, the executing authority should have additional optional grounds for non-recognition and non-execution at their disposal for these data categories.

(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 service provider should inform*** the person whose data is being sought ***without undue delay. When informing the person, the service provider should take the necessary state-of-the-art operational and technical measures to ensure the security, confidentiality and integrity of the EPOC or the EPOC-PR and of the data produced or preserved***.

(43a) As long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings or in order to protect the fundamental rights of another person, the issuing authority, taking due account of the impact of the measure on the fundamental rights of the person whose data is sought, may request the service provider to refrain from informing the person whose data is being sought, based on a judicial order, which should be duly justified, specify the duration of the obligation of confidentiality and be subject to periodic review. Where the issuing authority requests the service provider to refrain from informing the person, the issuing authority should inform the person whose data is being sought without undue delay about the data production or preservation. That information could be delayed as long as necessary and proportionate, taking into account the rights of the suspected and accused person and without prejudice to defence rights and effective legal remedies. User information should include information about any available remedies as referred to in this Regulation.

(43b) Electronic information obtained in accordance with this Regulation should not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except for where there is an imminent threat to the life or physical integrity of a person. Where the disruption or destruction of a critical infrastructure would directly imply an imminent risk to the life or physical integrity of a person, such a situation should also be treated as an imminent threat to the life or physical integrity of a person, in accordance with EU law.

(43c) Electronic information that has been gathered in breach of any of the conditions listed in this Regulation should be erased without undue delay. Electronic information that is no longer necessary for the investigation or prosecution for which it was produced or preserved, including possible appeals, should also immediately be erased, unless this would affect the defence rights of the suspected or accused person. For this purpose, periodic reviews for the need of the storage of the electronic information should be established. The person whose data was sought should be informed about the erasure.

(43d) Electronic information that has been gathered in breach of this Regulation should not be admissible before a court. This should also include all cases where the criteria laid down in this Regulation are not fulfilled. Where electronic information has been obtained before a ground for non-recognition listed in this Regulation has been invoked, it neither should be admissible before a court. When assessing the admissibility of electronic information, obtained in accordance with this Regulation, the competent judicial authorities should at any stage of the proceedings ensure that the rights of the defence and the fairness of the proceedings are respected. For such an assessment, the competent judicial authorities should also take into due account whether the criteria laid down in this Regulation were fulfilled, in particular where the data sought might be protected by immunities or privileges.

(43e) Where claimed by the service provider, the issuing State should reimburse the justified costs born by the service provider and related to the execution of the European Production Order or the European Preservation Order. To this end, Member States should inform the Commission on the rules for reimbursement, which the Commission should make public. Where for practical reasons, such as the economic size of the service provider, different language regimes between the issuing State and the executing State or different national rules for the reimbursement of costs between these States, the service provider is substantially hampered from claiming the reimbursement of costs related to the execution of a European Production Order or European Investigation order from the issuing State, the service provider should be entitled to claim reimbursement of the costs from the executing State. Where the service provider chooses the executing State, the issuing State should reimburse the executing State for these costs.

(43f) Member States should lay down the rules on sanctions applicable to infringements of the obligations pursuant to this Regulation. These sanctions should be effective, proportionate and dissuasive. When determining the appropriate sanction applicable to infringements of service providers, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence and whether the service provider was held responsible for similar previous breaches. Particular attention should, in this respect, be given to micro enterprises.

(43g) Where a service provider acts with due diligence, in particular with regards to data protection obligations, and requested clarification or justification from the issuing authority, in accordance with this Regulation, it should not be held liable for the consequences of any delays caused. In addition, sanctions applied to infringements of the obligations of service provider pursuant to this Regulation should be annulled, where an order has been successfully challenged in accordance with this Regulation.

(44) ***Where the service provider does not comply with an EPOC within the deadlines or with an EPOC-PR, without providing sufficient reasons, and where, as regards the EPOC, the executing authority has not invoked any of the grounds as provided for in this Regulation***, the issuing authority may ***request*** the competent authority in the ***executing*** State ***to enforce the Order***. ***In such a case, the executing*** State should ***formally require the service provider to comply with the Order, informing the service provider of the possibility to oppose the execution by invoking one of the grounds which the service provider has at its disposal for correction or reconsideration of the order, in accordance with this Regulation***. ***Where a service provider still does not comply with its obligations,*** Member States should ***impose a*** sanction ***in accordance with this Regulation***.

(45) ▌

(46) ▌

(47) In addition to the individuals whose data is ***sought***, the ***laws of a*** third ***country*** may be affected by the investigative measure. ***In such situations, judicial cooperation based on international agreements would generally be the most appropriate way to request electronic information when conflicts of law with a third country arise. Without prejudice to such international agreements and in order t***o 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 review where ***the service provider or the executing authority consider that*** compliance with a European Production Order ***or a European Preservation Order*** would ***conflict with applicable laws of*** third ***country prohibiting disclosure of the data concerned***.

(48) To this end, whenever the ***the service provider or the executing authority*** consider that the European Production Order ***or the European Preservation 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 ***and the relevant addressees, without undue delay and at the latest within 10 days from the receipt of the order, thereby suspending the execution of the Order***. ***Such notice should include all relevant details on the law of the third country, its applicability in the case at hand and the nature of the conflicting obligation.*** The issuing authority should then review the European Production Order ***or European Preservation Order, within 10 days of receiving the notice***, taking into account criteria ***including the interests protected*** by the relevant ***law, the connection of the criminal case and the third country, the connection between the service provider and the third country, the interests of the issuing*** State ***in obtaining the electronic information and the possible consequences for the addressees of complying with the European Production Order or the European Preservation*** Order. ***During this procedure, the requested data should be preserved where possible.***

(48a) The issuing authority should be able to withdraw, uphold or adapt the Order where necessary, to give effect to the relevant criteria. In the event of withdrawal, the issuing authority should immediately inform the addressees of the withdrawal. Where the

issuing authority decides to uphold the Order, it should inform the addressees of its decision. The executing authority, while duly taking into account the decision of the issuing authority should take a final decision based on the criteria listed in this Regulation, within 10 days of receiving the decision of the issuing authority, and inform the issuing authority and the service provider of its final decision.

(49) In determining the existence of a conflicting obligation in the specific circumstances of the case under examination, the ***issuing authority and the executing authority should seek information from the*** competent ***authority of the third country***, for example if the review raises questions on the interpretation of the law of the third country concerned***, in compliance with Directive (EU) 2016/680 and to the extent that this does not obstruct the deadlines provided for in this Regulation***.

