Council of the European Union

Brussels, 26 November 2018
(OR. en)

Interinstitutional File: 2018/0108(COD)

14351/1/18 REV 1

LIMITE

JAI 1145
COPEN 397
CYBER 281
ENFOPOL 563
DROIPEN 184
JAIEX 157
DAPIX 358
EJUSTICE 159
MI 880
TELECOM 428
DATAPROTECT 255
CODEC 2085

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	12113/5/18 REV5
No. Cion doc.:	8110/18
Subject:	Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach

INTRODUCTION

1. On 17 April 2018, the Commission adopted and transmitted to the Council and to the European Parliament the above-mentioned proposal with Article 82(1) TFEU as a legal basis. It aims to create European 'Production' and 'Preservation' Orders to obtain or preserve e-evidence in another jurisdiction without the involvement of the competent authorities of that jurisdiction. The orders target specifically the cross-border access to e-evidence, seeking to adapt judicial cooperation mechanisms to the requirements of fighting crime in the digital age.

2. The proposed Regulation establishes the possibility to request any category of stored data. However, it sets a specific threshold for traffic and content data [as opposed to subscriber and access data] which can be requested only for crimes punishable in the issuing State by a maximum custodial sentence of at least three years or for specific cyber-dependent, cyber-enabled or terrorism-related crimes.

3. The proposal envisages ten days as a mandatory deadline for the execution of the European Production Order, but in emergency situations (imminent threat to life or physical integrity of a person or critical infrastructure) the deadline is six hours. For the European Preservation Order the competent authority has 60 days to confirm that it has launched a subsequent request for the data production (including through MLA). In case of non-compliance with an Order, sanctions can be imposed on the service provider.

4. The Orders are to be addressed to a service provider offering services in the Union or to a legal representative designated by the service provider, located in another Member State, for the purpose of gathering e-evidence in accordance with the proposed Directive. The draft Regulation uses as criteria the type of the services provided (e-communications, information society, hosting, IP numbering, privacy or proxy services), but also names certain types of service providers (internet domain name registries or registrars).

5. On 18 October 2018, the European Council[1] called for a solution to be found to ensure swift and efficient cross-border access to e-evidence in order to effectively fight terrorism and other serious and organised crime, both within the EU and at international level. It stressed that the Commission proposals on e-evidence should be agreed on by the end of the current legislature.

6. In the European Parliament, Ms Birgit Sippel (LIBE, S&D) was appointed as rapporteur on 24 May 2018. The LIBE Committee discussed the proposal on 11 June 2018 and has held several meetings and hearings, including a public hearing on 27 November 2018. No timeline has been set for the adoption of the report.

7. The European Economic and Social Committee adopted its opinion on 12 July 2018[2].

[1] EUCO 13/18, paragraph 9.
[2] 11533/18.

II. WORK WITHIN THE COUNCIL

8. The Commission presented this proposal to the COPEN Working Party on 27 April 2018, followed by an article-by-article examination of the draft regulation and an exchange of views on the impact assessment in the Working Party on 5-6 May 2018. In general, both the impact assessment and the proposal were positively received by delegations.

9. Discussions were centered mainly around the concept proposed by the Commision to serve a European Production Order directly on the service provider or its legal representative without the involvement of the Member State where the latter are located (i.e. the enforcing State), the definition of the service provider, the immunities and privileges, the review procedure in case of conflicing obligations, as well as the sanctions for non-compliance with the obligations under the regulation.

10. The examination of the proposal by the Working Party were conducted under the Bulgarian and Austrian Presidency. Twelve meetings were held which resulted in five consecutive revised versions. Discussions were concluded on 20 November 2018 with a view to submitting of the compromise text set out in Annex to this note for adoption as a general approach on the proposal at the forthcoming JHA Council to be held on 6 and 7 December 2018.

11. The outcome of the discussions in the Working Party meetings, written input received from delegations as well as the Member States reservations on the text, are reflected in the revised Presidency compromise text which appears in the Annex. The recitals have been adapted to reflect the changes in the substantive provisions. All changes compared to the Commission proposal are indicated in **bold** (new text) or ~~strikethrough~~ (deleted text).

III. CONCLUSION

12. The text, as set out in the Annex, reflects the efforts of the Presidency and Member States to strike a compromise.

13. The Permanent Representatives Committee is therefore invited to agree submitting the text attached to this note to the Council, so as to allow it to reach a general approach. This will constitute the basis for the negotiations with the European Parliament in the framework of the ordinary legislative procedure (Art. 294 TFEU).

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on European Production and Preservation Orders for electronic evidence in criminal matters[3]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1) thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[4],

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 evidence are increasingly important to enable criminal investigations and prosecutions across the Union. Effective mechanisms to obtain electronic evidence are of the essence to combat crime, subject to conditions to ensure full accordance with fundamental rights and principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, in particular the principles of necessity and proportionality, due process, data protection, secrecy of correspondence and privacy.

---

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

4 OJ C , , p. .

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

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

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

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

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

(8) Due to this lack of connection, judicial cooperation requests are often addressed to states which are hosts to a large number of service providers, but which have no other relation to the case at hand. Furthermore, the number of requests has multiplied in view of increasingly used networked services that are borderless by nature. As a result, obtaining electronic evidence using judicial cooperation channels often takes a long time — longer than subsequent leads may be available. Furthermore, there is no clear framework for cooperation with service providers, while certain third-country providers accept direct requests for non-content data as permitted by their applicable domestic law. As a consequence, all Member States rely on the cooperation channel with service providers where available, using different national tools, conditions and procedures. In addition, for content data, some Member States have taken unilateral action, while others continue to rely on judicial cooperation.

---

5 JOIN(2017) 450 final.

6 2017/2068(INI).

(9) The fragmented legal framework creates challenges for service providers seeking to comply with law enforcement requests. Therefore there is a need to put forward a European legal framework for electronic evidence to impose an obligation on service providers covered by the scope of the instrument to respond directly to authorities without **systematic** ~~the~~ involvement of a judicial authority in the Member State of the service provider **in every case**.

