REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 July 2023

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee ([1]),

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

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 for criminal investigations and prosecutions across the Union. Effective mechanisms to obtain electronic evidence are essential to combat crime, and such mechanisms should be subject to conditions and safeguards to ensure full compliance with fundamental rights and principles recognised in Article 6 of the Treaty on European Union (TEU) and the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the principles of necessity and proportionality, due process, protection of privacy and personal data and confidentiality of communications.

(3) The Joint Statement of the Ministers of Justice and Home Affairs and representatives of the Union institutions of 24 March 2016 on the terrorist attacks in Brussels stressed the need, as a matter of priority, to secure and obtain more quickly and effectively digital evidence and to identify concrete measures to do so.

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

(5) In the joint communication of the Commission and of the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council of 13 September 2017 on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, the Commission emphasised that effective investigation and prosecution of cyber-enabled crime is a key deterrent to cyber-attacks, and that today's procedural framework needs to be better adapted to the internet age. The speed of cyber-attacks can sometimes overwhelm current procedures, thereby creating particular needs for swift cooperation across borders.

(6) The resolution of the European Parliament of 3 October 2017 on the fight against cybercrime ([3]) underlined the need to find means to secure and obtain electronic evidence more rapidly, as well as the importance of close cooperation between law enforcement authorities, third countries and service providers active on European territory, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]) and

([1]) OJ C 367, 10.10.2018, p. 88.
([2]) Position of the European Parliament of 13 June 2023 (not yet published in the Official Journal) and decision of the Council of 27 June 2023.
([3]) OJ C 346, 27.9.2018, p. 29.
([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Directive (EU) 2016/680 of the European Parliament and of the Council ([5]), and existing mutual legal assistance agreements. That resolution of the European Parliament also highlighted that the currently fragmented legal framework can create challenges for service providers seeking to comply with law enforcement requests and called on the Commission to put forward a Union legal framework for electronic evidence with sufficient safeguards for the rights and freedoms of all concerned, while welcoming the ongoing work of the Commission towards a cooperation platform with a secure communication channel for digital exchanges of European Investigation Orders (EIOs) for electronic evidence and replies between Union judicial authorities.

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

(8) Due to the way in which network-based services are provided, judicial cooperation requests are often addressed to States which are hosts to a large number of service providers. Furthermore, the number of requests has multiplied due to the fact that network-based services are being increasingly used. Directive 2014/41/EU of the European Parliament and of the Council ([6]) provides for the possibility of issuing an EIO for the purpose of gathering evidence in another Member State. In addition, the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union ([7]) (the 'Convention on Mutual Assistance in Criminal Matters') also provides for the possibility of requesting evidence from another Member State. However, the procedures and timelines provided for in Directive 2014/41/EU establishing the EIO and in the Convention on Mutual Assistance in Criminal Matters might not be appropriate for electronic evidence, which is more volatile and could more easily and quickly be deleted. Obtaining electronic evidence using judicial cooperation channels often takes a long time, resulting in situations where subsequent leads might no longer be available. Furthermore, there is no harmonised framework for cooperation with service providers, while certain third-country providers accept direct requests for data other than content data as permitted by their applicable national law. As a consequence, Member States increasingly rely on voluntary direct cooperation channels with service providers where available, and they apply different national tools, conditions and procedures. For content data, some Member States have taken unilateral action, while others continue to rely on judicial cooperation.

(9) The fragmented legal framework creates challenges for law enforcement authorities and judicial authorities as well as for service providers seeking to comply with legal requests for electronic evidence, as they are increasingly faced with legal uncertainty and, potentially, conflicts of law. Therefore, there is a need to provide for specific rules as regards cross-border judicial cooperation for preserving and producing electronic evidence, which address the specific nature of electronic evidence. Such rules should include an obligation on service providers covered by the scope of this Regulation to respond directly to requests stemming from authorities in another Member State. This Regulation will therefore complement the existing Union law and clarify the rules applicable to law enforcement authorities and judicial authorities as well as to service providers in the field of electronic evidence, while ensuring full compliance with fundamental rights.

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

([5]) 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).

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

([7]) Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 3).

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

(12) The mechanism of the European Production Order and of the European Preservation Order for electronic evidence in criminal proceedings relies on the principle of mutual trust between the Member States and on a presumption of compliance by Member States with Union law, the rule of law and, in particular, with fundamental rights, which are essential elements of the Union's area of freedom, security and justice. Such a mechanism enables national competent authorities to send such orders directly to service providers.

(13) The respect for private and family life and the protection of natural persons regarding the processing of personal data are fundamental rights. In accordance with Article 7 and Article 8(1) of the Charter, everyone has the right to respect for their private and family life, home and communications and to the protection of personal data concerning them.

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

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

(16) The procedural rights in criminal proceedings set out in Directives 2010/64/EU ([9]), 2012/13/EU ([10]), 2013/48/EU ([11]), (EU) 2016/343 ([12]), (EU) 2016/800 ([13]) and (EU) 2016/1919 ([14]) of the European Parliament and of the Council should apply, within the scope of those Directives, to criminal proceedings covered by this Regulation as regards the Member States bound by those Directives. The procedural safeguards under the Charter should also apply.

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

([8]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

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

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

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

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

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

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

(18) This Regulation lays down the rules under which a competent judicial authority in the Union may, in criminal proceedings, including criminal investigations, or for the execution of a custodial sentence or a detention order following criminal proceedings in accordance with this Regulation, order a service provider offering services in the Union to produce or to preserve electronic evidence through a European Production Order or a European Preservation Order. This Regulation should be applicable in all cross-border cases where the service provider has its designated establishment or legal representative in another Member State. This Regulation is without prejudice to the powers of national authorities to address service providers established or represented on their territory in order for them to comply with similar national measures.

(19) This Regulation should regulate the gathering of data stored by a service provider at the time of receipt of a European Production Order or a European Preservation Order only. It should not lay down a general data retention obligation for service providers and it should not have the effect of resulting in any general and indiscriminate retention of data. This Regulation also should not authorise the interception of data or the obtention of data that are stored after the receipt of a European Production Order or a European Preservation Order.

(20) The application of this Regulation should not affect the use of encryption by service providers or their users. Data requested by means of a European Production Order or a European Preservation Order should be provided or preserved regardless of whether they are encrypted or not. However, this Regulation should not lay down any obligation for service providers to decrypt data.

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

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

(23) As proceedings for mutual legal assistance might be considered as criminal proceedings in accordance with applicable national law in the Member States, it should be clarified that a European Production Order or a European Preservation Order should not be issued to provide mutual legal assistance to another Member State or a 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 national law.

(24) In the framework of criminal proceedings, the European Production Order and the European Preservation Order should only be issued for specific criminal proceedings concerning a specific criminal offence that has already taken place, after an individual evaluation of the necessity and proportionality of those orders in every single case, taking into account the rights of the suspect or the accused person.

(25) This Regulation should also apply to proceedings initiated by an issuing authority to locate a convicted person that has absconded from justice, in order to execute a custodial sentence or a detention order following criminal proceedings. However, where the custodial sentence or detention order was imposed by a decision rendered in absentia it should not be possible to issue a European Production Order or a European Preservation Order, as the national law of the Member States on judicial decisions rendered in absentia varies considerably throughout the Union.

(26) This Regulation should apply to service providers offering services in the Union, and it should only be possible to issue the orders provided for in this Regulation for data pertaining to services offered in the Union. Services offered exclusively outside the Union should not be included in the scope of this Regulation, even if the service provider is established in the Union. Therefore, this Regulation should not allow any access to data other than data related to the services offered to the user in the Union by those service providers.

(27) The service providers most relevant for gathering evidence in criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Electronic communication services are defined in Directive (EU) 2018/1972 of the European Parliament and of the Council [15] and include inter-personal

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

communications services such as voice-over-IP, instant messaging and email services. This Regulation should also be applicable to information society service providers within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council ([16]) that do not qualify as electronic communications service providers but offer their users the ability to communicate with each other or offer their users services that can be used to store or otherwise process data on their behalf. This would be in line with the terms used in the Council of Europe Convention on Cybercrime (ETS No 185), done at Budapest on 23 November 2001 ('Budapest Convention'). Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, that is to say technical operations to produce or alter data by means of computer processing power. The categories of service providers covered by this Regulation should include, for example, online marketplaces providing consumers and businesses with the ability to communicate with each other, and other hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms. Where an information society service provider does not provide its users with the ability to communicate with each other but only with the service provider, or does not provide the ability to store or otherwise process data, or where the storage of data is not a defining component, that is, an essential part, of the service provided to users, such as legal, architectural engineering and accounting services provided online at a distance, it should not fall within the scope of the definition of 'service provider' laid down in this Regulation, even if the services provided by that service provider are information society services within the meaning of Directive (EU) 2015/1535.

(28) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registries and registrars 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 websites. They hold data that could make the identification of an individual or entity behind a website used in a criminal activity, or the victim of a criminal activity, possible.

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

(30) A substantial connection to the Union should also be relevant to determining whether a service provider offers services in the Union. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be based on specific factual criteria such as the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from the provision of local advertising or advertising in the language generally used in that Member State, or from the handling of customer relations, such as by the provision of customer service in the language generally used in that Member State. A substantial connection should also be considered to exist where a service provider directs its activities towards one or more Member States as set out in Regulation (EU) No 1215/2012 of the European Parliament and of the Council ([17]). On the other hand, provision of a service for the purpose of mere compliance with the prohibition of discrimination laid down in Regulation (EU) 2018/302 of the European Parliament and of the Council ([18]) should not, without additional grounds, be considered to be directing or targeting activities towards a given territory within the Union. The same considerations should apply when determining whether a service provider offers services in a Member State.