(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) ▌

(52) ▌

(53) ▌

(54) ▌In line with Article 47 of the Charter of Fundamental Rights of the European Union***, it is essential that all persons whose data was sought via a European Production Order or a European Preservation Order have*** the right to effective remed***ies against such Orders in the issuing and executing State in accordance with national law, including*** the possibility to challenge the legality of ***the Order, including its necessity and proportionality, without prejudice to remedies available under Regulation (EU) 2016/679 and Directive (EU) 2016/680. The substantive reasons for issuing the*** European Production Order ***or the European Preservation Order*** should be ***challenged in the issuing State, without prejudice to the guarantees of fundamental rights in the executing State. The issuing authority and the executing authority should take the appropriate measures to ensure that information about the options for seeking legal remedies under national law is provided in due time, including about when such remedies become applicable, and ensure that they can be exercised effectively***.

(55) ▌

(56) ▌

(57) ▌

(57a) In order to monitor the outputs, results and impacts of this Regulation, the Commission should publish an annual report on the preceeding calendar year, based on data obtained from the Member States. For this purpose, Member States should collect and maintain comprehensive statistics from the relevant authorities on

different aspects of this Regulation, by type of data requested, the addressees (executive authority addressed), the type of service provider addressed [electronic communications service, information society service or internet domain name and IP number service (such as IP address providers, domain name registries, domain name registrars or related proxy services)] and whether it was an emergency case or not. Where applicable, the data collected should also include the grounds for non-recognition or non-execution raised, the legal remedies used, the sanctions imposed, the costs claimed by the service provider and the enforcement proceecing launched.

(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, should provide the basis for impact assessments ***and include an evaluation of the use of derogations (emergency derogation, derogation from the principle of user information) as well as an assessment of the functioning of the common European exchange system and of the functioning of this Regulation in relation with Directive 2014/41/EU*** ▌. Information should be collected regularly and in order to inform the evaluation of this Regulation.

(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information between ***different*** judicial authorities ***as well as with*** service providers, allowing ***for a quicker and more effective transmission of electronic information*** in a user-friendly manner. They ***could also*** reduce translation costs and contribute to a high quality standard. Response forms similarly should allow for a standardised exchange of information. The forms should also facilitate the gathering of statistics.

(60) ▌

(61) The measures based on this Regulation should not supersede European Investigation Orders in accordance with Directive 2014/41/EU ▌***or Mutual Legal Assistance Procedures*** to obtain electronic ***information***. Member States' authorities should choose the tool most adapted to their situation; they may prefer to use the European Investigation Order when requesting a set of different types of investigative measures including but not limited to the production of electronic ***information*** from another Member State.

(62) ▌

(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic ***information*** 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 the Protocol 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 and without prejudice to Article 4 of that Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

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

(66) The European Data Protection Supervisor was consulted in accordance with Article ***42(2)*** of Regulation ***(EU) 2018/1725***of the European Parliament and of the Council[1] and delivered an opinion on ***6 November 2019***[2],

HAVE ADOPTED THIS REGULATION:

---

1 ***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).***

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

Chapter 1: Subject matter, definitions and scope

Article 1

Subject matter

1. This Regulation lays down the rules under which an authority of a Member State***, in a criminal proceeding,*** may order a service provider offering services in the Union ***and established or, if not established, legally represented in another Member State*** to produce or preserve electronic ***information that may serve as evidence*****,** regardless of the location of data.

` ***Authorities of the Member States shall not issue domestic orders with extraterritorial effects for the production or preservation of electronic information that could be requested on the basis of this Regulation***.

1a. The issuing of a European Production or Preservation Order may also be requested on behalf of a suspected or accused person, 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, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement***,*** judicial authorities ***or service providers*** in this respect shall remain unaffected.

Article 2

Definitions

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

(1) ‘European Production Order’ means a decision ***which has been issued or validated*** by a ***judicial*** authority of a Member State ***('the issuing State') addressed to*** a service provider offering services in the Union and established or ***legally*** represented in another Member State ***bound by this Regulation (‘the executing State’)***, to produce electronic ***information***;

(2) ‘European Preservation Order' means a decision ***which has been issued or validated*** by a ***judicial*** authority of a Member State ***('the issuing State') addressed to*** a service provider offering services in the Union and established or ***legally*** represented in another Member State ***bound by this Regulation (‘the executing State’)***, to preserve electronic ***information*** 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 ***and, where it concerns personal data, acts as a data controller within the meaning of Regulation (EU) 2016/679:***

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

(b) 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[1] for which the storage of data is a defining component of the service provided to the user ▌;

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

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

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

(b) having a substantial connection 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) '***main*** establishment' means***, as regards a service provider with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of data are taken in another establishment of the service provider in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment***;

(6) 'electronic ***information***' means ***subscriber data, traffic data, or content data lawfully*** stored by a service provider at the time of the ***issuing*** of a ***European P***roduction or ***P***reservation order, ***that is requested for the purpose of serving as evidence during the investigation, prosecution and court proceedings relating to a criminal offence in a Member State, in accordance with national law***;

(7) 'subscriber data' means any data***, collected in the normal course of business,*** pertaining to ***the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address identifying the subscriber or customer as well as the type of service provided and the duration of the contract with the service provider, which is strictly necessary for the sole purpose of identifying the user of the service;***

(8) '***traffic*** data' means data ***collected in the normal course of business*** related to ▌***:***

(a)the type of service provided and its duration where it concerns technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of the service,

[1] 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).

excluding passwords or other authentication means used instead of a password that are provided by a user, or created at the request of a user;

(b) the commencement and termination of a user access session to a service, such as the date and time of use, or the log-in to, and log-off from the service;

(c) electronic communications metadata as processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content, including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication;

(9) ▌

(10) 'content data' means ***the*** stored data in a digital format ***by the service provider*** 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[1];

(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 authority in the issuing State, competent in the case concerned, to issue the European Production Order or European Preservation Order;

(13) '***executing*** State' means the Member State in which the ***service provider*** is established ***or legally represented*** 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 and*** enforcement ***of the order in accordance with this Regulation***;

(14) '***executing*** authority' means the competent authority in the ***executing*** 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 and enforcement of the order in accordance with this Regulation; where provided by national law, the executing authority may be a court authority in the executing State***;

(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person.

Article 3
Scope

[1] 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).

1. This Regulation applies to ***Member States and*** service providers***, offering services in one or more Member States bound by this Regulation and established or legally represented in one of these Member States***.

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, both during the pre-trial and trial phase. The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.

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

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

Article 4
Issuing authority

1. A European Production Order for ***obtaining*** subscriber data and ***IP addresses for the sole purpose of determining the identity of specific persons with a direct link to the specific proceedings referred to in Article 3(2)*** 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*** and content data may be issued only by:

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

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

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

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

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

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

Article 5

Conditions for issuing an 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 person concerned. It*** may only be issued if ***it could have been ordered under*** the same ***conditions in a similar*** domestic ***case, where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border production of the data and where the requested information is relevant for the investigation***. ***It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in Article 3(2).***

3. ***A*** European Production Order ***for obtaining*** subscriber data or ***IP addresses for the sole purpose of determining the identity of specific persons with a direct link to the specific proceedings referred to in Article 3(2)*** may be issued for all criminal offences.