(10) Orders under this Regulation should be addressed to legal representatives of service providers designated for that purpose If a service provider established in the Union has not designated a legal representative, the Orders can be addressed to any establishment of this service provider in the Union. This fall-back option serves to ensure the effectiveness of the system in case the service provider has not (yet) nominated a dedicated representative.

(11) The mechanism of the European Production Order and the European Preservation Order for electronic evidence in criminal matters can only work on the basis of a high level of mutual trust between the Member States, which is an essential precondition for the proper functioning of this instrument.

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

(**12a**) **In case, the issuing Member State has indications that parallel criminal proceedings may be ongoing in another Member State, it shall consult the authorities of this Member State in accordance with Council Framework Decision 2009/948/JHA[7]. In any case, a European Production Order should not be issued, if the issuing Member State has indications that this would be contrary to the ne bis in idem principle.**

[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).

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

(14) This Regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in Directives 2010/64/EU[8], 2012/13/EU[9], 2013/48/EU[10], 2016/343[11], 2016/800[12] and 2016/1919[13] of the European Parliament and of the Council.

(15) This instrument lays down the rules under which a competent judicial authority in the European Union may order a service provider offering services in the Union to produce or preserve electronic evidence through a European Production or Preservation Order. This Regulation is applicable in all cases where the service provider is established or represented in another Member State. For domestic situations where the instruments set out by this Regulation cannot be used, the Regulation should not limit the powers of the national competent authorities already set out by national law to compel service providers established or represented on their territory.

---

8 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).

9 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).

10 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).

11 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).

12 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).

13 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).

(16) The service providers most relevant for criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Providers of electronic communications services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. **This Regulation should also be applicable to other** ~~The categories of~~ information society services ~~providers within the meaning of Directive (EU) 2015/1535 included here 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~~ **that** do not qualify as electronic communications services ~~providers~~, **but offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf. This should be in line with the terms used in the Budapest Convention on cybercrime. Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, i.e. technical operations to produce or alter data by means of computer processing power. The categories of service providers included here are, for example** online marketplaces ~~facilitating transactions between their users (such as~~ **providing** consumers ~~or~~ **and** businesses **the ability to communicate with each other** and other hosting services, including where the service is provided via cloud computing, **as well as online gaming platforms and online gambling platforms. Where an information society service provider does not provide its users the ability to communicate with each other, but only with the service provider, or does not provide the ability to process or to store data, or where the ability to store/process data is not an essential part of the service provided to users, such as legal, architectural, engineering and accounting services provided online at a distance, it would not fall within the scope of the definition, even if within the definition of information society services pursuant to Directive (EU) 2015/1535.** ~~Information society services for which the storage of data is not a defining component of the service provided to the user, and for which it is only of an ancillary nature, such as legal, architectural, engineering and accounting services provided online at a distance, should be excluded from the scope of this Regulation, even where they may fall within the definition of information society services as per Directive (EU) 2015/1535.~~

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

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

(19) This Regulation regulates gathering of stored data only, that is, the data held by a service provider at the time of receipt of a European Production or Preservation Order Certificate. It does not stipulate a general data retention obligation, nor does it authorise interception of data or obtaining to data stored at a future point in time from the receipt of a production or preservation order certificate. Data should be provided regardless of whether it is encrypted or not.

(20) The categories of data this Regulation covers include subscriber data, access data, transactional data (these three categories being referred to as 'non-content data') and content data. This distinction, apart from the access data, exists in the ~~legal~~ laws of many Member States and also in the current US legal framework that allows service providers to share non-content data with foreign law enforcement authorities on a voluntary basis.

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

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

(23) All data categories contain personal data, and are thus covered by the safeguards under the Union data protection *acquis*, but the intensity of the impact on fundamental rights varies, in particular between subscriber data and access data on the one hand and transactional data and content data on the other hand. While subscriber data and access data are useful to obtain first leads in an investigation about the identity of a suspect, transactional and content data are the most relevant as probative material. It is therefore essential that all these data categories are covered by the instrument. Because of the different degree of interference with fundamental rights, different conditions are imposed for obtaining subscriber and access data on the one hand, and transactional and content data on the other.

(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 against the specific known or still unknow perpetrators of a concrete criminal offence that has already taken place, after an individual evaluation of the proportionality and necessity in every single case.

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

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

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

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

(27) The determination whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of an online interface as for instance the accessibility of the service provider's or an intermediary's website or of an email address and of other contact details in one or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.

(28) A substantial connection to the Union should also be relevant to determine the ambit of application of the present Regulation. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be ~~assessed on the~~ basi**sed** ~~of the existence~~ **on specific factual criteria such as** a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.[14] On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302[15] cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.

(29) A European Production Order should only be issued if it is necessary and proportionate. The assessment should take into account whether the Order is limited to what is necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the individual case only, **taking due account of the impact of the measure on fundamental rights of the person whose data are sought.**

---

14 Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

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

(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 transactional and content data, the issuing or validation of European Production Orders for production of these categories requires review by a judge. As subscriber and access data are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent prosecutors.

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

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

(33) Additionally, it is necessary to provide that the European Production Order may only be issued if a similar Order would be available for the same criminal offence in a comparable domestic situation in the issuing State.

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

(34) In cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, typically in case of hosting services, the European Production Order should only be used when other investigative measures addressed to the company or the entity are not appropriate, especially if this would create a risk to jeopardise the investigation. This is of relevance in particular when it comes to larger entities, such as corporations or government entities, that avail themselves of the services of service providers to provide their corporate IT infrastructure or services or both. The first addressee of a European Production Order, in such situations, should be the company or other entity. This company or other entity may not be a service provider covered by the scope of this Regulation. However, for cases where addressing that entity is not opportune, for example because it is suspected of involvement in the case concerned or there are indications for collusion with the target of the investigation, competent authorities should be able to address the service provider providing the infrastructure in question to provide the requested data. This provision does not affect the right to order the service provider to preserve the data.