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

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

([18]) Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (OJ L 60 I, 2.3.2018, p. 1).

(31) This Regulation should cover the data categories of subscriber data, traffic data and content data. Such categorisation is in line with the law of many Member States and Union law, such as Directive 2002/58/EC and the case law of the Court of Justice, as well as international law, in particular the Budapest Convention.

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

(33) Where IP addresses, access numbers and related information are not requested for the sole purpose of identifying the user in a specific criminal investigation, they are generally requested to obtain more privacy-intrusive information, such as the contacts and whereabouts of the user. As such, they could serve to establish a comprehensive profile of an individual concerned, but at the same time they can be processed and analysed more easily than content data, as they are presented in a structured and standardised format. It is therefore essential that, in such situations, IP addresses, access numbers and related information not requested for the sole purpose of identifying the user in a specific criminal investigation, be treated as traffic data and requested under the same regime as content data, as defined in this Regulation.

(34) All data categories contain personal data and are thus covered by the safeguards under the Union data protection *acquis*. However, the intensity of the impact on fundamental rights varies between the categories, in particular between subscriber data and data requested for the sole purpose of identifying the user as defined in this Regulation, on the one hand, and traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, and content data on the other. While subscriber data as well as IP addresses, access numbers and related information, where requested for the sole purpose of identifying the user, could be useful to obtain first leads in an investigation about the identity of a suspect, traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, and content data are often more relevant as probative material. It is therefore essential that all those data categories are covered by this Regulation. Given the varying degree of interference with fundamental rights, appropriate safeguards and conditions should be imposed for obtaining such data.

(35) Situations in which there is an imminent threat to the life, physical integrity or safety of a person should be treated as emergency cases, and entail shorter time limits for the service provider and the enforcing authority. Where the disruption or destruction of a critical infrastructure as defined in Council Directive 2008/114/EC ([19]) would imply such a threat, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State, such a situation should also be treated as an emergency case, in accordance with Union law.

(36) When a European Production Order or a European Preservation Order is issued, there should always be a judicial authority involved either in the process of issuing or in the process of validating the order. In view of the more sensitive nature of traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, and of content data, the issuing or validation of a European Production Order to obtain those data categories requires review by a judge. As subscriber data and data requested for the sole purpose of identifying the user as defined in this Regulation are less sensitive, a European Production Order to obtain

([19]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

such data can in addition be issued or validated by a competent public prosecutor. In accordance with the right to a fair trial, as protected by the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms, public prosecutors are to exercise their responsibilities objectively, taking their decision in relation to the issuing or validation of a European Production Order or a European Preservation Order solely on the basis of the factual elements in the case file and taking into account all incriminatory and exculpatory evidence.

(37) In order to ensure that fundamental rights are fully protected, any validation of European Production Orders or of European Preservation Orders by judicial authorities should in principle be obtained before the order concerned is issued. Exceptions to that principle should only be made in validly established emergency cases when requesting the production of subscriber data or data requested for the sole purpose of identifying the user, as defined in this Regulation, or the preservation of data, where it is not possible to obtain 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, such exceptions should only be made where the authority issuing the order concerned could issue an order in a similar domestic case under national law without prior validation.

(38) A European Production Order should only be issued if it is necessary, proportionate, adequate and applicable to the case at hand. The issuing authority should take into account the rights of the suspect or the accused person in proceedings relating to a criminal offence and should only issue a European Production Order if such order could have been issued under the same conditions in a similar domestic case. The assessment of whether to issue a European Production Order should take into account whether such order is limited to what is strictly necessary to achieve the legitimate aim of obtaining data that are relevant and necessary as evidence in an individual case.

(39) In cases where a European Production Order is issued to obtain different data categories, the issuing authority should ensure that the conditions and procedures, such as notification to the enforcing authority, are met for each of those data categories respectively.

(40) In view of the more sensitive nature of traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, and of content data, a distinction should be made regarding the material scope of this Regulation. It should be possible to issue a European Production Order to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user, as defined in this Regulation, for any criminal offence, whereas a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or to obtain content data should be subject to stricter requirements to reflect the more sensitive nature of such data. This Regulation should provide for a threshold in relation to its scope, allowing for a proportionate approach, together with a number of other *ex ante* and *ex post* conditions and safeguards to ensure respect for proportionality and the rights of the persons affected. At the same time, such a threshold should not limit the effectiveness of this Regulation and its use by practitioners. Allowing the issuing of European Production Orders in criminal proceedings only for offences that carry at least a three-year maximum custodial sentence will limit the scope of this Regulation to more serious offences, without excessively affecting the possibilities of its use by practitioners. That limitation would exclude from the scope of this Regulation a significant number of offences which are considered less serious by Member States, as expressed in a lower maximum penalty. That limitation will also have the advantage of being easily applicable in practice.

(41) 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 offences, even those which might not be considered serious in and of themselves but which could cause extensive or considerable damage, in particular offences with low individual impact but high volume and overall damage. For most cases in which the offence has been committed by means of an information system, applying the same threshold as for other types of offences would to a large extent lead to impunity. That justifies the application of this Regulation for such offences also where they carry a maximum custodial sentence of less than three years. Additional terrorism-related offences within the meaning of Directive (EU) 2017/541 of the European Parliament and of the Council ([20]) as well as offences concerning sexual abuse and sexual exploitation of children within the

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

meaning of Directive 2011/93/EU of the European Parliament and of the Council ([21]) should not require the minimum threshold of a three-year maximum custodial sentence.

(42) As a matter of principle, a European Production Order should be addressed to the service provider, acting as controller. However, in some circumstances, determining whether a service provider has the role of controller or processor can prove particularly challenging, in particular where several service providers are involved in the processing of data or where service providers process the data on behalf of a natural person. Distinguishing between the roles of controller and processor with regard to a particular set of data requires not only specialised knowledge of the legal context, but could also require interpretation of often very complex contractual frameworks providing in a specific case for allocation to various service providers of different tasks and roles with regard to a particular set of data. Where service providers process data on behalf of a natural person, it may be difficult in some cases to determine who the controller is, even where there is only one service provider involved. Where the data concerned are stored or otherwise processed by a service provider and there is no clarity as to who the controller is, despite reasonable efforts on the part of the issuing authority, it should therefore be possible to address a European Production Order directly to that service provider. Moreover, in some cases, addressing the controller could be detrimental to the investigation in the case concerned, for example because the controller is a suspect or an accused or convicted person or there are indications that the controller could be acting in the interest of the person that is the subject of the investigation. Also in those cases, it should be possible to address a European Production Order directly to the service provider processing the data on behalf of the controller. That should not affect the right of the issuing authority to order the service provider to preserve the data.

(43) In accordance with Regulation (EU) 2016/679, the processor that stores or otherwise processes the data on behalf of the controller should inform the controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. In that case, the issuing authority should indicate in the case file the reasons for the delay in informing the controller and a short justification should also be added in the accompanying certificate transmitted to the addressee.

(44) Where the data are stored or otherwise processed as part of an infrastructure provided by a service provider to a public authority, it should only be possible to issue a European Production Order or a European Preservation Order where the public authority for which the data are stored or otherwise processed is located in the issuing - State.

(45) In cases where data protected by professional privilege under the law of the issuing State are stored or otherwise processed by a service provider as part of an infrastructure provided to professionals covered by professional privilege ('privileged professional'), in their business capacity, it should only be possible to issue a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or to obtain content data where the privileged professional resides in the issuing State, where addressing the privileged professional might be detrimental to the investigation, or where the privileges were waived in accordance with the applicable law.

(46) The principle of *ne bis in idem* is a fundamental principle of law in the Union, as recognised by the Charter and developed by the case law of the Court of Justice of the European Union. Where the issuing authority has grounds to believe that parallel criminal proceedings could be ongoing in another Member State, it should consult the authorities of that Member State in accordance with Council Framework Decision 2009/948/JHA ([22]). In any case, a European Production Order or a European Preservation Order is not to be issued where the issuing authority has grounds to believe that this would be contrary to the *ne bis in idem* principle.

(47) 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 in Directive 2014/41/EU establishing the EIO. The range and impact of immunities and privileges differ according to the applicable national law that should be taken into account at the time of issuing a European Production Order or a European Preservation Order, as the issuing authority should only be able to issue the order if it could have been issued under the same conditions in a similar domestic case. There is no common definition of what constitutes an immunity or privilege in Union law. The precise definition of those terms is therefore left to national law, and the definition

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

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

can include protections which apply to, for instance, medical and legal professions, including when specialised platforms are used in those professions. The precise definition of immunities and privileges can also include rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media.

(48) Where the issuing authority seeks to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or to obtain content data, by issuing a European Production Order and has reasonable grounds to believe that the data requested are protected by immunities or privileges granted under the law of the enforcing State, or that those data are subject in that State to rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media, the issuing authority should be able to seek clarification before issuing the European Production Order, including by consulting the competent authorities of the enforcing State, either directly or via Eurojust or the European Judicial Network.

(49) It should be possible to issue a European Preservation Order for any criminal offence. The issuing authority should take into account the rights of the suspect or the accused person in proceedings relating to a criminal offence and should only issue a European Preservation Order if such order could have been issued under the same conditions in a similar domestic case and where it is necessary, proportionate, adequate and applicable to the case in hand. The assessment of whether to issue a European Preservation Order should take into account whether such order is limited to what is strictly necessary to achieve the legitimate aim of preventing the removal, deletion or alteration of data that are relevant and necessary as evidence in an individual case in situations where it could take more time to obtain the production of those data.