4. ***A*** European Production Order to produce ***traffic*** data or content data may only be issued ***for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years.***

4a. ***European Production Orders to produce traffic data or content data may also be issued for the following offences:***

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

– offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA ;

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

(b) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541;

(ba) for criminal offences as defined in Articles 3 to 7 of Directive 2011/93/EU .

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

(a) the issuing and, where applicable, the validating authority; ***for traffic and content data and where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) of the Treaty on European Union, information on the special procedure as referred to in Article 9 (2a) of this Regulation;***

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

(c) ***the individually identifiable persons, or*** where the sole purpose of the order is to identify a person, ***any other unique identifier such as user name or Login ID***;

(d) the requested data category (subscriber data, ***traffic*** data or content data);

(e) the time range requested to be produced***, tailored as narrowly as possible***;

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

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

(h) ▌

(i) the grounds for the necessity and proportionality of the measure***, taking due account of the impact of the measure on the fundamental rights of the specific persons whose data is sought and the seriousness of the offence***.

6. ▌

7. If the issuing authority has reasons to believe that data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed ***or under the law of the Member State where the person whose data is sought resides or is bound by an obligation of professional secrecy or lawyer-client privilege***, or its disclosure may impact fundamental interests of that Member State such as national security and defence, the issuing authority ***shall*** 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 ***in criminal matters***. ***Where*** the issuing authority finds that the requested data is protected by such immunities and privileges or its disclosure would impact fundamental interests of the other Member State, ***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.

2. It may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order***, taking into account the rights of the person concerned***. European Preservation Orders to preserve data may be issued for all criminal offences***, if it could have been ordered under the same conditions in a similar domestic case in the issuing State, where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border preservation of the data and where the requested information is relevant for that investigation***. ***It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in Article 3 (2)***.

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

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

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

(c) the ***individually identifiable persons*** whose data shall be preserved, ***or,*** where the sole purpose of the order is to identify a person, ***any other unique identifier such as user name or Login ID***;

(d) the data category to be preserved (subscriber data, ***traffic*** data or content data);

(e) the time range requested to be preserved***, tailored as narrowly as possible***;

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

(g) the grounds for the necessity and proportionality of the measure***, taking due account of the impact of the measure on the fundamental rights of the specific persons whose data is sought and the seriousness of the offence.***

3a. If the issuing authority has reasons to believe that data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, or its preservation may impact fundamental interests of that Member State such as national security and defence, the issuing authority shall seek clarification before issuing the European Preservation Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network in criminal matters. Where the issuing authority finds that the requested data is protected by such immunities and privileges or its preservation would impact fundamental interests of the other Member State, the issuing authority shall not issue the European Preservation Order.

Article 6a

Legal representative

1. Service providers, offering services in the Member States bound by this Regulation, but not established in the Union, shall designate one legal representative for receipt

of, compliance with and enforcement of European Production Orders and European Preservation Orders issued by the competent authorities of the Member States, for the purpose of gathering electronic information in criminal proceedings. The legal representative shall be established in one of the Member States (bound by this Regulation) where the service provider offers its services.

2. Service providers, offering services in the Member States bound by this Regulation, but established in a Member State not bound by this Regulation, shall designate one legal representative for receipt of, compliance with and enforcement of European Production Orders and European Preservation Orders issued by the competent authorities of the Member States, for the purpose of gathering electronic information in criminal proceedings. The legal representative shall be established in one of the Member States bound by this Regulation where the service provider offers its services.

3. Service providers which are part of a group shall be allowed to collectively designate one legal representative.

4. The legal representative shall be entrusted with the receipt, compliance and enforcement of those decisions and orders on behalf of the service provider concerned.

5. Upon designation of the legal representative, service providers shall notify in writing that Member State where their legal representative is established. The notification shall contain the designation and contact details of its legal representative as well as any changes thereof.

6. The notification shall specify the official language(s) of the Union, as referred to in Regulation 1/58, in which the legal representative can be addressed. This shall include, at least, one of the languages accepted by the Member State where the legal representative is established.

7. Information, notified to Member States in accordance with this Article, shall be made available on a dedicated internet page of the European Judicial Network in criminal matters. Such information shall be regularly updated.

8. Member States shall ensure that the designated legal representative can be held liable for non-compliance with obligations under this Regulation when receiving decisions and orders, without prejudice to the liability and legal actions that could be initiated against the service provider.

9. Member States shall lay down rules on sanctions applicable to infringements pursuant to this Article and shall take all measures necessary to ensure that they are implemented. The sanctions provided for shall be effective, proportionate and dissuasive.

Article 7

Addressees of a European Production Order and a European Preservation Order

1. ***For the purpose of gathering electronic information in criminal proceedings, t***he European Production Order and the European Preservation Order shall be addressed directly ***and simultaneously:***

(a) to the main establishment of the service provider***, or, where applicable, its legal representative in the executing State*** designated by the service provider for the purpose of gathering evidence in criminal proceedings***; and***

(b) to the executing authority.

1a. Member States shall ensure that any service provider established on their territory notifies that Member State in writing of where its main establishment is. The notification shall contain the contact details, as well as any changes thereof.

1b. Information, notified to Member States in accordance with paragraph 1a, shall be made available on a dedicated internet page of the European Judicial Network in criminal matters. Such information shall be regularly updated.

2. ▌

3. ▌

4. ▌

Article 7a

Common European exchange system

1. By ... [date of application of this Regulation], the Commission shall establish a common European exchange system with secure channels for the handling of authorised cross-border communication, authentication and transmission of the Orders and of the requested data between the competent authorities and service providers. The competent authorities and service providers shall use this system for the purpose of this Regulation.

2. The Commission shall ensure that the system guarantees an effective, reliable and smooth exchange of the relevant information and a high level of security, confidentiality and integrity as well as the necessary protection of privacy and personal data in line with Regulation (EU) 2018/1725, Regulation (EU) 2016/679, Directive (EU) 2016/680, and Directive (EC) 2002/58. To this end, open and commonly used state-of-the-art electronic signature and encryption technology shall be applied.

3. Where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, it shall be possible to interconnect such systems or channels with this common European exchange system.

Article 8

European Production and Preservation Order Certificate

1. A European Production or Preservation Order shall be transmitted to the addressee**s** as defined in Article 7 ***via the system as defined in Article 7a*** through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).

   The issuing or validating authority shall complete the EPOC set out in Annex I or the EPOC-PR set out in Annex II, shall sign it and shall certify its content as being accurate and correct.

2. The EPOC or the EPOC-PR shall be directly transmitted ***via the system as defined in Article 7a, allowing the addressees to produce*** a written record allowing the addressee***s*** to establish ***the*** authenticity ***of the Order and of the issuing authority***.

3. The EPOC shall contain ***all*** the information listed in Article 5(5) (a) to (***i***), including sufficient information to allow the addressee***s*** to identify and contact the issuing authority***, and information regarding the means and technical interfaces it has at its disposal to receive the produced data, or where to find this information***.