(34a) In case data are stored or processed as part of an infrastructure provided by a service provider to a public authority only authorities of the same Member State should be able to issue a European Production or Preservation Order because such data can be considered particularly sensitive. Public authority should be understood as any authority that, by its applicable national law has a mandate to govern, administrate a part or aspect of public life, such as branches of the judiciary, the legislative or executive power of a state, province, municipality.

(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege **or the right of journalists not to disclose their sources of information)**, are referred to in other mutual recognition instruments such as the European Investigation Order. Their range and impact differ according to the applicable national law that should be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order if a similar order would be available in a comparable domestic situation. ~~In addition to this basic principle,~~ **Whether a second legal framework needs to be taken into account should depend on the strength of the connection of the person whose data is sought to the issuing State. Where the person is residing on the territory of the issuing State, a strong link to the issuing State exists. The applicable legal framework to assess immunities and privileges should therefore be that of the issuing State alone. The same principle applies for rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, and fundamental interests of the enforcing State. By the time a request for content or transactional data is made, authorities will regularly have an indication of where the person resides on the basis of previous investigatory steps. Moreover, statistics show that in a large majority of cases, the person resides in the issuing State. Where that is not the case, for example because the person whose data is sought has taken steps to conceal his or her location, the same principle should be applied.**

(35a) **I**mmunities and privileges **as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media,** which protect ~~access,~~ transactional or content data in the **enforcing** ~~Member~~ State ~~of the service provider~~ should **therefore** be taken into account ~~as far as possible~~ ~~in the issuing State~~ **where the issuing authority has reasonable grounds to believe the person whose data is sought is not residing on its territory.** ~~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 th**at~~e~~** Member State ~~where the service provider or its legal representative is addressed~~ provide for a higher protection than the law of the issuing State. The provision also ensures respect for cases where the disclosure of the data may impact fundamental interests of that Member State such as national security and defence. ~~As an additional safeguard,~~ **T**hese aspects should be taken into account not only when the Order is issued, but also later, ~~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 enforcing authority.

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

(35c) In cases where the European Production Order concerns content data and where the issuing authority has reasonable grounds to believe the person whose data are sought is not residing on its territory, the enforcing State is notified and can as soon as possible, preferably within 10 days, inform the issuing authority of issues that might lead to a withdrawal or adaptation of the Order, such as privileges or immunities of the person whose data are sought or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media. As opposed to non-content data, content data is of particularly sensitive nature because persons may reveal their thoughts as well as sensitive details of their private life. This justifies a different treatment and an involvement of the authorities of the enforcing State early on in the procedure. In such cases, the issuing Member State should provide a copy of the Certificate to the enforcing State at the same time as the Certificate is provided to the service provider. In the interest of allowing for a swift check, the issuinig authority should choose one of the languages accepted by the enforcing State if a translation of the Certificate is needed, even where the service provider indicated that it would also accept Certificates in another language than one of the official languages of the enforcing State. Where ~~applicable~~ the notified authority raises issues, it should provide the issuing authority with any relevant information regarding the immunities or privileges as well as the rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media granted to the person under its law or information, or if the Order impacts fundamental interests of that Member State such as national security and defence.

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

(35e) In order to provide for a swift procedure, the relevant point in time to determine whether there is a need to notify the authorities of the enforcing State should be the time when the Order is issued or validated. Any subsequent change of residency should not have any impact on the procedure. Where the issuing authority did not have reasonable grounds to believe the person whose data are sought is not residing on its territory at the time of issuing or validating the Order, and it later emerges that this person was in fact not residing on the territory of the issuing Member State no later check or notification should be required. However, the person concerned can invoke his or her rights as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media during the whole criminal proceeding, and the other Member State could also raise its fundamental interests such as national security and defence at any time during the criminal proceedings. In addition, these grounds could also be invoked during the enforcement procedure.

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

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

(36) The European Preservation Order may be issued for any offence. Its aim 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, for example because judicial cooperation channels will be used.

(36a) In order to ensure full protection of fundamental rights, any validation of European Production or Preservation Orders by judicial authorities should in principle be obtained before the order is issued. Exceptions to this principle can only be made in exceptional cases when seeking subscriber and access data where the issuing authority validly establishes an emergency case and where it is not possible to obtain the prior validation by the judicial authority in time, in particular because the validating authority cannot be reached to obtain validation and the threat is so imminent that immediate action has to be taken. However, this only applies where this procedure is provided for in a similar domestic case under national law.

(37) European Production and Preservation Orders should be addressed to the legal representative designated by the service provider. In the absence of a designated legal representative, Orders can be addressed to an establishment of the service provider in the Union. This can be the case where there is no legal obligation for the service provider to nominate a legal representative. In case of non-compliance by the legal representative in emergency situations, the European Production or Preservation Order may also be addressed to the service provider alongside or instead of pursuing enforcement of the original Order according to Article 14. In case of non-compliance by the legal representative in non-emergency situations, but where there are clear risks of loss of data, a European Production or Preservation Order may also be addressed to any establishment of the service provider in the Union. Because of these various possible scenarios, the general term 'addressee' is used in the provisions. Where an obligation, such as on confidentiality, applies not only to the addressee, but also to the service provider if it is not the addressee, this is specified in the respective provision. **In cases where the European Production or Preservation Order is addressed to the service provider following non-compliance by the legal representative, it can also be enforced against the service provider.**

(38) The European Production and European Preservation Orders should be transmitted to the ~~service provider~~ **addressee** through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR), which should be translated. The Certificates should contain the same mandatory information as the Orders, except for the grounds for the necessity and proportionality of the measure or further details about the case to avoid jeopardising the investigations. But as they are part of the Order itself, they allow the suspect to challenge it later during the criminal proceedings. Where necessary, a Certificate needs to be translated into (one of) the official language(s) of the ~~Member State of the addressee~~ **enforcing State**, or into another official language that the service provider has declared it will accept.