(50) European Production Orders and European Preservation Orders should be addressed directly to the designated establishment or to the legal representative, designated or appointed by the service provider pursuant to Directive (EU) 2023/1544 of the European Parliament and of the Council ([23]). Exceptionally, in emergency cases as defined in this Regulation, where the designated establishment or the legal representative of a service provider does not react to the accompanying European Production Order Certificate (EPOC) or European Preservation Order Certificate (EPOC-PR) within the deadlines or has not been designated or appointed within the deadlines set out in Directive (EU) 2023/1544 it should be possible to address the EPOC or the EPOC-PR to any other establishment or legal representative of the service provider in the Union alongside or instead of pursuing enforcement of the initial order in accordance with this Regulation. Given those various possible scenarios, the general term 'addressee' is used in the provisions of this Regulation.

(51) In view of the more sensitive nature of a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, or to obtain content data, it is appropriate to provide for a notification mechanism applicable to European Production Orders to obtain those data categories. That notification mechanism should involve an enforcing authority and consist in the transmission of the EPOC to that authority at the same time as the EPOC is transmitted to the addressee. However, where a European Production Order is issued to obtain electronic evidence in criminal proceedings with substantial and strong links to the issuing State, no notification to the enforcing authority should be required. Such links should be assumed where, at the time of issuing the European Production Order, the issuing authority has reasonable grounds to believe that the offence has been committed, is being committed or is likely to be committed in the issuing State, and where the person whose data are requested resides in the issuing State.

(52) For the purposes of this Regulation, an offence should be considered as having been committed, being committed or being likely to be committed in the issuing State if it is so considered in accordance with the national law of the issuing State. In some cases, especially in the cybercrime field, some factual elements, such as the place of residence of the victim, are usually important indications to consider when determining where the offence has been committed. For instance, ransomware crimes can often be considered as having been committed where the victim of such a crime resides, even when the exact location from where the ransomware has been launched is uncertain. Any determination as to the place where the offence was committed should be without prejudice to the rules on jurisdiction over the relevant offences pursuant to the applicable national law.

([23]) Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (see page 181 of this Official Journal).

(53) It is for the issuing authority to assess, at the time of issuing the European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or to obtain content data, and on the basis of the material before it, whether there are reasonable grounds to believe that the person whose data are requested resides in the issuing State. In that regard, various objective circumstances that could indicate that the person concerned has established the habitual centre of their interests in a particular Member State or has the intention to do so, can be of relevance. It follows from the need for uniform application of Union law and from the principle of equality that the notion of 'residence' in this particular context should be given uniform interpretation throughout the Union. Reasonable grounds to believe that a person resides in an issuing State could exist, in particular, where a person is registered as a resident in an issuing State, as indicated by holding an identity card or a residence permit or by being registered in an official residence register. In the absence of registration in the issuing State, residence could be indicated by the fact that a person has manifested the intention to settle in that Member State or has acquired, following a stable period of presence in that Member State, certain connections with that State which are of a similar degree as those resulting from establishing a formal residence in that Member State. In order to determine whether, in a specific situation, there are sufficient connections between the person concerned and the issuing State that give rise to reasonable grounds to believe that the person concerned resides in that State, various objective factors characterising the situation of that person could be taken into account, which include, in particular, the length, nature and conditions of the person's presence in the issuing State or the family ties or economic connections which that person has with that Member State. A registered vehicle, a bank account, the fact that the person's stay in the issuing State has been uninterrupted or other objective factors could be of relevance for determining that there are reasonable grounds to believe that the person concerned resides in the issuing State. A short visit, a holiday stay, including in a holiday home, or a similar stay in the issuing State without any further substantial link is not enough to establish a residence in that Member State. In cases where, at the time of issuing the European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in this Regulation, or to obtain content data, the issuing authority does not have reasonable grounds to believe that the person whose data are requested resides in the issuing State, the issuing authority should notify the enforcing authority.

(54) In order to provide for a swift procedure, the relevant point in time at which to determine whether there is a need to notify the enforcing authority should be the time when the European Production Order is issued. Any subsequent change of residence should not have any impact on the procedure. The person concerned should be able to invoke their rights as well as the rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media, during the entire criminal proceedings, and the enforcing authority should be able to raise a ground for refusal where, in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter. In addition, it should also be possible to invoke those grounds during the procedure for enforcement.

(55) A European Production Order should be transmitted through an EPOC, and a European Preservation Order should be transmitted through an EPOC-PR. Where needed, the EPOC or the EPOC-PR should be translated into an official language of the Union accepted by the addressee. Where no language has been specified by the service provider, the EPOC or the EPOC-PR should be translated into an official language of the Member State where the designated establishment or the legal representative of the service provider is located, or into another official language that the designated establishment or the legal representative of the service provider declared it will accept. Where a notification to the enforcing authority is required pursuant to this Regulation, the EPOC to be transmitted to that authority should be translated into an official language of the enforcing State or into another official language of the Union accepted by that State. In that regard, each Member State should be encouraged to state, at any time, in a written declaration submitted to the Commission if, and in which official language or languages of the Union in addition to the official language or languages of that Member State, they would accept translations of EPOCs and EPOC-PRs. The Commission should make such declarations available to all Member States and to the European Judicial Network.

(56) Where an EPOC has been issued and a notification to the enforcing authority is not required under this Regulation, the addressee should ensure, upon receipt of the EPOC, that the requested data are transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days following receipt of the EPOC. Where a notification to the enforcing authority is required pursuant to this Regulation, upon receipt of the EPOC, the service provider should act expeditiously to preserve the data. Where the enforcing authority has not raised any grounds for refusal pursuant to this

Regulation within 10 days following receipt of the EPOC, the addressee should ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the end of that 10-day period. Where the enforcing authority, already before the end of the 10-day period, confirms to the issuing authority and the addressee that it will not raise any grounds for refusal, the addressee should act as soon as possible upon such confirmation and at the latest at the end of that 10-day period. The shorter time limits applicable in emergency cases as defined in this Regulation should be respected by the addressee, and, where applicable, the enforcing authority. The addressee, and, where applicable, the enforcing authority, should execute the EPOC as soon as possible and at the latest within the deadlines set out in this Regulation, taking as full account as possible of the procedural deadlines and other deadlines indicated by the issuing State.

(57) Where the addressee considers, based solely on the information contained in the EPOC or in the EPOC-PR, that the execution of the EPOC or of the EPOC-PR could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State, the addressee should inform the issuing authority and the enforcing authority. As regards EPOCs, where no notification to the enforcing authority took place pursuant to this Regulation, the issuing authority should take the information received from the addressee into account, and should decide, on its own initiative or at the request of the enforcing authority, whether to withdraw, adapt or maintain the European Production Order. Where a notification to the enforcing authority took place pursuant to this Regulation, the issuing authority should take the information received from the addressee into account and decide whether to withdraw, adapt or maintain the European Production Order. It should also be possible for the enforcing authority to raise the grounds for refusal set out in this Regulation.

(58) In order to allow the addressee to address formal problems with an EPOC or an EPOC-PR, it is necessary to set out a procedure for the communication between the addressee and the issuing authority, as well as, where a notification to the enforcing authority took place pursuant to this Regulation, between the addressee and the enforcing authority, in cases where the EPOC or EPOC-PR is incomplete or contains manifest errors or does not contain sufficient information to execute the order concerned. Moreover, should the addressee not provide the information in an exhaustive or timely manner for any other reason, for example because it considers that there is a conflict with an obligation under the law of a third country, or because it considers that the European Production Order or the European Preservation Order has not been issued in accordance with the conditions set out by this Regulation, it should inform the issuing authority, as well as, where a notification to the enforcing authority took place, the enforcing authority, and provide the justification for not executing the EPOC or the EPOC-PR in a timely manner. The communication procedure should thus allow for the correction or reconsideration of the European Production Order or of the European Preservation Order by the issuing authority at an early stage. To guarantee the availability of the data requested, the addressee should preserve those data if that addressee can identify those data.

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

(60) Upon receipt of an EPOC-PR, the addressee should preserve the requested data for a maximum of 60 days unless the issuing authority confirms that a subsequent request for production has been issued, in which case the preservation should be continued. The issuing authority should be able to extend the duration of the preservation by an additional 30 days where necessary to allow for the issuing of a subsequent request for production, using the form set out in this Regulation. Where the issuing authority confirms during the period of preservation that a subsequent request for production has been issued, the addressee should preserve the data as long as necessary to produce the data once the subsequent request for production is received. Such a confirmation should be sent to the addressee within the relevant deadline, in an official language of the enforcing State or in any other language accepted by the addressee, using the form set out in this Regulation. To prevent the preservation from ceasing, it should be sufficient that the subsequent request for production has been issued and the confirmation has been sent by the issuing authority; it should not be necessary to complete further required formalities for the transmission, such as the translation of documents, at that point in time. Where the preservation is no longer necessary, the issuing authority should inform the addressee without undue delay and the obligation to preserve on the basis of the European Preservation Order should cease.

(61) Notwithstanding the principle of mutual trust, it should be possible for the enforcing authority to raise grounds for refusal of a European Production Order, where a notification to the enforcing authority took place pursuant to this Regulation, based on the list of grounds for refusal provided for in this Regulation. Where a notification to the enforcing authority, or enforcement, takes place in accordance with this Regulation, the enforcing State could provide under its national law that the execution of a European Production Order might require the procedural involvement of a court in the enforcing State.

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

(63) It should be possible for the enforcing authority, where it is notified pursuant to this Regulation, to refuse a European Production Order where the data requested are protected by immunities or privileges granted under the law of the enforcing State which prevent the execution or enforcement of the European Production Order, or where the data requested are covered by rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, which prevent the execution or enforcement of the European Production Order.