4. The EPOC-PR shall contain ***all*** the information listed in Article 6(3) (a) to (***g***), including sufficient information to allow the addressee***s*** to identify and contact the issuing authority.

5. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the ***executing State or in any other*** language ***explicitly accepted by the executing*** State ***in accordance with paragraph 5a***.

Article 8a

Execution of an EPOC for subscriber data and IP addresses

for the sole purpose of identifying a person

1. An EPOC for subscriber data and IP addresses, for the sole purpose of identifying a person, shall be addressed directly and simultaneously:

(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and

(b) to the executing authority.

The simultaneous information of the executing authority shall not have a suspensive effect on the obligations of the service provider as referred to in paragraph 1.

2. Upon receipt of the EPOC for subscriber data and IP addresses, for the sole purpose of identifying a person, the service provider shall ensure that the requested data is transmitted directly to the issuing authority, or the law enforcement authorities as indicated in the EPOC, as soon as possible and at the latest within 10 days upon

receipt of the EPOC. When transmitting the requested data, the service provider shall simultaneously send a copy of the data transferred for information to the executing authority.

3. In emergency cases, the service provider shall transmit the requested data without undue delay, at the latest within 16 hours upon receipt of the EPOC. When transmitting the requested data, the service provider shall simultaneously make the data available to the executing authority for information.

4. Where the executing authority decides to invoke any of the grounds listed in Article 10a (1), it shall act as soon as possible and at the latest within the time periods as referred to in paragraphs 1 or 2, and immediately inform the issuing authority and the service provider of its decision. The issuing authority shall erase the data. Where the requested data has not yet been transmitted to the issuing authority, the addressed service provider shall not transmit the data.

5. Where the EPOC is incomplete, contains manifest errors, in form or content, or does not contain sufficient information to execute the EPOC, the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC without undue delay and ask for clarification or, where necessary, correction from the issuing authority, using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.

6. Where the service provider cannot comply with its obligations because of force majeure or of de facto impossibility due to circumstances not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. Where the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC and inform the addressees of its decision.

7. In all cases where the service provider does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons, including for technical or operational ones, it shall inform the issuing authority as well as the executing authority referred to in the EPOC without undue delay and at the latest within the deadlines set out in paragraphs 1 and 2 of the reasons for this using the Form in Annex III. The issuing authority shall review the order in light of the information provided by the service provider and if necessary, set a new deadline for the addressees.In case the service provider considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it is manifestly abusive or that it exceeds the purpose of the order, the service provider shall also send the Form in Annex III to the issuing authority as well as to the

executing authority referred to in the EPOC with a suspensive affect as regards the transmission of the requested data. In such cases the executing authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network in criminal matters. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.

8. Where the service provider does not produce the data requested immediately, in accordance with paragraphs 3, 4, and 5, it shall preserve the data requested, where possible. The preservation shall be upheld until the data is produced or until the EPOC is withdrawn or null and void.

Article 9

Execution of an EPOC ***for traffic or content data***

- 1a. An EPOC for traffic or content data shall be addressed directly and simultaneously:

(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and

(b) to the executing authority.1. Upon receipt of the EPOC ***for traffic and content data, the service provider shall act expeditiously to preserve the data***.

1a. Where the executing authority decides to refuse the EPOC, based on one of the grounds provided for in Article 10a, it shall act as soon as possible and at the latest within 10 days upon receipt of the EPOC and inform the issuing authority and the service provider of such decision immediately. 2. In emergency cases***, where the executing authority decides to refuse the EPOC based on one of the grounds provided for in Article 10a , it shall act as soon as possible and at the latest*** within ***16*** hours upon receipt of the EPOC ***and inform the issuing authority and the service provider of such decision immediately***.

2a. Where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) of the Treaty on European Union, the service provider shall transmit the requested data only after receiving the explicit written approval of the executing authority. For this, the executing authority shall assess the order of the issuing authority with due diligence and check in particular for grounds for non-recognition or non-execution pursuant to Article 10a , before giving its written approval within the deadlines set out in paragraph 1a and 2.

2b. Without prejudice to paragraph 2a, where the executing authority has not invoked any of the grounds listed in Article 10a within the time periods referred to in paragraphs 1a and 2, the service provider to which the order is addressed shall ensure that the requested data is immediately transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC.

2c. ***Where it is not possible in a specific case for the executing authority to meet the time limit set out in paragraph 1 or 2, it shall, without undue delay, inform the issuing authority and the service provider by any means, giving the reasons for the delay and the estimated time necessary for the decision to be taken.***

3. ***Where*** the EPOC is incomplete, contains manifest errors***, in form or content,*** or does not contain sufficient information to execute the EPOC, the ***service provider*** shall inform the issuing authority ***as well as the executing authority*** referred to in the EPOC without undue delay and ask for clarification ***or, where necessary, correction from the issuing authority***, using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1***a*** and 2 shall not apply until the clarification is provided. ***In the absence of a reaction from the issuing authority, the order shall be considered null and void.***

4. ***Where*** the ***service provider*** cannot comply with its obligation***s*** because of *force majeure* or of de facto impossibility ***due to circumstances*** not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the ***service provider*** shall inform the issuing authority ***as well as the executing authority*** referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. ***Where*** the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC ***and inform the addressees of its decision***.

5. In all cases where the ***service provider*** does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons, ***including for technical or operational ones,*** it shall inform the issuing authority ***as well as the executing authority referred to in the EPOC*** without undue delay and at the latest within the deadlines set out in paragraphs 1***a*** 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 service provider and if necessary, set a new deadline for the ***addressees***.

   In case the ***service provider*** considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it is manifestly abusive ***or that it exceeds the purpose of the order***, the ***service provider*** shall also send the Form in Annex III ***to the issuing authority as well as*** to the ***executing*** authority ***referred to in the EPOC with a suspensive affect as regards the transmission of the requested data***. In such cases the competent ***executing*** authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network ***in criminal matters***. ***The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1a and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.***

6. ***During the procedure referred to in paragraphs 1, 1a, 2, 2b, 2c, 3, 4, and 5, the service provider*** shall preserve the data requested***, where possible***. The preservation shall be upheld until the data is produced ***or until the EPOC is withdrawn or null and void***.

Article 10
Execution of an EPOC-PR

- 1a. An EPOC-PR shall be addressed directly and simultaneously:

(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and

(b) to the executing authority.

The simultaneous information of the executing authority shall not have a suspensive effect on the obligations of the service provider as referred to in paragraph 1.

1. Upon receipt of the EPOC-PR, the ***service provider*** shall ***act expeditiously to*** preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been launched. ***The EPOC-PR can be extended by additional 30 days, only when necessary to allow further assessment of the relevance of the data***.