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

(40) The requested data should be transmitted to the authorities **in a secure and reliable way that allows to establish the auhenticity of the sender and integrity of the data** at the latest within 10 days upon receipt of the EPOC. Shorter time limits should be respected by the provider in emergency cases and if the issuing authority indicates other reasons to depart from the 10 day deadline. In addition to the imminent danger of the deletion of the requested data, such reasons could include circumstances that are related to an ongoing investigation, for example where the requested data is associated to other urgent investigative measures that cannot be conducted without the missing data or are otherwise dependent on it.

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

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

(42) Upon receipt of a European Preservation Order Certificate ('EPOC-PR'), the service provider should preserve requested data for a maximum of 60 days unless the issuing authority informs the service provider that it has launched the procedure for issuing a subsequent request for production, in which case the preservation should be continued. The 60 day period is calculated to allow for the launch of an official request. This requires that at least some formal steps have been taken, for example by sending a mutual legal assistance request to translation. Following receipt of that information, the data should be preserved as long as necessary until the data is produced in the framework of a subsequent request for production.

(43) Service providers and their legal representatives should ensure confidentiality**. Furthermore they should** ~~and when requested by the issuing authority~~refrain from informing the person whose data is being sought in order to safeguard the investigation of criminal offences, in compliance with Article 23 of Regulation (EU) 2016/679[16]. ~~However~~ **except where requested by the issuing authority to inform the person. In these cases, the issuing authority should also provide the necessary information about the applicable legal remedies to the service provider, so that it can be included in the information to the person**. I**n any case**, user information is an essential element in enabling review and judicial redress and should be provided by the authority if the service provider was **not** asked ~~not~~ to inform the user, ~~where~~ **as soos as** there is no risk of jeopardising ongoing investigations, in accordance with the national measure implementing Article 13 of Directive (EU) 2016/680[17]. **The issuing authority may abstain from informing the person whose subscriber or access data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought. This could be the case where an Order concerns subscriber or access data of a third person, in light of the presumption of innocence of the suspect. Where the identity of the person concerned is unknown to the issuing authority, investigations to determine the identity of this person should only be carried out insofar as it seems necessary and proportionate in relation to the invasiveness of the measure and the respective effort associated with establishing their identity.**

(44) In case of non-compliance by the addressee, the issuing authority may transfer the full Order including the reasoning on necessity and proportionality, accompanied by the Certificate, to the competent authority in the Member State where the addressee of the Certificate resides or is established. This Member State should enforce it in accordance with its national law. Member States should provide for the imposition of effective, proportionate and deterrent pecuniary sanctions in case of infringements of the obligations set up by this Regulation.

---

16 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).

17 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).

(45) The enforcement procedure is a procedure where the addressee can ~~oppose~~ **invoke formal grounds against** the enforcement based on certain restricted grounds. The enforcing authority can refuse to recognise and enforce the Order based on the same grounds, ~~or~~ **and additionally, in case they have to be taken into account under this Regulation,** if immunities and privileges **as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media** under its national law apply or the disclosure may impact its fundamental interests such as national security and defence. The enforcing authority should consult the issuing authority before refusing to recognise or enforce the order, based on these grounds. In case of non-compliance, authorities can impose sanctions. These sanctions should be proportionate also in view of specific circumstances such as repeated or systemic non-compliance.

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

(46) ~~Notwithstanding their data protection obligations,~~ **S**ervice providers should not be held liable in Member States for prejudice to their users or third parties ~~exclusively~~ resulting from good faith compliance with an EPOC or an EPOC-PR. **The responsibility to ensure the legality of the Order, in particular its necessity and proportionality, should lie with the issuing authority.**

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

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

(49) In determining the existence of a conflicting obligation in the specific circumstances of the case under examination, the competent court ~~should~~ **may** rely on appropriate external expertise where needed, for example ~~if the review raises questions~~ on the interpretation of the law of the third country concerned. This could include consulting the central authorities of that country.

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

(51) Where conflicting obligations exist, the court should determine whether the conflicting provisions of the third country **law applies and if so, whether they** prohibit disclosure of the data concerned ~~on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations.~~ Where the court concludes that conflicting provisions of the third country prohibit disclosure of the data ~~concerned on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence, it should consult the third country via its central authorities, which are already in place for mutual legal assistance purposes in most parts of the world. It should set a deadline for the third country to raise objections to the execution of the European Production Order; in case the third country authorities do not respond within the (extended) deadline despite a reminder informing them of the consequences of not providing a response, the court upholds the Order. If the third country authorities object to disclosure, the court should lift the Order.~~

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

(53) The conditions set out in Article 9 are applicable also where conflicting obligations deriving from the law of a third country occur. During this procedure, the data should be preserved. Where the Order is lifted, a new Preservation Order may be issued to permit the issuing authority to seek production of the data through other channels, such as mutual legal assistance.

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

(55) ~~In addition,~~During the enforcement procedure **the enforcing authority may refuse the recognititon and enforcement of a European Production or Preservation Order on a number of limited grounds.** ~~and subsequent legal remedy the addressee.may oppose the enforcement of a European Production or Preservation Order on a number of limited grounds, including it not being issued or validated by a competent authority or it being apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or is manifestly abusive. For example, an Order requesting the production of content 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 Order.~~

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

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

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

(57) Personal data obtained under this Regulation should only be processed when necessary and proportionate to the purposes of prevention, investigation, detection and prosecution of crime or enforcement of criminal sanctions and the exercise of the rights of defence. In particular, Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers for the purposes of this Regulation, including measures to ensure the security of the data. Service providers should ensure the same for the transmission of personal data to relevant authorities. Only authorised persons should have access to information containing personal data which may be obtained through authentication processes. The use of mechanisms to ensure authenticity should be considered, such as notified national electronic identification systems or trust services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

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

(60) In order to effectively address a possible need for improvement regarding the content of the EPOCs and EPOC-PRs and of the Form to be used to provide information on the impossibility to execute the EPOC or EPOC-PR, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[18]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(61) The measures based on this Regulation should not supersede European Investigation Orders in accordance with Directive 2014/41/EU of the European Parliament and of the Council[19] to obtain electronic evidence. Member States' authorities should choose the tool most adapted to ~~their situation~~ **the case at hand**; they may prefer to use the European Investigation Order when requesting a set of different types of investigative measures including but not limited to the production of electronic evidence from another Member State.