(64) It should be possible for the enforcing authority to refuse an order, in exceptional situations, where there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the European Production Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter. In particular, when assessing that ground for refusal, where the enforcing authority has at its disposal evidence or material such as that set out in a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission, adopted pursuant to Article 7(1) TEU, indicating that there is a clear risk, if the order were executed, of a serious breach of the fundamental right to an effective remedy and to a fair trial under Article 47 of the Charter, on account of systemic or generalised deficiencies concerning the independence of the issuing State's judiciary, the enforcing authority should determine specifically and precisely whether, having regard to the personal situation of the person concerned, as well as to the nature of the offence for which the criminal proceedings are conducted, and the factual context that forms the basis of the order, and in the light of the information provided by the issuing authority, there are substantial grounds for believing that there is a risk of a breach of a person's right to a fair trial.

(65) It should be possible for the enforcing authority to refuse an order where the execution of such order would be contrary to the principle of *ne bis in idem*.

(66) It should be possible for the enforcing authority, where it is notified pursuant to this Regulation, to refuse a European Production Order in the event that the conduct for which the order has been issued does not constitute an offence under the law of the enforcing State, unless it concerns an offence listed within the categories of offences set out in an annex to this Regulation, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years.

(67) Since informing the person whose data are requested is an essential element as regards data protection rights and defence rights, in that it enables effective review and judicial redress, in accordance with Article 6 TEU and the Charter, the issuing authority should inform the person whose data are being requested, without undue delay, about the production of data on the basis of a European Production Order. However, the issuing authority should be able, in accordance with national law, to delay or restrict informing or omit to inform the person whose data are being requested, to the extent that, and for as long as, the conditions of Directive (EU) 2016/680 are met, in which case the issuing authority should indicate in the case file the reasons for the delay, restriction or omission and add a short justification in the EPOC. The addressees and, if different, the service providers should take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.

(68) It should be possible for a service provider to claim reimbursement of its costs for responding to a European Production Order or to a European Preservation Order from the issuing State, if that possibility is provided for in the national law of the issuing State for domestic orders in similar situations, in accordance with the national law of that State. Member States should inform the Commission about their national rules for reimbursement, and the Commission should make them public. This Regulation provides for separate rules applicable to the reimbursement of costs related to the decentralised IT system.

(69) Without prejudice to national laws providing for the imposition of criminal penalties, Member States should lay down the rules on pecuniary penalties applicable to infringements of this Regulation and should take all measures necessary to ensure that they are implemented. Member States should ensure that pecuniary penalties provided for in their national law are effective, proportionate and dissuasive. Member States should, without delay, notify the Commission of those rules and of those measures and should notify it, without delay, of any subsequent amendment affecting them.

(70) When assessing in the individual case the appropriate pecuniary penalty, 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 has been held responsible for similar previous breaches and the financial strength of the service provider held liable. In exceptional circumstances, that assessment could lead the enforcing authority to decide to abstain from imposing any pecuniary penalties. In this respect, particular attention is to be given to microenterprises that fail to comply with a European Production Order or a European Preservation Order in an emergency case due to lack of human resources outside normal business hours, if the data are transmitted without undue delay.

(71) Without prejudice to data protection obligations, service providers should not be held liable in Member States for prejudice caused to their users or third parties exclusively resulting from compliance in good faith with an EPOC or an EPOC-PR. The responsibility for ensuring the legality of the order concerned, in particular its necessity and proportionality, should lie with the issuing authority.

(72) Where the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority, and, if applicable, where the enforcing authority has not invoked any of the grounds for refusal as provided for in this Regulation, it should be possible for the issuing authority to request the enforcing authority to enforce the European Production Order or the European Preservation Order. To that end, the issuing authority should transfer the order concerned, the relevant form provided for in this Regulation, as completed by the addressee, and any relevant document to the enforcing authority. The issuing authority should translate the order concerned and any document to be transferred into one of the languages accepted by the enforcing State and should inform the addressee of the transfer. That State should enforce the order concerned in accordance with its national law.

(73) The procedure for enforcement should allow the addressee to invoke grounds against the enforcement, based on a list of specific grounds provided for in this Regulation, including that the order concerned has not been issued or validated by a competent authority as provided for in this Regulation, or where the order does not concern data stored by or on behalf of the service provider at the time of receipt of the relevant certificate. The enforcing authority should be able to refuse to recognise and enforce a European Production Order or a European Preservation Order based on those same grounds, and also, in exceptional situations, on account of the manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter. The enforcing authority should consult the issuing authority before deciding not to recognise or not to enforce the order, based on those grounds. Where the addressee does not comply with its obligations under a recognised European Production Order or European Preservation Order the enforceability of which has been confirmed by the enforcing authority, that authority should impose a pecuniary penalty. That penalty should be proportionate, in particular in view of specific circumstances such as repeated or systemic non-compliance.

(74) Compliance with a European Production Order could conflict with an obligation under the applicable law of a third country. To ensure comity in respect of the sovereign interests of third countries, to protect the individual concerned and to address conflicting obligations on service providers, this Regulation provides for a specific mechanism for judicial review where compliance with a European Production Order would prevent a service provider from complying with legal obligations deriving from the law of a third country.

(75) Where an addressee considers that a European Production Order in a specific case would entail the violation of a legal obligation deriving from the law of a third country, it should inform the issuing authority and the enforcing authority of its reasons for not executing the order by way of a reasoned objection, using the form provided for in this Regulation. The issuing authority should review the European Production Order on the basis of the reasoned objection and any input provided by the enforcing State, taking into account the same criteria that the competent court of the issuing State would have to follow. Where the issuing authority intends to uphold the order, it should request a review by the competent court of the issuing State, as notified by the relevant Member State, which should review the order.

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

(77) Expertise on interpretation could also be provided through expert opinions where available. Information and case law on the interpretation of the law of a third country and on conflict of law procedures in Member States should be made available on a central platform such as the SIRIUS project or the European Judicial Network, with a view to making it possible to benefit from experience and expertise gathered on the same or similar questions. The availability of such information on a central platform should not prevent a renewed consultation of the third country where appropriate.

(78) When assessing whether conflicting obligations exist, the competent court should determine whether the law of the third country is applicable and, if so, whether the law of the third country prohibits disclosure of the data concerned. Where the competent court establishes that the law of the third country prohibits disclosure of the data concerned, that court should determine whether to uphold or lift 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 the disclosure of the data, and the possible consequences for the addressee or for the service provider of complying with the order. Particular importance and weight should be given to the protection of fundamental rights by the relevant law of the third country and other fundamental interests, such as national security interests of the third country, as well as the degree of connection between the criminal case and either of the two jurisdictions when conducting the assessment. Where the court decides to lift the order, it should inform the issuing authority and the addressee. If the competent court determines that the order is to be upheld, it should inform the issuing authority and the addressee, and that addressee should proceed with the execution of that order. The issuing authority should inform the enforcing authority about the outcome of the review procedure.

(79) The conditions set out in this Regulation for the execution of an EPOC should also be applicable in the event of conflicting obligations deriving from the law of a third country. Therefore, during the judicial review, where compliance with a European Production Order would prevent service providers from complying with a legal obligation deriving from the law of a third country, the data requested by that order should be preserved. Where, following the judicial review, the competent court decides to lift a European Production Order, it should be possible to issue a European Preservation Order to allow the issuing authority to seek production of the data through other channels, such as mutual legal assistance.

(80) It is essential that all persons whose data are requested in criminal investigations or proceedings have access to an effective legal remedy, in line with Article 47 of the Charter. In line with that requirement and without prejudice to further legal remedies available in accordance with national law, any person whose data were requested via a European Production Order should have the right to effective remedies against that order. Where that person is a suspect or an accused person, such person should have the right to effective remedies during the criminal proceedings in which the data are being used as evidence. The right to effective remedies should be exercised before a court in the issuing State in accordance with its national law and should include the possibility of challenging the legality of the measure, including its necessity and proportionality, without prejudice to the guarantees of fundamental rights in the enforcing State, or other additional remedies in accordance with national law. This Regulation should not limit the possible grounds for challenging the legality of an order. The right to effective remedies provided for in this Regulation should be without prejudice to the right to seek remedies under Regulation (EU) 2016/679 and Directive (EU) 2016/680. Information should be provided in due time about the possibilities under national law for seeking remedies and it should be ensured that they can be exercised effectively.

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

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

(83) The decentralised IT system should comprise the IT systems of Member States and the Union agencies and bodies, and interoperable access points, through which those IT systems are interconnected. The access points of the decentralised IT system should be based on the e-CODEX system, established by Regulation (EU) 2022/850 of the European Parliament and of the Council ([24]).

(84) Service providers who make use of bespoke IT solutions for the purposes of exchanging information and data related to requests for electronic evidence should be provided with automated means of accessing the decentralised IT systems by means of a common data exchange standard.

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

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

(87) The use of mechanisms to ensure authenticity, as provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council ([25]), should be considered.

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

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

(90) The Commission should be responsible for the creation, maintenance and development of the reference implementation software. The Commission should design, develop and maintain the reference implementation software in compliance with the data protection requirements and principles laid down in Regulation (EU) 2018/1725 of the European Parliament and of the Council ([26]), Regulation (EU) 2016/679, and Directive (EU) 2016/680, in particular the principles of data protection by design and by default as well as a high level of cybersecurity. It is important that the reference implementation software also include appropriate technical measures and make it possible to take the organisational measures necessary for ensuring an appropriate level of security and interoperability.

([24]) Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 1.6.2022, p. 1).

([25]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

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

(91) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([27]).