2. ***Where*** the issuing authority ***submits the subsequent European Production Order*** within ***the deadline referred to in paragraph 1, the service provider*** shall preserve the data as long as necessary ***for the execution of that European P***roduction ***Order pursuant to Articles 8a or 9***.

3. ***Where*** the preservation is no longer necessary, the issuing authority shall inform the addressee***s*** without undue delay ***and the preservation shall cease immediately***.

4. ***Where the EPOC-PR*** is incomplete, contains manifest errors***, in form or content,*** or does not contain sufficient information to execute the EPOC-PR, the ***service provider*** shall inform the issuing authority ***as well as the executing authority referred to*** in the EPOC-PR without undue delay and ask for clarification ***or, where necessary, correction from the issuing authority,*** using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The addressee***s*** shall ensure that the needed clarification can be received in order***, for the service provider,*** to fulfil its obligation***s*** set out in paragraph***s*** 1***, 2 and 3***. ***In the absence of a reaction from the issuing authority, the order shall be considered null and void***.

5. ***Where*** the ***service provider*** cannot comply with its obligation***s*** because of *force majeure,* or of de facto impossibility ***due to circumstances*** not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the ***EPOC-PR***, ***the service provider*** shall contact the issuing authority ***as well as the executing authority referred to*** in the EPOC-PR without undue delay explaining the reasons, using the Form set out in

Annex III. ***Where*** the ***relevant*** conditions are fulfilled, the issuing authority shall withdraw the EPOC-PR ***and inform the addressees of its decision***.

6. In all cases where the ***service provider*** does not preserve the requested information, for other reasons listed in the Form of Annex III, ***including for technical or operational ones,*** the ***service provider*** shall inform the issuing authority ***as well as the executing authority referred to in the EPOC-PR*** without undue delay of the reasons for this in the Form set out in Annex III. The issuing authority shall review the Order in light of the justification provided by the service provider.

In case the service provider considers that the EPOC-PR cannot be executed because based on the sole information contained in the EPOC-PR it is apparent that it is manifestly abusive or that it exceeds the purpose of the order, the service provider shall also send the Form in Annex III to the issuing authority as well as to the executing authority referred to in the EPOC-PR. In such cases the competent executing authority may seek clarifications from the issuing authority on the European Preservation Order, either directly or via Eurojust or the European Judicial Network in criminal matters. The issuing authority shall react expeditiously and within 5 days at the latest. The deadline set out in paragraph 1 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.

Article 10a
Grounds for non-recognition or non-execution

1. Without prejudice to Article 1(2), where the EPOC is assessed by the executing authority, the EPOC shall be refused, where:

(a) the conditions for issuing a European Production Order as laid down in Article 5 of this Regulation are not fulfilled;

(b) the execution of the European Production Order would be contrary to the principle of ne bis in idem;

(c) there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter; or

(d) there is an immunity, a privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the executing State, which makes it impossible to execute the European Production Order.

2. In addition to paragraph 1, an EPOC for traffic and content data may be refused by the executing authority, where:

(a) the execution of the European Production Order would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities;

(b) the European Production Order relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct for which the EPOC was issued does not constitute a criminal offence under the law of the executing State;(c) the conduct for which the EPOC has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex IIIa, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years;

(d) the execution of the European Production Order is restricted under the law of the executing State to a list or category of offences or to offences punishable by a higher threshold; or

(e) compliance with the European Production Order would conflict with applicable laws of a third country that prohibits disclosure of the data concerned.

3. Point (e) of paragraph 2 shall be applied according to the procedure set out in Article 14a.

4. Where the European Production Order concerns an offence in connection with taxes or duties, customs and exchange, the executing authority shall not refuse recognition or execution on the ground that the law of the executing State does not impose the same kind of tax or duty or does not contain a tax, duty, customs and exchange regulation of the same kind as the law of the issuing State.

5. In the cases referred to in paragraphs 1 and 2 of this Article, before deciding not to recognise or not to execute a European Production Order, either in whole or in part, the executing authority shall consult the issuing authority, by any appropriate means, and shall, where appropriate, request the issuing authority to supply any necessary information without delay.

6. In the case referred to in point (d) of paragraph 1 and where power to waive the privilege or immunity lies with an authority of the executing State, the executing authority shall request it to exercise that power forthwith. Where power to waive the privilege or immunity lies with an authority of another State or international

organisation, it shall be for the issuing authority to request the authority concerned to exercise that power.

7. The executing authority shall inform the issuing authority about the use of any of the grounds for non-recognition or non-execution as listed in paragraphs 1 and 2 of this Article, by using the form set out in Annex III.

Article 11
User information ***and confidentiality***

1. ***The service provider shall inform the person whose data is being sought without undue delay. The service provider*** 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.

1a. As long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings or in order to protect the fundamental rights of another person, the issuing authority, taking into due account the impact of the measure on the fundamental rights of the person whose data is sought, may request the service provider to refrain from informing the person whose data is being sought, based on a judicial order. Such an order shall be duly justified, specify the duration of the obligation of confidentiality and shall be subject to periodic review.

2. Where the issuing authority requested the addressee**s** to refrain from informing the person whose data is being sought***, based on a judicial order***, the issuing authority shall inform the person whose data is being sought by the EPOC ***or the EPOC-PR*** without undue delay about the data production ***or preservation***. This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings***, taking into account the rights of the suspected and accused person and without prejudice to defence rights and effective legal remedies.***

3. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.

Article 11a
Limitations to the use of information obtained

Electronic information obtained in accordance with this Regulation shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except for where there is an imminent threat to the life or physical integrity of a person.

Article 11b
Erasure of electronic information

1. Electronic information that has been gathered in breach of this Regulation shall be erased without undue delay.

2. Electronic information that is no longer necessary for all phases of the proceeding for which it was produced or preserved, including possible appeals, shall be erased without undue delay, unless this would affect the defence rights of the suspected or accused person. Periodic reviews for the need of the storage of the electronic information shall be established.

3. The person whose data was sought shall be informed about the erasure without undue delay.

Article 11c

Admissibility of electronic information in court proceedings

Electronic information that has been obtained in breach of this Regulation, including where the criteria laid down in this Regulation are not fulfilled, shall not be admissible before a court. Where electronic information has been obtained before a ground for non-recognition listed in Article 10a (new) has been invoked, it neither shall be admissible before a court.