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

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

---

18 OJ L 123, 12.5.2016, p. 1.

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

(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, ~~[the United Kingdom /~~Ireland has notified its wish to take part in the adoption and application of this Regulation~~] or [and~~ without prejudice to Article 4 of that Protocol, the United Kingdom~~/Ireland~~ is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

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

(66) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[20] and delivered an opinion on (…)[21],

---

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

[21] OJ C , , p. .

HAVE ADOPTED THIS REGULATION:

Chapter 1: Subject matter, definitions and scope

Article 1
Subject matter

1. This Regulation lays down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data. This Regulation is without prejudice to the powers of national authorities to compel service providers established or represented on their territory to comply with similar national measures.

2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities 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 binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;

(2) 'European Preservation Order' means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production;

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

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

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

(c) **other** information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[22] **that provide:**

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

– to process or store data on behalf of the users to whom the service is provided ~~for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users and other hosting service providers;~~[23]

(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 (3) above; and

(b) having a substantial connection **based on specific factual criteria** to the Member State(s) referred to in point (a);

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

(6) 'electronic evidence' means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data;

---

22 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).

23 Finland, Latvia and Luxemburg have a reservation because public authorities should not be obliged to comply with a European Production or Preservation Order (Finland) and the definition being still too vague and legally uncertain (Luxemburg); on the necessity to explore the definition further, especially with relation to the proposal of the Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (Latvia).

(7) ‘subscriber data’ means any data pertaining to:

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

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

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

(9) ‘transactional data’ means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitues access data. This includes electronic communications metadata as defined in point (~~g~~**c**) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];

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

(11) ‘information system’ means information system as defined in point (a) of Article 2 of Directive 2013/40/EU of the European Parliament and of the Council[24];

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

---

[24] 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).

(13) 'enforcing State' means the Member State in which the addressee of the European Production Order or the European Preservation Order resides or is established and to which**, if necessary,** the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted for enforcement;

(14) 'enforcing authority' means the competent authority in the enforcing State to which the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted by the issuing authority for enforcement;

(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC[25].

Article 3
Scope

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

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

2. The European Production Orders and European ~~Production~~**Preservation** Orders may only be issued for criminal proceedings, ~~both during the pre-trial and trial phase~~ **and for the execution of custodial sentences or detention orders that were not rendered in absentia in case the convict absconded from justice**~~.~~ The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.[26]

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.

---

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

26 Czech Republic, Finland, Latvia and Germany have a reservation on the extension of the scope regarding convicts who absconded from justice; also for the parallel provisions in Article 5(3) and 6(2).

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

Article 4
Issuing authority

1. A European Production Order for subscriber data and access data may be issued by:

   (a) a judge, a court, an investigating judge or 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 prosecutor in the issuing State.

2. A European Production Order for transactional 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 may be issued by:

   (a) a judge, a court, an investigating judge or 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 prosecutor in the issuing State.

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

5. In validly established emergency cases, the authorities mentioned under paragraphs 1(b) and 3(b) may issue the respective Order for subscriber and access data, without prior validation if the validation cannot be obtained in time and if these authorities could issue the Order in a similar domestic case without validation. The issuing authority shall seek validation ex-post without undue delay, at the latest within 48 hours. Where such ex-post validation is not granted the issuing authority shall withdraw the Order immediately and shall, in accordance with its national law, either delete any data that was obtained or ensure that the data are not used as evidence.[27]

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

[27] Greece, Luxemburg and Slovenia have a reservation on the possibility for ex-post validation.

Article 5
Conditions for issuing a European Production Order

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

2. The European Production Order shall be necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2) and may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State.

3. European Production Orders to produce subscriber data or access data may be issued for all criminal offences **and for the execution of a custodial sentence or a detention order of at least 4 months.**

4. European Production Orders to produce transactional data or content data may only be issued[28]:

   (a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years[29], or

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

   – offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA[30];

   – offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[31];

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

---

28 Finland and Slovenia would prefer a list approach.

29 Cyprus has a reservation regarding the conditions to issue a European Production Order for criminal offences punishable for less than 5 years;

30 Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (OJ L 149, 2.6.2001, p. 1).

31 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).

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[32].

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

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

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

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

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

(d) the requested data category (subscriber data, access data, transactional data or content data);

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

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

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

(h) in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, a confirmation that the Order is made in accordance with paragraph 6;

(i) the grounds for the necessity and proportionality of the measure.

6. In cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigatory measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.

---

[32] 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).

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

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

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

b. **the** data requested is protected by immunities and privileges granted under the law of the ~~Member State where the service provider is addressed~~ **enforcing** State or **it is subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media** its disclosure may impact fundamental interests of th~~eat Member~~ **enforcing** State such as national security and defence, the issuing authority ~~has to~~ **shall** seek clarification **on the circumstances referred to in point b)** before issuing the European Production Order, including by consulting the competent authorities of the ~~Member~~ **enforcing** State~~ concerned~~, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested ~~access,~~ transactional ~~or content~~ data ~~*is*~~ **are** protected by such immunities and privileges **or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media** or its disclosure would impact fundamental interests of the other Member State **such as national security and defence**, **it shall take these circumstances into account in the same way as if they were provided for under its national law and** it **shall** not issue **or shall adapt** the European Production Order **where necessary to give effect to these grounds**.[33]

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

---

33 Germany and Czech Republic advocates for the addition of content data. Germany also requested the inclusion of a fundamental rights clause both in this provision and in Article 12a. Hungary entered a substantial reservation due to the logic of the provision as in its view when there are reasonable grounds to believe that denial is foreseeable a prior consultation should be available in general, also for parallel provisions in Article 5(7), 7a, 9(5), 12a and 14.

Article 6
Conditions for issuing a European Preservation Order

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

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. European Preservation Orders to preserve data may be issued for all criminal offences **and for the execution of a custodial sentence or a detention order of at least 4 months**.