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

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

(94) The use of pre-translated and standardised forms would facilitate cooperation and the exchange of information under this Regulation, thereby allowing for quicker and more effective communication in a user-friendly manner. Such forms would reduce translation costs and contribute to a high-quality standard of communication. Response forms would similarly make a standardised exchange of information possible, in particular where service providers are unable to comply because the user account does not exist or because no data are available. The forms provided for in this Regulation would also facilitate the gathering of statistics.

(95) In order to effectively address a possible need for improvements regarding the content of the EPOC and EPOC-PR forms and of the forms to be used for providing information on the impossibility of executing an EPOC or an EPOC-PR, for confirming the issuance of a request for production following a European Preservation Order and for extending the preservation of electronic evidence, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in respect of the amendment of the forms provided for in this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([28]). 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.

(96) This Regulation should not affect Union or other international instruments, agreements and arrangements on the gathering of evidence that falls within the scope of this Regulation. Member States' authorities should choose the tool most adapted to the case at hand. In some cases, they might prefer to use Union and other international instruments, agreements and arrangements when requesting a set of different types of investigative measures that are not limited to the production of electronic evidence from another Member State. Member States should notify the Commission at the latest three years after the entry into force of this Regulation of the existing instruments, agreements and arrangements referred to in this Regulation which they will continue to apply. Member States should also notify the Commission within three months of the signing of any new agreement or arrangement as referred to in this Regulation.

(97) Given technological developments, new forms of communication tools could prevail in a few years, or gaps could emerge in the application of this Regulation. It is therefore important to provide for an evaluation of its application.

(98) The Commission should carry out an evaluation of this Regulation that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU added value, and that evaluation should provide the basis for impact assessments of possible further measures. The evaluation report should include an assessment of the application of this Regulation and of the results that have been achieved with regard to its objectives, as well as an assessment of this Regulation's impact on fundamental rights. The Commission should collect information regularly in order to inform the evaluation of this Regulation.

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

([28]) OJ L 123, 12.5.2016, p. 1.

(99) Since the objective of this Regulation, namely to improve the securing and obtaining of 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 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(100) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, Ireland has notified its wish to take part in the adoption and application of this Regulation.

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

(102) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 6 November 2019 ([29]),

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter

1. This Regulation lays down the rules under which an authority of a Member State, in criminal proceedings, may issue a European Production Order or a European Preservation Order and thereby order a service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of the data.

This Regulation is without prejudice to the powers of national authorities to address service providers established or represented on their territory for the purpose of ensuring that they comply with national measures similar to those referred to in the first subparagraph.

2. The issuing of a European Production Order or of a European Preservation Order may also be requested by a suspect or an accused person, or by a lawyer on that person's behalf within the framework of applicable defence rights in accordance with national criminal procedural law.

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

Article 2

Scope

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

2. European Production Orders and European Preservation Orders may be issued only in the framework and for the purposes of criminal proceedings, and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice. Such orders may also be issued in proceedings relating to a criminal offence for which a legal person could be held liable or punished in the issuing State.

3. European Production Orders and European Preservation Orders may be issued only for data pertaining to the services referred to in Article 3, point (3), offered in the Union.

4. This Regulation does not apply to proceedings initiated for the purpose of providing mutual legal assistance to another Member State or a third country.

([29]) OJ C 32, 31.1.2020, p. 11.

Article 3

Definitions

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

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

(2) 'European Preservation Order' means a decision which orders the preservation of electronic evidence for the purposes of a subsequent request for production, and which is issued or validated by a judicial authority of a Member State in accordance with Article 4(3), (4) and (5), and addressed to a designated establishment or to a legal representative of a service provider offering services in the Union, where that designated establishment or legal representative is located in another Member State bound by this Regulation;

(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 as referred to in Article 2(2), point (b), of Directive 2006/123/EC of the European Parliament and of the Council ([30]):

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

(b) internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services;

(c) other information society services as referred to in Article 1(1), point (b), of Directive (EU) 2015/1535 that:

(i) enable their users to communicate with each other; or

(ii) make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user;

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

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

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

(5) 'establishment' means an entity that actually pursues an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or the business is managed;

(6) 'designated establishment' means an establishment with legal personality designated in writing by a service provider established in a Member State taking part in a legal instrument referred to in Article 1(2) of Directive (EU) 2023/1544, for the purposes referred to in Article 1(1) and Article 3(1) of that Directive;

(7) 'legal representative' means a natural or legal person appointed in writing by a service provider not established in a Member State taking part in a legal instrument referred to in Article 1(2) of Directive (EU) 2023/1544, for the purposes referred to in Article 1(1) and Article 3(1) of that Directive;

(8) 'electronic evidence' means subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form, at the time of the receipt of a European Production Order Certificate (EPOC) or of a European Preservation Order Certificate (EPOC-PR);

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

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

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

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

(10) 'data requested for the sole purpose of identifying the user' means IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation;

(11) 'traffic data' means data related to the provision of a service offered by a service provider which serve to provide context or additional information about such service and are 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, the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, and other electronic communications metadata and data, other than subscriber data, relating to the commencement and termination of a user access session to a service, such as the date and time of use, the log-in to and log-off from the service;

(12) 'content data' means any data in a digital format, such as text, voice, videos, images and sound, other than subscriber data or traffic data;

(13) 'information system' means an information system as defined in Article 2, point (a), of Directive 2013/40/EU of the European Parliament and of the Council ([31]);

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

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

(16) 'enforcing State' means the Member State in which the designated establishment is established or the legal representative resides and to which a European Production Order and an EPOC or a European Preservation Order and an EPOC-PR are transmitted by the issuing authority for notification or for enforcement in accordance with this Regulation;

(17) 'enforcing authority' means the authority in the enforcing State, which, in accordance with the national law of that State, is competent to receive a European Production Order and an EPOC or a European Preservation Order and an EPOC-PR transmitted by the issuing authority for notification or for enforcement in accordance with this Regulation;

(18) 'emergency case' means a situation in which there is an imminent threat to the life, physical integrity or safety of a person, or to a critical infrastructure, as defined in Article 2, point (a), of Directive 2008/114/EC, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State;

(19) 'controller' means controller as defined in Article 4, point (7), of Regulation (EU) 2016/679;

(20) 'processor' means processor as defined in Article 4, point (8), of Regulation (EU) 2016/679;

([31]) 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).

(21) 'decentralised IT system' means a network of IT systems and interoperable access points, operating under the individual responsibility and management of each Member State, Union agency or body, which enables the cross-border exchange of information to take place in a secure and reliable manner.

CHAPTER II

EUROPEAN PRODUCTION ORDER, EUROPEAN PRESERVATION ORDER AND CERTIFICATES

Article 4

Issuing authority

1. A European Production Order to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user, as defined in Article 3, point (10), may be issued only by:

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

(b) any other competent authority as defined by the issuing State which, in the case concerned, 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; in such a case, the European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.

2. A European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or to obtain 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 case concerned, 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; in such a case, the European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court or an investigating judge in the issuing State.

3. A European Preservation Order for data of any category may be issued only by:

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

(b) any other competent authority as defined by the issuing State which, in the case concerned, 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; in such a case, the European Preservation Order shall be validated, after examination of its conformity with the conditions for issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.

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

5. In a validly established emergency case, as defined in Article 3, point (18), the competent authorities referred to in paragraph 1, point (b), and in paragraph 3, point (b), of this Article may exceptionally issue a European Production Order for subscriber data or for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or a European Preservation Order, without prior validation of the order concerned, where validation cannot be obtained in time and where those authorities could issue an order in a similar domestic case without prior validation. The issuing authority shall seek *ex post* validation of the order concerned without undue delay, at the latest within 48 hours. Where such *ex post* validation of the order concerned is not granted, the issuing authority shall withdraw the order immediately and shall delete or otherwise restrict the use of any data that were obtained.

6. Each Member State may designate one or more central authorities to be responsible for the administrative transmission of EPOCs and EPOC-PRs, of European Production Orders and European Preservation Orders and of notifications, and for the receipt of data and notifications as well as for the transmission of other official correspondence relating to such certificates or orders.

Article 5

Conditions for issuing a European Production Order

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

2. A European Production Order shall be necessary for and proportionate to the purpose of the proceedings referred to in Article 2(3), taking into account the rights of the suspect or the accused person, and may only be issued if a similar order could have been issued under the same conditions in a similar domestic case.

3. A European Production Order to obtain subscriber data or to obtain data requested for the sole purpose of identifying the user as defined in Article 3, point (10), may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.

4. A European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), of this Regulation or to obtain content data shall only be issued:

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

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

(i) offences as defined in Articles 3 to 8 of Directive (EU) 2019/713 of the European Parliament and of the Council ([32]);

(ii) offences as defined in Articles 3 to 7 of Directive 2011/93/EU;

(iii) offences as defined in Articles 3 to 8 of Directive 2013/40/EU;

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

(d) for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice, for criminal offences referred to in points (a), (b) and (c) of this paragraph.

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

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

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

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

(d) the requested data category as defined in Article 3, points (9) to (12);

(e) if applicable, the time range of the data for which production is requested;

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

(g) in emergency cases as defined in Article 3, point (18), the duly justified reasons for the emergency;

(h) in cases where the European Production Order is directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, a confirmation that the conditions set out in paragraph 6 of this Article are met;

(i) the grounds for determining that the European Production Order fulfils the conditions of necessity and proportionality under paragraph 2 of this Article;

(j) a summary description of the case.

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

6. A European Production Order shall be addressed to the service provider acting as controller in accordance with Regulation (EU) 2016/679.

By way of exception, the European Production Order may be directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, where:

(a) the controller cannot be identified despite reasonable efforts on the part of the issuing authority; or

(b) addressing the controller might be detrimental to the investigation.