Article 12

Reimbursement of costs

Where so claimed by the service provider, the issuing State shall reimburse the justified costs borne by the service provider ***and related to the execution of the European Production Order or the European Preservation Order. For practical reasons, t***he service provider may claim reimbursement of the costs ***from*** the ***executing*** State***. Where the service provider chooses the executing State, the issuing State shall reimburse the executing State for these costs***. ***Member States shall inform the Commission on the rules for reimbursement, which the Commission shall make public.***

Chapter 3: Sanctions, ***review procedure and remedies***

Article 13

Sanctions

1. Member States shall lay down the rules on sanctions applicable to infringements of the obligations pursuant to Articles ***8a,*** 9, 10 and 11 of this Regulation ***as regards to the service providers on their territory*** and shall take all necessary measures to ensure that they are implemented. The sanctions provided for ***by national laws of the Member States*** shall be effective, proportionate and dissuasive. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

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

Article 14

Procedure for enforcement

1. ***Where*** the ***service provider*** does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons ***and where the executing authority has not invoked any of the grounds for non-recognition or non-execution as provided for in Article 10a***, the issuing authority may ***request*** the competent authority in the ***executing*** State ***to enforce*** the European Production Order or the European Preservation Order [redacted].

2. [redacted]

3. [redacted] The ***executing*** authority it shall formally require the ***service provider*** to comply with the relevant obligation, informing the ***service provider*** of the possibility to oppose the ***execution*** by invoking the grounds listed in ***Articles 8a, 9 and 10***, as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.

4. [redacted]

5. [redacted]

6. In case of an objection by the ***service provider***, the ***executing*** authority shall decide whether to enforce ***or not to recognise*** the Order on the basis of the information provided by the ***service provider*** and, if necessary, supplementary information obtained from the issuing authority. ***The executing authority shall notify its decision without undue delay to the service and the issuing authority.***

7. [redacted]
8. [redacted]

9. If the ***executing*** authority obtains the data from the ***service provider***, it shall transmit it to the issuing authority ***without undue delay.***

10. In case the ***service provider*** does not comply with its obligations, ***the executing*** authority shall impose a sanction in accordance with ***Article 13***. An effective judicial remedy shall be available against the decision to impose a fine.

Article 14 a

Review procedure in case of conflicting obligations with third country law

1. ***Where the service provider or the executing authority considers that compliance with the European Production Order or the European Preservation Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned, it shall inform the issuing authority and the relevant addressees without undue delay***

and at the latest within 10 days from the receipt of the order. In this case, execution of an order shall be suspended.

2. Such notice shall 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.

3. The competent authority of the issuing State shall review the European Production Order or the European Preservation Order and inform the addressees, within 10 days after receiving the notice, on the basis of the following criteria:

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

b. the degree of connection of the criminal case for which the Order was issued to the jurisdiction of the issuing State and the third country, as indicated inter alia by:

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

ii. 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;

d. the interests of the issuing State in obtaining the electronic information concerned, based on the seriousness of the offence and the importance of obtaining the electronic information in an expeditious manner;

e. the possible consequences for the addressees of complying with the European Production Order or the European Preservation Order, including the sanctions that may be imposed against the service providers under the law of the third country.

4. Within 10 days after receiving the notice, the issuing authority shall withdraw, uphold or adapt the Order where necessary, to give effect to these criteria. To this end, the issuing authority shall request clarifications on the applicable law from the competent authority of the third country, in compliance with Directive (EU) 2016/680, to the extent that this does not obstruct the deadlines provided for in this Regulation. In the event of withdrawal, the issuing authority shall immediately inform the addressees of the withdrawal.

5. Where the issuing authority decides to uphold the Order, it shall inform the addressees of its decision. While duly taking into account the decision of the issuing authority and after also consulting the competent authority of the third country, in compliance with Directive (EU) 2016/680, to the extent that this does not obstruct the deadlines provided for in this Regulation, the executing authority shall take a final decision based on the criteria listed in paragraph 3, within 10 days after receiving the

decision of the issuing authority, and inform the issuing authority, the service provider and the competent authority of the third country about its final decision.

6. For the duration of the procedure referred to in Article 14a , the service provider shall preserve the data requested.

Article 15

▌

Article 16

▌

Article 17

Effective remedies

1. ***Persons*** whose data was ***sought*** via a European Production Order ***or a European Preservation Order*** shall have the right to effective remedies against ***such Orders***, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

2. ▌

3. Such right to an effective remedy shall ***be exercised before a court in the issuing State or the executing State in accordance with national law and shall*** include the possibility to challenge the legality of the measure, including its necessity and proportionality.

3a. The substantive reasons for issuing the European Production Order or the European Preservation Order shall be challenged in the issuing State, without prejudice to the guarantees of fundamental rights in the executing State.

4. Without prejudice to Article 11, the issuing authority ***and the executing authority*** shall take the appropriate measures to ensure that information is provided ***in due time*** about the possibilities under national law for seeking ***legal*** remedies***, including about when such remedies apply,*** and ensure that they can be exercised effectively***.***

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

6. ▌

Article 18

▌

Chapter 5: Final provisions

Article 19

Monitoring and reporting

1. By**...** *[date of application of this Regulation]* at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the means by which and the intervals at which the data and other necessary ***information*** will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data and other ***information***.

2. In any event, 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, including details on circumstances and possible outcomes;

ab) the number of EPOCs and EPOC-PRs issued making use of the possibility of the issuing authority to request the service provider to refrain from informing the person whose data is being sought pursuant to Article 11(1a), including information of the circumstances and possible later information pursuant to Article 11(2);

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 EPOCs that were refused, by the type of data requested, the addressees, the situation (emergency case or not) and the ground for non-recognition or non-execution 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 EPOC procedure following the EPOC-PR, from the moment the EPOC-PR is issued to the moment the EPOC is issued, by the type of data requested and the addressees;

d) ▌;

e) the number of legal remedies ***used*** against European Production Orders ***and European Preservation Orders*** in the issuing State and in the ***executing*** State by ***the*** type of data requested***;***

f) the sanctions imposed, in accordance with Article 13, by the type of data requested, the addressees, the situation (emergency case or not) and the amount of sanctions.

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.

h) the number of enforcement procedures launched by the type of data requested, the addressees, the situation (emergency case or not) and the final outcome.

2a. The Commission shall, by 30 June of each year, publish a report containing the data referred to in paragraph 2 in a compiled form subdivided into Member States.

Article 20

▌

Article 21

▌

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 to Article 4 to issue and/or validate European Production Orders and European Preservation Orders;

(b) the ***executing*** authority ***to*** which ***the EPOC or EPOC-PR is transmitted for the execution or enforcement*** of European Production Orders and European Preservation Orders;

(ba) where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, the means and technical interfaces the competent authorities have at their disposal to receive or access data produced to be interconnected with the system referred to in Article 7a;

(c) ▌

1a. By the same date, service providers with establishments in more than one Member State shall notify the Commission of the place of their main establishment in the Union.

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[1].

Article 23

Relationship to European Investigation Orders ***and Mutual Legal Assistance Procedures***

The a*uthorities of the Member States** may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU, or to use the existing mutual legal assistance procedures*** for the gathering of ***electronic information,*** that would also fall within the scope of this Regulation.