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

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

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

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

   (d) the data category to be preserved (subscriber data, access data, transactional data or content data);

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

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

   (g) the grounds for the necessity and proportionality of the measure.

Article 7
Addressee of a European Production Order and a European Preservation Order

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

2. If no ~~dedicated~~ legal representative has been appointed, the European Production Order and the European Preservation Order may be addressed to any establishment of the service provider in the Union.

3. Where the legal representative does not comply with an EPOC in an emergency case pursuant to Article 9(2), the **European Production Order**~~EPOC~~ may be addressed to any establishment of the service provider in the Union.

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

Article 7a
Notification[34]

1. In cases where the European Production Order concerns content data, and the issuing authority has reasonable grounds to believe that the person whose data are sought is not residing on its own territory, the issuing authority shall submit a copy of the EPOC to the competent authority of the enforcing State at the same time the EPOC is submitted to the addressee in accordance with Article 7.

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

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

4. The notification shall not have suspensive effect on the obligations of the addressee under this Regulation.

---

34 Czech Republic, Finland, Germany, Greece, Hungary and Latvia have a reservation on the notification procedure advocating for a procedure with more effect that also includes transactional data and a fundamental rights clause, i.e. providing for grounds for refusal to the notified authority; furthermore also rule on what should be considered a "national case" should be reversed; finally Germany advocating for submission of the Order instead of the Certificate, whereas Czech Republic is of the view that both the Order and the Certificate should be submitted.
Belgium, Bulgaria, Estonia, France, Ireland, Italy,Poland, Portugal and Spain have a reservation on the notification procedure and provisions linked to the introduction of a notification procedure, in particular Article 5(7), 9, 12a and 14 as well as the related recitals stating that the Commission's proposal without notification would be preferred; Belgium, Luxembourg, Ireland, Slovenia and Poland would prefer, if at all, a notification to the Member State where the person whose data are sought is residing.

Article 8
European Production and Preservation Order Certificate

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

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

2 The EPOC or the EPOC-PR shall be ~~directly~~ transmitted by **or on behalf of the issuing authority** ~~any means capable~~ **in a secure and reliable way allowing** ~~of producing a written record under conditions allowing~~ the addressee to **produce a written record and to** establish ~~its~~ **the** authenticity **of the Certificate**.

   Where service providers, Member States or Union bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities, the issuing authority may also choose to transmit the Certificate via these channels.

3. The EPOC shall contain the information listed in Article 5(5) (a) to (h), including sufficient information to allow the addressee to identify and contact the issuing authority. The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.

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

5. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the Union accepted by the addressee. Where no language has been specified, the EPOC or the EPOC-PR shall be translated into one of the official languages of the Member State where the legal representative resides or is established.

Article 9
Execution of an EPOC

1. Upon receipt of the EPOC, the addressee shall ensure that the requested data ~~is~~ **are** transmitted **in a secure and reliable way allowing the establishment of authenticity and integrity** directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure.[35]

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

3. If the addressee cannot comply with its obligation because the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC, the addressee shall inform the issuing authority referred to in the EPOC without undue delay and ask for clarification, using the Form set out in Annex III. It shall inform the issuing authority whether an identification and preservation was possible as set out in paragraph 6. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided.

4. If the addressee cannot comply with its obligation because ~~of force majeure or~~ of de facto impossibility **due to circumstances not created by the addressee or the service provider at the time the order was received** ~~not attributable to the addressee or, if different, 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 addressee shall inform the issuing authority referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. ~~If the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC.~~

[35] Germany proposes at least the addition of a new recital requesting the Commission and the Member States to work on and establish as soon as possible secure electronic channels of communication allowing the establishment of authenticity and integrity.

5. In all cases where the addressee does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons~~listed in the Form of Annex III~~, it shall inform the issuing authority 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 service provider to produce the data.

~~In case~~ the ~~addressee considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive, the addressee shall also send the Form in Annex III to the competent enforcement authority in the Member State of the addressee. In such cases the competent enforcement authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network.~~[36]

6. The addressee shall preserve the data requested, if it does not produce it immediately, unless the information in the EPOC does not allow it to identify the data requested, in which case it shall seek clarification in accordance with paragraph 3. The preservation shall be upheld until the data is produced, whether it is on the basis of the clarified European Production Order and its Certificate or through other channels, such as mutual legal assistance. If the production of data and its preservation is no longer necessary, the issuing authority and where applicable pursuant to Article 14(8) the enforcing authority shall inform the addressee without undue delay.

[36] Hungary has a reservation on the deletion.

Article 10
Execution of an EPOC-PR

1. Upon receipt of the EPOC-PR, the addressee shall, without undue delay, preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been launched.

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

3. If the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay.

4. If the addressee cannot comply with its obligation because the Certificate is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC-PR, the addressee shall inform the issuing authority set out in the EPOC-PR without undue delay and ask for clarification, using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The addressee shall ensure that on its side the needed clarification can be received in order to fulfil its obligation set out in paragraph 1.

5. If the addressee cannot comply with its obligation because ~~of force majeure or~~ of de facto impossibility **due to circumstances not created by the addressee or the service provider at the time the order was received** ~~not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the Order, it~~ **the addressee** shall ~~contact~~ **inform** the issuing authority set out in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. ~~If these conditions are fulfilled, the issuing authority shall withdraw the EPOC-PR.~~

6. In all cases where the addressee does not preserve the requested information, for other reasons ~~listed in the Form of Annex III~~, the addressee shall inform the issuing authority without undue delay of the reasons for this in the Form set out in Annex III. The issuing authority shall review the Order in light of the justification provided by the service provider.