7. In accordance with Regulation (EU) 2016/679, the processor that stores or otherwise processes the data on behalf of the controller shall inform the controller about the production of the data unless the issuing authority has requested the service provider to refrain from informing the controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. In that case, the issuing authority shall indicate in the case file the reasons for the delay in informing the controller. A short justification shall also be added in the EPOC.

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

9. In cases where data protected by professional privilege under the law of the issuing State are stored or otherwise processed by a service provider as part of an infrastructure provided to professionals covered by professional privilege ('privileged professional'), in their business capacity, a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or to obtain content data may only be issued:

(a) where the privileged professional resides in the issuing State;

(b) where addressing the privileged professional might be detrimental to the investigation; or

(c) where the privileges were waived in accordance with the applicable law.

10. If the issuing authority has reasons to believe that the traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or the content data requested by the European Production Order are protected by immunities or privileges granted under the law of the enforcing State, or that those data are subject in that State to rules on determination and limitation of criminal liability relating to freedom of the press or freedom of expression in other media, the issuing authority may seek clarification before issuing the European Production Order, including by consulting the competent authorities of the enforcing State, either directly or via Eurojust or the European Judicial Network.

The issuing authority shall not issue a European Production Order if it finds that the requested traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or the content data are protected by immunities or privileges granted under the law of the enforcing State, or that those data are subject in that State to rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media.

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(8) shall apply *mutatis mutandis*.

2. A European Preservation Order shall be necessary for and proportionate to the purpose of preventing the removal, deletion or alteration of data with a view to issuing a subsequent request for production of those data via mutual legal assistance, a European Investigation Order (EIO) or a European Production Order, taking into account the rights of the suspect or the accused person.

3. A European Preservation Order may be issued for all criminal offences, if it could have been issued under the same conditions in a similar domestic case, and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.

4. A European Preservation Order shall include the following information:

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

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

(c) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, login ID or account name to determine the data for which preservation is requested;

(d) the requested data category as defined in Article 3, points (9) to (12);

(e) if applicable, the time range of the data for which preservation is requested;

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

(g) the grounds for determining that the European Preservation Order fulfils the conditions of necessity and proportionality under paragraph 2 of this Article.

Article 7

Addressees of European Production Orders and European Preservation Orders

1. European Production Orders and European Preservation Orders shall be addressed directly to a designated establishment or to a legal representative of the service provider concerned.

2. Exceptionally, in emergency cases as defined in Article 3, point (18), where the designated establishment or the legal representative of a service provider does not react to an EPOC or an EPOC-PR within the deadlines, that EPOC or EPOC-PR may be addressed to any other establishment or legal representative of the service provider in the Union.

Article 8

Notification to the enforcing authority

1. Where a European Production Order is issued to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 3, point (10), or to obtain content data, the issuing authority shall notify the enforcing authority by transmitting the EPOC to that authority at the same time as it transmits the EPOC to the addressee in accordance with Article 9(1) and (2).

2. Paragraph 1 shall not apply if, at the time of issuing the order, the issuing authority has reasonable grounds to believe that:

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

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

3. When transmitting the EPOC as referred to in paragraph 1 of this Article to the enforcing authority, the issuing authority shall, where appropriate, include any additional information that could be needed for the evaluation of the possibility of raising a ground for refusal in accordance with Article 12.

4. The notification to the enforcing authority referred to in paragraph 1 of this Article shall have a suspensive effect on the obligations of the addressee as set out in Article 10(2), except in emergency cases as defined in Article 3, point (18).

Article 9

European Production Order Certificate (EPOC) and European Preservation Order Certificate (EPOC-PR)

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

The issuing authority or, where applicable, the 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 that its content is accurate and correct.

2. An EPOC shall contain the information listed in Article 5(5), points (a) to (h), including sufficient information to allow the addressee to identify and contact the issuing authority and the enforcing authority, if necessary.

Where a notification to the enforcing authority is required pursuant to Article 8, the EPOC transmitted to that authority shall contain the information listed in Article 5(5), points (a) to (j).

3. An EPOC-PR shall contain the information listed in Article 6(4), points (a) to (f), including sufficient information to allow the addressee to identify and contact the issuing authority.

4. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the Union accepted by the addressee as provided for in Article 4 of Directive (EU) 2023/1544. Where no language has been specified by the service provider, the EPOC or the EPOC-PR shall be translated into an official language of the Member State where the designated establishment or the legal representative of the service provider is located.

Where a notification to the enforcing authority is required pursuant to Article 8, the EPOC to be transmitted to that authority shall be translated into an official language of the enforcing State or into another official language of the Union accepted by that State.

Article 10

Execution of an EPOC

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

2. Where a notification to the enforcing authority is required pursuant to Article 8 and that authority has not raised any ground for refusal in accordance with Article 12 within 10 days following receipt of the EPOC, the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities, as indicated in the EPOC, at the end of that 10-day period. Where the enforcing authority already before the end of that 10-day period confirms to the issuing authority and the addressee that it will not raise any ground for refusal, the addressee shall act as soon as possible upon such confirmation and at the latest at the end of that 10-day period.

3. Where a notification to the enforcing authority is not required pursuant to Article 8, upon receipt of an EPOC, the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities, as indicated in the EPOC, at the latest within 10 days following receipt of the EPOC.

4. In emergency cases, the addressee shall transmit the requested data without undue delay, at the latest within eight hours following receipt of the EPOC. Where a notification to the enforcing authority is required pursuant to Article 8, the enforcing authority may, if it decides to raise a ground for refusal in accordance with Article 12(1), without delay and at the latest within 96 hours following receipt of the notification, notify the issuing authority and the addressee that it objects to the use of the data or that the data may only be used under conditions which it shall specify. Where a ground for refusal is raised by the enforcing authority, if the data have already been transmitted by the addressee to the issuing authority, the issuing authority shall delete or otherwise restrict the use of the data or, in the event that the enforcing authority has specified conditions, the issuing authority shall comply with those conditions when using the data.

5. Where the addressee considers, based solely on the information contained in the EPOC, that the execution of the EPOC could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State, the addressee shall inform the issuing authority and the enforcing authority using the form set out in Annex III.

Where no notification to the enforcing authority took place pursuant to Article 8, the issuing authority shall take the information referred to in the first subparagraph of this paragraph into account, and shall decide, on its own initiative or at the request of the enforcing authority, whether to withdraw, adapt or maintain the European Production Order.

Where a notification to the enforcing authority took place pursuant to Article 8, the issuing authority shall take the information referred to in the first subparagraph of this paragraph into account, and shall decide whether to withdraw, adapt or maintain the European Production Order. The enforcing authority may decide to raise the grounds for refusal set out in Article 12.

6. Where the addressee cannot comply with its obligation to produce the requested data because the EPOC is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC, the addressee shall, without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the EPOC, and seek clarification, using the form set out in Annex III. At the same time, the addressee shall inform the issuing authority of whether identification of the data requested and preservation of those data as set out in paragraph 9 of this Article was possible.

The issuing authority shall react expeditiously and at the latest within five days following receipt of the form. The addressee shall ensure that it can receive the necessary clarification or any correction provided by the issuing authority, in order for the addressee to fulfil its obligations set out in paragraphs 1 to 4. The obligations set out in paragraphs 1 to 4 shall not apply until such clarification or correction is provided by the issuing authority or the enforcing authority.

7. Where the addressee cannot comply with its obligation to produce the requested data because of a *de facto* impossibility due to circumstances not attributable to the addressee, the addressee shall, without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the EPOC, explaining the reasons for such a *de facto* impossibility, using the form set out in Annex III. Where the issuing authority concludes that there is such a *de facto* impossibility, it shall inform the addressee, and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority, that the EPOC no longer needs to be executed.

8. In all cases where the addressee does not provide the requested data, does not provide the requested data exhaustively or does not provide the requested data within the specified deadline, for reasons other than those referred to in paragraphs 5, 6 and 7 of this Article, the addressee shall, without undue delay and at the latest within the deadlines set out in paragraphs 2, 3 and 4 of this Article, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the EPOC, of those reasons using the form set out in Annex III. The issuing authority shall review the European Production Order in light of the information provided by the addressee and, if necessary, set a new deadline for the addressee to produce the data.

9. The data shall be preserved, to the extent possible, until they are produced, irrespective of whether the production is ultimately requested on the basis of a clarified European Production Order and its EPOC or through other channels, such as mutual legal assistance, or until the European Production Order is withdrawn.

Where the production of data and their preservation are no longer necessary, the issuing authority and, where applicable pursuant to Article 16(8), the enforcing authority shall inform the addressee without undue delay.

Article 11

Execution of an EPOC-PR

1. Upon receipt of an EPOC-PR, the addressee shall, without undue delay, preserve the data requested. The obligation to preserve the data shall cease after 60 days, unless the issuing authority confirms, using the form set out in Annex V, that a subsequent request for production has been issued. During that 60-day period, the issuing authority may, using the form set out in Annex VI, extend the duration of the obligation to preserve the data by an additional 30-day period, where necessary to allow for the issuing of a subsequent request for production.

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

3. Where the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay and the obligation to preserve on the basis of the relevant European Preservation Order shall cease.

4. Where the addressee considers, based solely on the information contained in the EPOC-PR, that the execution of the EPOC-PR could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State, the addressee shall inform the issuing authority and the enforcing authority using the form set out in Annex III.

The issuing authority shall take the information referred to in the first subparagraph into account, and shall decide, on its own initiative or at the request of the enforcing authority, whether to withdraw, adapt or maintain the European Preservation Order.

5. Where the addressee cannot comply with its obligation to preserve the requested data because the EPOC-PR is incomplete, contains manifest errors or does not contain sufficient information to execute the EPOC-PR, the addressee shall, without undue delay, inform the issuing authority referred to in the EPOC-PR and seek clarification, using the form set out in Annex III.