Article 24

Evaluation

By ... *[**2** years from the date of application of this Regulation]* at the latest, the Commission shall carry out an evaluation of the Regulation and present a report to the European Parliament and to the Council on the functioning of this Regulation, which shall, ***in particular, evaluate the number of cases in which the emergency derogation, pursuant to Article 9 (2), and the derogation from the principle of user information, pursuant to Article 11, were applied.*** ▌The report shall be accompanied by ***an assessment of the functioning of the common European exchange system as well as an assessment of the functioning of the Regulation in relation with Directive 2014/41/EU of the European Parliament and of 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 25

Entry into force

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

It shall apply from [***18*** months after its entry into force].

---

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

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

Done at Strasbourg,

For the European Parliament	For the Council
The President	The President

ANNEX I

EUROPEAN PRODUCTION ORDER CERTIFICATE (EPOC) FOR THE PRODUCTION OF ELECTRONIC ***INFORMATION***

Under Regulation (EU)….[1] the addressee of the European Production Order Certificate (EPOC) must ***be addressed directly and simultaneously to the service provider and the executing*** ▌authority ***to execute*** ▌the EPOC. If the data is not produced, the addressee must, upon receipt of the EPOC, 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 ***addressees*** must take necessary measures to ensure the confidentiality of the EPOC and of the data produced or preserved.

SECTION A:
Issuing State: ……..
NB: details of issuing authority to be provided at the end (Sections E and F)
Addressees (***tick the appropriate box)***:
- servicer provider, or where applicable, its legal representative:
- executing authority

SECTION B: Deadlines
The data requested must be produced (tick the appropriate box and complete, if necessary):
□ within 10 days at the latest***, where the executing authority has not invoked any of the grounds for non-recognition or non-execution;***
□ within ***16 hours*** at the latest in the event of an emergency***, where the executing authority has not invoked any of the grounds for non-recognition or non-execution;***
- an imminent threat to ***the life of a person*** or physical integrity. Justification:
▌

SECTION C: ***Information to the user***
Please note that (tick, if applicable):
□ the ***service provider*** must refrain from informing the person whose data is being sought of the EPOC ***based on s judicial order. Justification:...***

SECTION D: Electronic ***information*** to be produced

(i) This EPOC concerns (tick the relevant box(es)):
□ subscriber data ▌:
□ name, address, date of birth, contact information (email address, phone number) and other relevant information pertaining to the identity of the user/subscription holder
□ date and time of first 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, including identifier (phone number, ▌SIM-card number, MAC address) and associated device(s)
□ profile information (user name, profile photo)

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

▌

□ PUK-codes

□ ***IP address, for the sole purpose of identifying the user:***

- IP address

-IP connection records / logs for identification purposes

□ traffic data ▌:

(a) for (mobile) telephony:

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

□ time and duration of connections

□ call attempts

□ 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)

(b) for internet:

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

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

□ volume of data

(c) for hosting:

□ logfiles

□ tickets

□ purchase history

- prepaid balance charging history

▌

□ content data ▌:

- contact lists

□ (web)mailbox dump

□ online storage dump (user generated data)

□ pagedump

□ message log/backup

□ voicemail dump

□ server contents

□ device backup

(ii) ***Additional information in order to execute*** the EPOC:

IP address:……..
Telephone number:…….
Email address:……...
IMEI number:…….
MAC address:…….
Person(s) whose data is being requested:…….……..
Name of the service: ……..
Other: …….

(iii) ***The*** time range requested to be produced:

……..…….

(iv) Please note that (tick and complete if applicable):
□ the requested data was preserved in accordance with an earlier request for preservation issued by……..……..…… (indicate the authority, and, if available, the date of transmission of request and reference number) and transmitted to ……..…… (indicate the ***addresses*** to which it was transmitted and, if available, the reference number given by the addressee)

(v) Nature and legal classification of the offence(s) in relation to which the EPOC is issued and the applicable statutory provision/code:
……..…….……
The current EPOC is issued for ***traffic*** 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;
the following offence(s), if wholly or partly committed by means of an information system:
offence(s) as defined in Articles 3, 4 and 5 of Council Framework Decision 2001/413/JHA;
offence(s) as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council;
offence(s) as defined in Articles 3 to 8 of Directive 2013/40/EU of the European Parliament and of the Council;
offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council.

(vi) Please note that (tick, if applicable):
The data sought is stored or processed as part of a corporate infrastructure provided by a service provider to a company or another entity other than natural persons, and the current EPOC is addressed to the service provider because investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.

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

SECTION E: Details of the authority which issued the EPOC
The type of authority which issued this EPOC (tick the relevant box):
□ judge, court, or investigating judge
□ public prosecutor (for subscriber and ***IP addresses for the sole purpose of determining the identity of specific persons***)
□ public prosecutor (for ***traffic*** and content data) → please complete also Section (F)
□ any other competent authority as defined by the issuing State → please complete also Section (F)
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 No:…..……..……..
Address:……..……..
Tel. No: (country code) (area/city code)……..…….

Fax No: (country code) (area/city code)……..……....
Email:……..…….
Date: ……..……
…
Official stamp (if available) and signature:……...……

SECTION F: Details of the authority which validated the EPOC
The type of authority which has validated this EPOC (tick the relevant box, if applicable):
□ judge, court or investigating judge
□ public prosecutor (for subscriber ***data*** and ***IP addresses for the sole purpose of determining the identity of specific persons***)
Details of the validating 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 No:…….……..…….
Address: ……...……..……..
Tel. No: (country code) (area/city code)…….……..……....
Fax No: (country code) (area/city code)…….……..
Email:…….…….
Date: …….…….
Official stamp (if available) and signature:……..……

SECTION G: Transfer of data and contact details
(i) Authority to whom the data has to be transferred (tick and complete, if neccessary):
□ issuing authority,
□ validating authority
□ other competent authority as defined by the issuing State:.....
(ii) Authority/contact point which can be contacted for any question related to the execution of the EPOC:…….……

ANNEX II

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

Under Regulation (EU) ... [2] the addressee of the European Preservation Order Certificate (EPOC-PR) must ***be addressed directly and simultaneously to the service provider (or, where applicable, its legal representative) and the executing authority to execute*** the EPOC-PR. ▌ The preservation will cease after 60 days, unless the issuing authority confirms that a subsequent request for production has been launched. If the issuing authority confirms within those 60 days that a subsequent request for production has been launched, the addressee must preserve the data for as long as necessary to produce the data once the subsequent request for production is served.
The ***addressees*** must take necessary measures to ensure the confidentiality of the EPOC-PR and of the data preserved or produced.

SECTION A:
Issuing State: ……
NB: details of issuing authority to be provided at the end (Sections D and E)
Addressees (tick the appropriate box and complete):
- service provider, or where applicable, its legal representative: ...
- executing authority: ...