Article 11
Confidentiality and user information[37]

1. Addressees and, if different, service providers shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and ~~where requested by the issuing authority,~~ shall refrain from informing the person whose data is being sought in order **to avoid** ~~not to~~ obstruct**ing** the relevant criminal proceedings. **They shall only inform the person whose data** ~~is~~ **are being sought if expicitly requested by the issuing authority. In this case the issuing authority shall also provide information pursuant to paragraph 4 of this Article to the addressee or, if different, to the service provider.**

2. Where the issuing authority **did not** request~~ed the addressee to refrain from~~ **the service provider to** inform~~ing~~ the person whose data **were** ~~being~~ sought **in accordance with paragraph 1**, the issuing authority shall inform this~~e~~ person ~~whose data is being sought by the EPOC without undue delay about the data production~~. The~~is~~ **issuing authority may delay informing the person whose data were sought as long as it constitutes a necessary and proportionate measure** ~~information shall be submitted as soon as this is possible without may be delayed as long as necessary and proportionate~~ to avoid obstructing ~~*the relevant*~~ criminal proceedings~~. Information about available remedies pursuant to Article 17 shall be included. The issuing authority may abstain from informing the person whose subscriber or access data was sought about the production of data where fundamental rights and legitimate interests of another person outweigh the interest of the person whose data was sought.~~

3. **The issuing authority may abstain from informing the person whose subscriber or access data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought**~~. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.~~

4. Information about available remedies pursuant to Article 17 shall be included.

---

[37] Finland and Germany have reservations advocating for further details (provisions on language, legal aid, detailed information on legal remedies etc.) and in addition, Germany stating that persons concerned (not only person whose data are sought) should be informed.

Article 12
Reimbursement of costs

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

Article **12a** ~~18~~
~~Ensuring privileges and immunities under the law of the enforcing State~~**Limitations to the use of data obtained**

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

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

Article 12b
Speciality principle

1. Electronic evidence shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except:

(a) for the purpose of proceedings for which a European Production Order could have been issued in accordance with Article 5(3) and (4); or

(b) for preventing an immediate and serious threat to public security of the issuing State or its essential interests;

2. Electronic evidence obtained in accordance with this Regulation may only be transmitted to another Member State:

a) for the purpose of proceedings for which a European Production Order could have been issued in accordance with Article 5(3) and (4); or

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

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

Chapter 3: Sanctions and enforcement

Article 13
Sanctions[38]

Without prejudice to national laws which provide for the imposition of criminal sanctions, Member States shall lay down the rules on pecuniary sanctions applicable to infringements of the obligations pursuant to Articles 9, 10 and 11 **(1)** of this Regulation and shall take all necessary measures to ensure that they are implemented. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

The **Member States shall ensure that** pecuniary sanctions provided for ~~shall be~~ **are** effective, proportionate and dissuasive.

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

Article 14
Procedure for enforcement

1. If the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority, the issuing authority may transfer to the competent authority in the enforcing State the European Production Order with the EPOC or the European Preservation Order with the EPOC-PR as well as the Form set out in Annex III filled out by the addressee and any other relevant document with a view to its enforcement by any means capable of producing a written record under conditions allowing the enforcing authority to establish authenticity. To this end, the issuing authority shall translate the Order, the Form and any other accompanying documents into one of the ~~official~~ languages ~~of~~ **accepted by** this Member State and shall inform the addressee of the transfer.

2. Upon receipt, the enforcing authority shall without further formalities recognise **and take the necessary measures for enforcement of**

   (a) a European Production Order **unless the enforcing authority considers that one of the grounds provided for in paragraph 4 apply,** or

   (b) **a** European Preservation Order ~~transmitted in accordance with paragraph 1 and shall take the necessary measures for its enforcement,~~ unless the enforcing authority considers that one of the grounds provided for in paragraph ~~4 or~~ 5 apply ~~or that the data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence.~~

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

[38] Finland, Germany and Latvia have a reservation on the harmonisation of sanctions.

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

3. Where the enforcing authority recognises the Order, it shall formally require the addressee to comply with the relevant obligation, informing the addressee of the possibility to oppose the enforcement by invoking the grounds listed in paragraph~~s~~ 4 **point (a) to (e)** or **paragraph** 5, as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.

4. ~~The addressee may only oppose the~~ **Recognition or** enforcement of the European Production Order **may only be denied** on the basis of the following grounds:

   (a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;

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

   (c) the addressee could not comply with the EPOC because of de facto impossibility ~~or force majeure~~ or because the EPOC contains manifest errors;

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

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

   (f) ~~based on the sole information contained in the EPOC, it is apparent that it manifestly violates the Charter or that it is manifestly abusive~~ **one of the grounds referred to in Article 12a (1) apply.**[39]

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

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

   (b) the service provider could not comply with the EPOC-PR because of de facto impossibility ~~or force majeure~~ or because the EPOC-PR contains manifest errors;

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

   (d) the service is not covered by the scope of the present Regulation~~;~~**.**

   ~~(e) based on the sole information contained in the EPOC-PR, it is apparent that the EPOC-PR manifestly violates the Charter or is manifestly abusive.~~

---

39 Czech Republic, Finland, Hungary, Germany, Latvia have a reservation on the deletion of Article 14(4) point f) and paragraph (5), point e) advocating that the deletion could only be supported in case a clause on fundamental rights as well as on respect for national constitutional rules would be added to Articles 5, 7a(2) and 12a(1).

6. In case of an objection by the addressee **pursuant to paragraphs 4 point (a) to (e) and 5**, the enforcing authority shall decide whether to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority in accordance with paragraph 7.

7. Before deciding not to recognise or enforce the Order in accordance with paragraph 2 and 6, the enforcing authority shall consult the issuing authority by any appropriate means. Where appropriate, it shall request further information from the issuing authority. The issuing authority shall reply to any such request within 5 working days.

8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.

9. If the enforcing authority obtains the data from the addressee, it shall transmit it to the issuing authority within 2 working days, unless the data concerned is protected by an immunity or privilege **or by rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media** under its own domestic law or it impacts its fundamental interests such as national security and defence. In such case, it shall inform the issuing authority of the reasons for not transmitting the data.

10. In case the addressee does not comply with its obligations under a recognised Order whose enforceability has been confirmed by the enforcing authority, that authority shall impose a pecuniary sanction in accordance with its national law. An effective judicial remedy shall be available against the decision to impose a fine.