The issuing authority shall react expeditiously and at the latest within five days of the receipt of the form. The addressee shall ensure that it can receive the necessary clarification or any correction provided by the issuing authority in order for the addressee to fulfil its obligations set out in paragraphs 1, 2 and 3. In the absence of a reaction from the issuing authority within the five-day period, the service provider shall be exempt from the obligations set out in paragraphs 1 and 2.

6. Where the addressee cannot comply with its obligation to preserve the requested data because of a *de facto* impossibility due to circumstances not attributable to the addressee, the addressee shall, without undue delay, inform the issuing authority referred to in the EPOC-PR explaining the reasons for such *de facto* impossibility, using the form set out in Annex III. Where the issuing authority concludes that such impossibility does exist, it shall inform the addressee that the EPOC-PR no longer needs to be executed.

7. In all cases where the addressee does not preserve the requested data, for reasons other than those referred to in paragraphs 4, 5 and 6, the addressee shall, without undue delay, inform the issuing authority of those reasons, using the form set out in Annex III. The issuing authority shall review the European Preservation Order in light of the justification provided by the addressee.

Article 12

Grounds for refusal of European Production Orders

1. Where the issuing authority has notified the enforcing authority pursuant to Article 8, and without prejudice to Article 1(3), the enforcing authority shall, as soon as possible but at the latest within 10 days following receipt of the notification, or, in emergency cases, at the latest within 96 hours following such receipt, assess the information set out in the order and, where appropriate, raise one or more of the following grounds for refusal:

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

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

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

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

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

3. Before deciding to raise a ground for refusal, the enforcing authority notified pursuant to Article 8 shall contact the issuing authority by any appropriate means, in order to discuss the appropriate measures to take. On that basis, the issuing authority may decide to adapt or to withdraw the European Production Order. Where, following such discussions, no solution is reached, the enforcing authority notified pursuant to Article 8 may decide to raise grounds for refusal of the European Production Order and inform the issuing authority and the addressee accordingly.

4. Where the enforcing authority decides to raise grounds for refusal pursuant to paragraph 1, it may indicate whether it objects to the transfer of all data requested in the European Production Order or whether the data may only be partly transferred or used under conditions specified by the enforcing authority.

5. Where the power to waive the immunity or privilege as set out in paragraph 1, point (a), of this Article, lies with an authority of the enforcing State, the issuing authority may request the enforcing authority notified pursuant to Article 8 to contact that authority of the enforcing State to request it to exercise that power without delay. Where the power to waive the immunity or privilege lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.

Article 13

User information and confidentiality

1. The issuing authority shall, without undue delay, inform the person whose data are being requested about the production of data on the basis of a European Production Order.

2. The issuing authority may, in accordance with the national law of the issuing State, delay or restrict informing, or omit to inform, the person whose data are being requested, to the extent that, and for as long as, the conditions in Article 13(3) of Directive (EU) 2016/680 are met, in which case the issuing authority shall indicate in the case file the reasons for the delay, restriction or omission. A short justification shall also be added in the EPOC.

3. When informing the person whose data are being requested as referred to in paragraph 1 of this Article, the issuing authority shall include information about available remedies pursuant to Article 18.

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

Article 14

Reimbursement of costs

1. The service provider may claim reimbursement of its costs from the issuing State, if that possibility is provided for in the national law of the issuing State for domestic orders in similar situations, in accordance with the national law of that State. Member States shall inform the Commission about their national rules for reimbursement, and the Commission shall make them public.

2. This Article shall not apply to the reimbursement of costs of the decentralised IT system as referred to in Article 25.

CHAPTER III

PENALTIES AND ENFORCEMENT

Article 15

Penalties

1. Without prejudice to national laws providing for the imposition of criminal penalties, Member States shall lay down rules on pecuniary penalties applicable to infringements of Articles 10 and 11 and Article 13(4), in accordance with Article 16(10), and shall take all measures necessary to ensure that they are implemented. The pecuniary penalties provided for shall be effective, proportionate and dissuasive. Member States shall ensure that pecuniary penalties of up to 2 % of the total worldwide annual turnover of the service provider's preceding financial year can be imposed. 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.

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

Article 16

Procedure for enforcement

1. Where the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority, and, if applicable, where the enforcing authority has not invoked any of the grounds for refusal as provided for in Article 12, the issuing authority may request the enforcing authority to enforce the European Production Order or the European Preservation Order.

For the purpose of enforcement as referred to in the first subparagraph, the issuing authority shall transfer the order concerned, the form set out in Annex III as completed by the addressee, and any relevant document in accordance with Article 19. The issuing authority shall translate the order concerned and any document to be transferred into one of the languages accepted by the enforcing State and shall inform the addressee of the transfer.

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

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

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

The enforcing authority shall take the decision on the recognition of the order concerned without undue delay and no later than five working days after the receipt of that order.

3. The enforcing authority shall formally require the addressee to comply with their relevant obligations, and shall inform the addressee of the following:

(a) the possibility of objecting to the execution of the order concerned by invoking one or more of the grounds listed in paragraph 4, points (a) to (f), or in paragraph 5, points (a) to (e);

(b) the applicable penalties in the event of non-compliance; and

(c) the deadline for compliance or objection.

4. Enforcement of the European Production Order may only be denied on the basis of one or more of the following grounds:

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

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

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

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

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

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

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

5. The enforcement of the European Preservation Order may only be denied on the basis of one or more of the following grounds:

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

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

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

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

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

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

6. In the event of an objection by the addressee as referred to in paragraph 3, point (a), the enforcing authority shall decide whether or not to enforce the European Production Order or the European Preservation Order on the basis of any 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 not to enforce the European Production Order or the European Preservation Order in accordance with paragraph 2 or 6, respectively, 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 five working days.

8. The enforcing authority shall notify all of its decisions immediately to the issuing authority and to the addressee.

9. If the enforcing authority obtains the data requested by a European Production Order from the addressee, it shall transmit those data to the issuing authority without undue delay.

10. Where the addressee does not comply with its obligations under a recognised European Production Order or European Preservation Order the enforceability of which has been confirmed by the enforcing authority, that authority shall impose a pecuniary penalty in accordance with Article 15. An effective judicial remedy shall be available against a decision to impose a pecuniary penalty.

CHAPTER IV

CONFLICTS OF LAW AND REMEDIES

Article 17

Review procedure in the event of conflicting obligations

1. Where an addressee considers that compliance with a European Production Order would conflict with an obligation under the applicable law of a third country, it shall inform the issuing authority and the enforcing authority of its reasons for not executing the European Production Order, in accordance with the procedure set out in Article 10(8) and (9) using the form set out in Annex III ('the reasoned objection').

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. The reasoned objection shall not be based on:

(a) the fact that similar provisions concerning the conditions, formalities and procedures for issuing an order for production do not exist in the applicable law of the third country; or

(b) the sole fact that the data are stored in a third country.

The reasoned objection shall be filed no later than 10 days after the date on which the addressee received the EPOC.

3. The issuing authority shall review the European Production Order on the basis of the reasoned objection and any input provided by the enforcing State. Where the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court of the issuing State. The execution of the European Production Order shall be suspended pending completion of the review procedure.

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

(a) the law of the third country is applicable based on the specific circumstances of the case in question; and

(b) the law of the third country, if applicable as referred to in point (a), prohibits disclosure of the data concerned when applied to the specific circumstances of the case in question.

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

6. Where the competent court establishes, based on the examination pursuant to paragraph 4, point (b), that the law of the third country prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or lift the European Production Order. That assessment shall in particular be based on the following factors, while giving particular weight to the factors referred to in points (a) and (b):

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

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

(i) the location, nationality and place of residence of the person whose data are being requested or of the victim or victims of the criminal offence in question;

(ii) the place where the criminal offence in question was committed;

(c) the degree of connection between the service provider and the third country in question; in this context, the data storage location alone shall not suffice for the purpose of 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 for the service provider of complying with the European Production Order, including the potential penalties.

7. The competent court may request information from the competent authority of the third country, taking into account Directive (EU) 2016/680, in particular Chapter V thereof, and to the extent that such request does not obstruct the relevant criminal proceedings. Information shall, in particular, be requested from the competent authority of the third country by the issuing State where the conflict of obligations concerns fundamental rights or other fundamental interests of the third country related to national security and defence.

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

9. For the purposes of the procedures under this Article, the time limits shall be calculated in accordance with the national law of the issuing authority.

10. The issuing authority shall inform the enforcing authority about the outcome of the review procedure.

Article 18

Effective remedies

1. Without prejudice to further legal remedies available in accordance with national law, any person whose data were requested via a European Production Order shall have the right to effective remedies against that order. Where that person is a suspect or an accused person, such person shall have the right to effective remedies during the criminal proceedings in which the data were being used. The right to effective remedies referred to in this paragraph shall be without prejudice to the right to seek remedies under Regulation (EU) 2016/679 and Directive (EU) 2016/680.

2. The right to effective remedies shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility of challenging the legality of the measure, including its necessity and proportionality, without prejudice to the guarantees of fundamental rights in the enforcing State.

3. For the purposes of Article 13(1), information shall be provided in due time about the possibilities under national law for seeking remedies and it shall be ensured that they can be exercised effectively.

4. The same time limits or other conditions for seeking remedies in similar domestic cases shall apply for the purposes of this Regulation and in a way that guarantees that the persons concerned can exercise their right to those remedies effectively.

5. Without prejudice to national procedural rules, the issuing State and any other Member State to which electronic evidence has been transmitted under this Regulation shall ensure that the rights of defence and fairness of the proceedings are respected when assessing evidence obtained through the European Production Order.