SECTION B: ***Information to the user***
Please note that (tick, if applicable):
□ the ***service provider*** must refrain from informing the person whose data is being sought of the EPOC-PR ***based on a judicial order. Justification:...***

SECTION C: ***Electronic information*** to be preserved
(i) The EPOC-PR concerns (tick the relevant box(es)):
subscriber data ▌:
□ name, address, date of birth, contact information (email address, phone number) and other relevant information pertaining to the identity of the user/subscription holder
□ date and time of first 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, including identifier (phone number, ▌SIM-card number, MAC-address) and associated device(s)
□ profile information (user name, profile photo)
□ data on the validation of the use of service, such as an alternative email address provided by the user/subscription holder
▌
□ PUK-codes
IP addresses, for the sole purpose of identifying the user:
- ***IP address***
- IP connection records / logs for identification purposes

▌
□ traffic data ▌:
(a) for (mobile) telephony:

□ outgoing (A) and incoming (B) identifiers (phone number, IMSI, IMEI)
□ time and duration of connections
□ call attempts
□ 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)
(b) for internet:
□ routing information (source IP address, destination IP address(es), port number(s), browser, ▌ message-ID)
□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection
□ volume of data
(c) for hosting:
□ logfiles
□ tickets
□ purchase history
□ other ***traffic*** data ▌:
□ prepaid balance charging history
▌content data ▌:
- contact list
□ (web)mailbox dump
□ online storage dump (user generated data)
□ pagedump
□ message log/backup
□ voicemail dump
□ server contents
□ device backup

(ii) ***Additional information in order to execute*** the EPOC-PR:
IP address:……..…..……..
Telephone number:…….……..
Email address:…….…….
IMEI number:…….……
MAC address:…….
Person(s) whose data is being requested:…….
Name of the service: ……..
Other: …….……

(iii) ***The*** time range requested to be preserved:
……..…….

(iv) Nature and legal classification of the offence(s) for which the EPOC-PR is issued and the applicable statutory provision/code:
……..…….……

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

SECTION D: Details of the authority which issued the EPOC-PR

The type of authority which issued this EPOC-PR (tick the relevant box):
□ judge, court, or investigating judge
□ public prosecutor
□ any other competent authority as defined by the law of the issuing State → please complete also Section (E)
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 No:.…….……..
Address:.…….……..
Tel. No: (country code) (area/city code)…….…….
Fax No: (country code) (area/city code)…….…….....
Email:…….…….
Date: ……
…
Official stamp (if available) and signature:……...……

SECTION E: Details of the authority which validated the EPOC-PR
The type of authority which has validated this EPOC-PR (tick the relevant box):
□ 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 No:……..……..
Address: ……..
Tel. No: (country code) (area/city code)……...
Fax No: (country code) (area/city code)……..……
Email:……..……
Date: ……..
Official stamp (if available) and signature:……...……

SECTION F: Contact details
The authority which can be contacted for any question related to the execution of the EPOC-PR:
……

ANNEX III

INFORMATION ON THE IMPOSSIBILITY TO EXECUTE THE EPOC / EPOC-PR ***OR NON-RECOGNITION OF THE EPOC***

SECTION A:
The following information concerns:
□ the European Production Order (EPOC)
□ the European Preservation Order (EPOC-PR)

SECTION B:
Addressees of the EPOC / EPOC-PR:
- service provider, or where applicable, its legal representative: ...
- executing authority: ...
Authority which issued the EPOC / EPOC-PR: ……..……
If applicable, authority which validated the EPOC / EPOC-PR: …….

SECTION C:
File reference of the addressee of the EPOC / EPOC-PR: ……..…….
File reference of the issuing authority: ……
If applicable, file reference of the validating authority:…….…….
Date of transmission of the EPOC / EPOC-PR: ……...……

SECTION D: Reasons for ***impossibility of executing the EPOC/EPOC-PR***

(i) The EPOC / EPOC-PR cannot be executed or cannot be executed within the requested deadline for the following reason(s):
□ the EPOC / EPOC-PR is incomplete
□ the EPOC / EPOC-PR contains manifest errors***, in form or content,***
□ the EPOC / EPOC-PR does not contain sufficient information
□ force majeure or de facto impossibility ***due to the circumstances*** not attributable to the addressee or the service provider
□ the European Production Order has not been issued or validated by an issuing authority as specified in Article 4 of Regulation (EU) …
□ the 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 has not been issued for an offence provided for by Article 5(4) of Regulation (EU)…
□ the service ***provider*** is not covered by the scope of the Regulation (EU)....
□ the European Production Order / the European Preservation Order does not concern data stored by or on behalf of the service provider at the time of ***issuing*** of the EPOC / EPOC-PR
□ based on the sole information contained in the EPOC / EPOC-PR, it is apparent that the EPOC / EPOC-PR manifestly ***abusive or that it exceeds the purpose of the order***
□ compliance with the European Production Order ***or the European Preservation Order*** would conflict with the applicable law(s) of a third country prohibiting disclosure of the data concerned.

(ii) Please explain further the reasons for non-execution in this case, including, where necessary, an indication of other reasons not listed under point (i) of this Section:

…….

SECTION Da:

Grounds for non-recognition or non-execution of the EPOC (tick the appropriate box):

For all EPOC:

[ ] the conditions for issuing a European Production Order as laid down in Article 5 of this Regulation are not fulfilled;

[ ] the execution of the European Production Order would be contrary to the principle of ne bis in idem;

[ ] there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter;

[ ] there is an immunity, a privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the executing State, which makes it impossible to execute the European Production Order;

For EPOC for traffic and content data:

[ ] the execution of the European Production Order would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities;

[ ] the European Production Order relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct for which the EPOC was issued does not constitute a criminal offence under the law of the executing State;

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

[ ] the execution of the European Production Order is restricted under the law of the executing State to a list or category of offences or to offences punishable by a higher threshold;

[ ] compliance with the European Production Order would conflict with applicable laws of a third country that prohibits disclosure of the data concerned.

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, including the relevant provision(s):
……
- 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 defence (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:
……...

SECTION F: Information that is requested
Further information is required from the issuing authority for the EPOC/ EPOC-PR to be executed (complete, if applicable):
……..

SECTION G: Preservation of data
The requested data (tick the relevant box and complete, if applicable):
□ will be preserved ***for 5 days for clarification, or, where necessary, correction by*** the issuing authority ▌
□ will not be ***produced or*** preserved since the information provided in the EPOC / EPOC-PR does not allow to identify it.
- will not be produced since one of the grounds for non-recognition or non-execution exists.

SECTION H: Details of the service provider ***or, where applicable,*** its legal representative
Name of the service provider/ legal representative:……
Name of the authorised person:……
Official stamp (if available) and signature:……..

ANNEX IIIa

The categories of offences referred to in Article 10a (2) (c):

- ***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 that affecting the financial interests of the European Union within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,***
- ***laundering of the proceeds of crime,***
- ***counterfeiting currency, including of 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, grievous bodily injury,***
- ***illicit trade in human organs and tissue,***
- ***kidnapping, illegal restraint and 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/ships,***
- ***sabotage.***