Chapter 4: Remedies

Article 15

Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country

1. If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5).

2. The reasoned objection 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. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country.

3. The issuing authority shall review the European Production Order on the basis of the reasoned objection. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.

   The competent court shall first assess whether a conflict exists, based on an examination of whether

   (a) the third country law applies based on the specific circumstances of the case in question and if so,

   (b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.

4. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations.

~~5. If the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. If the competent court establishes that a relevant conflict within the meaning of paragraphs 1 and 4 exists, the competent court shall transmit all relevant factual and legal information as regards the case, including its assessment, to the central authorities in the third country concerned, via its national central authority, with a 15 day deadline to respond. Upon reasoned request from the third country central authority, the deadline may be extended by 30 days.~~

~~6. If the third country central authority, within the deadline, informs the competent court that it objects to the execution of the European Production Order in this case, the competent court shall lift the Order and inform the issuing authority and the addressee. If no objection is received within the (extended) deadline, the competent court shall send a reminder giving the third country central authority 5 more days to respond and informing it of the consequences of not providing a response. If no objection is received within this additional deadline, the competent court shall uphold the Order.~~

~~7. If the competent court determines that the Order is to be upheld, it shall inform the issuing authority and the addressee, who shall proceed with the execution of the Order.~~

Article 16
Review procedure in case of conflicting obligations ~~based on other grounds~~

1. If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country ~~prohibiting disclosure of the data concerned on other grounds than those referred to in Article 15~~, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5) **and (6).**

2. The reasoned objection must include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country. **It shall be filed no later than 10 days after the date on which the addressee was served with the EPOC. Time limits shall be calculated in accordance with the national law of the issuing authority**.

3. The issuing authority shall review the European Production Order on the basis of the reasoned objection. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.

4. The competent court shall first assess whether a conflict exists, based on an examination of whether

(a) the third country law applies based on the specific circumstances of the case in question and if so,

(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.

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

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

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

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

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

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

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

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

5b. **The court may seek information from the competent authority of the third country taking into account Directive 2016/680, in particular its Chapter V and to the extent that such the transmission does not obstruct the relevant criminal proceedings.**

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

Article 17
Effective remedies[40]

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

~~2. Where the person whose data was obtained is not a suspect or accused person in criminal proceedings for which the Order was issued, this person shall have the right to effective remedies against a European Production Order in the issuing State, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.~~

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

[40] Germany has a reservation stating that every person that is concerned by an Order should be entitled to a legal remedy not only a person whose data were sought and that legal remedies should also be made available in criminal proceedings against Preservation Orders.

4. Without prejudice to Article 11, the issuing authority shall take the appropriate measures to ensure that information is provided about the possibilities under national law for seeking remedies and ensure that they can be exercised effectively.

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

6. Without prejudice to national procedural rules, Member States shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the European Production Order.

~~*Article 18*~~

~~*Ensuring privileges and immunities under the law of the enforcing State*~~

~~If transactional or content data obtained by the European Production Order is protected by immunities or privileges granted under the law of the Member State of the addressee or it impacts fundamental interests of that Member State such as national security and defence, the court in the issuing State shall ensure during the criminal proceedings for which the Order was issued that these grounds are taken into account in the same way as if they were provided for under their national law when assessing the relevance and admissibility of the evidence concerned.The court may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust.~~

Chapter 5: Final provisions

Article 18a
Language

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

Article 19
Monitoring and reporting

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

2. In any event, Member States shall collect and maintain comprehensive statistics from the relevant authorities. The data collected shall be sent to the Commission each year by 31 March for the preceding calendar year and shall**, as far as possible,** include:

   (a) the number of EPOCs and EPOC-PRs issued by type of data requested, service providers addressed and situation (emergency case or not**, ex-post validation**);

   (b) the number of fulfilled and non-fulfilled EPOCs by type of data requested, service providers addressed and situation (emergency case or not);

   (c) for fulfilled EPOCs, the average duration for obtaining the requested data from the moment the EPOC is issued to the moment it is obtained, by type of data requested, service provider addressed and situation (emergency case or not);

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

(e) the number of legal remedies against European Production Orders in the issuing State and in the enforcing State by type of data requested;

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

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

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

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

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

Article 20
Amendments to the Certificates and the Forms

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

Article 21
Exercise of delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 20 shall be conferred for an indeterminate period of time from *[date of application of this Regulation]*.

3. The delegation of powers referred to in Article 20 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[41].

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

6. A delegated act adopted pursuant to Article 20 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 2 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 2 months at the initiative of the European Parliament or of the Council.

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

Article 22
Notifications

1. By *[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, **transmit and/or receive** European Production Orders and European Preservation Orders **or the notifications thereof**;

   (b) the enforcing authority or authorities which are competent to enforce European Production Orders and European Preservation Orders on behalf of another Member State;

   (c) the courts competent to deal with reasoned objections by addressees in accordance with Article~~s 15 and~~ 16;

   (d) **languages accepted for the transmission of the EPOC or EPOC-PR and/or a European Production Order and a European Preservation Order, in case of enforcement in accordance with Article 18a**.

2. The Commission shall make the information received under this Article publicly available, either on a dedicated website or on the website of the European Judicial Network referred to in Article 9 of the Council Decision 2008/976/JHA[42].

Article 23
Relationship to ~~European Investigation Orders~~ ***other instruments, agreements and arrangements***

This Regulation does not affect EU and other international instruments, agreements and arrangements on ~~Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for~~ the gathering of evidence that would also fall within the scope of this Regulation.

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

Article 24
Evaluation

By *[5 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 include an assessment of the need to enlarge its scope. If necessary, the report shall be accompanied by legislative proposals. The evaluation shall be conducted according to the Commission's better regulation guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

Article 25
Entry into force

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

It shall apply from *[~~6~~ **24** months after its entry into force]*.

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

Done at Strasbourg,

For the European Parliament *For the Council*

The President *The President*