CHAPTER V

DECENTRALISED IT SYSTEM

Article 19

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

1. Written communication between competent authorities and designated establishments or legal representatives under this Regulation, including the exchange of forms provided for in this Regulation and the data requested under a European Production Order or a European Preservation Order, shall be carried out through a secure and reliable decentralised IT system ('the decentralised IT system').

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

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

4. Written communication between competent authorities under this Regulation, including the exchange of forms provided for in this Regulation, and of the requested data under the procedure for enforcement as provided for in Article 16, as well as written communication with competent Union agencies or bodies, shall be carried out through the decentralised IT system.

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

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

Article 20

Legal effects of electronic documents

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

Article 21

Electronic signatures and seals

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

2. Where a document transmitted as part of the electronic communication under Article 19(1) or (4) of this Regulation requires a seal or a signature in accordance with this Regulation, the document shall feature a qualified electronic seal or qualified electronic signature as defined in Regulation (EU) No 910/2014.

Article 22

Reference implementation software

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

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

Article 23

Costs of the decentralised IT system

1. Each Member State shall bear the costs of the installation, operation and maintenance of the access points of the decentralised IT system for which that Member State is responsible.

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

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

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

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

Article 24

Transition period

Before the obligation to carry out written communication through the decentralised IT system referred to in Article 19 becomes applicable ('transition period'), the written communication between competent authorities and designated establishments or legal representatives under this Regulation shall take place by the most appropriate alternative means, taking into account the need to ensure a swift, secure and reliable exchange of information. Where service providers, Member States or Union agencies or bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement authorities and judicial authorities, issuing authorities may also choose to transmit an EPOC or an EPOC-PR via those channels to designated establishments or legal representatives during the transition period.

Article 25

Implementing acts

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

(a) the technical specifications defining the methods of communication by electronic means for the purposes of the decentralised IT system;

(b) the technical specifications for communication protocols;

(c) the information security objectives and relevant technical measures ensuring minimum information security standards and a high level of cybersecurity for the processing and communication of information within the decentralised IT system;

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

2. The implementing acts referred to in paragraph 1 of this Article shall be adopted in accordance with the examination procedure referred to in Article 26.

3. The implementing acts referred to in paragraph 1 shall be adopted by 18 August 2025.

Article 26

Committee procedure

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

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

CHAPTER VI

FINAL PROVISIONS

Article 27

Languages

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

Article 28

Monitoring and reporting

1. By 18 August 2026, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the means by which and the intervals at which the data will be collected. It shall specify the action to be taken by the Commission and by the Member States in collecting and analysing the data.

2. In any event, from 18 August 2026, Member States shall collect from the relevant authorities comprehensive statistics and keep a record of such statistics. The data collected for the preceding calendar year shall be sent to the Commission each year by 31 March, and shall include:

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

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

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

(d) the number of notifications to enforcing authorities pursuant to Article 8, and the number of EPOCs that were refused, by the type of data requested, the addressees, the situation (emergency case or not) and the ground for refusal raised;

(e) for fulfilled EPOCs, the average period between the moment the EPOC was issued and the moment the data requested were obtained, by the type of data requested, the addressees and the situation (emergency case or not);

(f) for fulfilled EPOC-PRs, the average period between the moment the EPOC-PR was issued and the moment the subsequent request for production was issued, by the type of data requested and the addressees;

(g) the number of European Production Orders or European Preservation Orders transmitted to and received by an enforcing State for enforcement, by the type of data requested, the addressees and the situation (emergency case or not) and the number of such orders fulfilled;

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

(i) the number of cases where *ex post* validation in accordance with Article 4(5) was not granted;

(j) an overview of the costs claimed by service providers in relation to the execution of EPOCs or EPOC-PRs and the costs reimbursed by the issuing authorities.

3. From 18 August 2026, for the data exchanges carried out via the decentralised IT system pursuant to Article 19(1), the statistics referred to in paragraph 2 of this Article may be programmatically collected by national portals. The reference implementation software referred to in Article 22 shall be technically equipped to provide for such functionality.

4. Service providers may collect, keep a record of and publish statistics in accordance with existing data protection principles. If any such statistics are collected for the preceding calendar year, they may be sent to the Commission by 31 March and may, as far as possible, include:

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

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

(c) for fulfilled EPOCs, the average period needed to provide the requested data from the moment the EPOC was received to the moment the data were provided, by the type of data requested, the issuing State and the situation (emergency case or not);

(d) for fulfilled EPOC-PRs, the average period between the moment the EPOC-PR was issued and the moment the subsequent request for production was issued, by the type of data requested and the issuing State.

5. From 18 August 2027, the Commission shall, by 30 June each year, publish a report containing the data referred to in paragraphs 2 and 3 in a compiled form, subdivided into Member States and type of service provider.

Article 29

Amendments to the certificates and the forms

The Commission shall adopt delegated acts in accordance with Article 30 to amend Annexes I, II, III, V and VI in order to effectively address a possible need for improvements regarding the content of the EPOC and EPOC-PR forms and of the forms to be used for providing information on the impossibility of executing an EPOC or an EPOC-PR, for confirming the issuance of a request for production following a European Preservation Order and for extending the preservation of electronic evidence.

Article 30

Exercise of the delegation

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

2. The power to adopt delegated acts referred to in Article 29 shall be conferred on the Commission for an indeterminate period of time from 18 August 2026.

3. The delegation of power referred to in Article 29 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 of 13 April 2016 on Better Law-Making.

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 29 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two 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 two months at the initiative of the European Parliament or of the Council.

Article 31

Notifications to the Commission

1. By 18 August 2025 each Member State shall notify the Commission of:

(a) the authority or authorities which, in accordance with its national law, are competent in accordance with Article 4 to issue, validate or transmit European Production Orders and European Preservation Orders or the notifications thereof;

(b) the authority or authorities which are competent to receive notifications pursuant to Article 8, and to enforce European Production Orders and European Preservation Orders on behalf of another Member State, in accordance with Article 16;

(c) the authority or authorities which are competent to deal with reasoned objections by addressees in accordance with Article 17;

(d) the languages accepted for the notification and the transmission of an EPOC, an EPOC-PR, a European Production Order or a European Preservation Order in the case of enforcement, in accordance with Article 27.

2. The Commission shall make the information received under this Article publicly available, either on a dedicated website or on the website of the European Judicial Network in criminal matters referred to in Article 9 of Council Decision 2008/976/JHA ([33]).

Article 32

Relationship to other instruments, agreements and arrangements

1. This Regulation does not affect Union or other international instruments, agreements and arrangements on the gathering of evidence that falls within the scope of this Regulation.

2. Member States shall notify the Commission by 18 August 2026 of any existing instruments, agreements and arrangements as referred to in paragraph 1 which they will continue to apply. Member States shall also notify the Commission within three months of the signing of any new agreement or arrangement as referred to in paragraph 1.

Article 33

Evaluation

By 18 August 2029, the Commission shall carry out an evaluation of this Regulation. The Commission shall transmit an evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Union Agency for Fundamental Rights. That evaluation report shall include an assessment of the application of this Regulation and of the results that have been achieved with regard to its objectives, as well as an assessment of this Regulation's impact on fundamental rights. The evaluation shall be conducted in accordance with the Commission's better regulation guidelines. Member States shall provide the Commission with the information necessary for the preparation of the evaluation report.

Article 34

Entry into force and application

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

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

2. It shall apply from 18 August 2026.

However, the obligation for competent authorities and service providers to use the decentralised IT system established in Article 19 for written communication under this Regulation shall apply from one year after the adoption of the implementing acts referred to in Article 25.

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

Done at Strasbourg, 12 July 2023.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	P. NAVARRO RÍOS

ANNEX I

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

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council [1] the addressee of this European Production Order Certificate (EPOC) must execute this EPOC and must transmit the requested data in accordance with the deadline(s) specified in Section C of this EPOC to the competent authority indicated under point (a) of Section L of this EPOC.

In all cases, the addressee must, upon receipt of the EPOC, act expeditiously to preserve the data requested, unless the information in the EPOC does not allow it to identify those data. The data must continue to be preserved until the data are produced or until the issuing authority or, where applicable, the enforcing authority, indicates that it is no longer necessary to preserve and produce the data.

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

SECTION A: Issuing/validating authority

Issuing State: .....

Issuing authority: .....

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

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

File number of the issuing authority: .....

File number of the validating authority: .....

SECTION B: Addressee

Addressee: .....

☐ Designated establishment

☐ Legal representative

☐ This order is issued in an emergency case to the specified addressee because the designated establishment or the legal representative of a service provider did not react to the EPOC within the deadlines set out in Article 10 of Regulation (EU) 2023/1543 or has not been designated or appointed within the deadlines set out in Directive (EU) 2023/1544 of the European Parliament and of the Council [2]

Address: .....

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

Contact person (if known): .....

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

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

Any other relevant information: .....

[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

[2] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181).

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

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

☐ as soon as possible and at the latest within 10 days (no notification to the enforcing authority)

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

☐ without undue delay and at the latest within eight hours in an emergency case involving:

☐ an imminent threat to the life, physical integrity or safety of a person

☐ an imminent threat to a critical infrastructure as defined in Article 2, point (a), of Council Directive 2008/114/EC ([3]), where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State.

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

Please provide additional information where relevant: ....

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

☐ The requested data were totally/partially preserved in accordance with an earlier request for preservation

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

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

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

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

☐ The requested data are related to an earlier request for production

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

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

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

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

Any other relevant information: ....

([3]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

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

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

Tel No: ....

Email address(es): ....

IMEI number(s): ....

MAC address(es): ....

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

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

Other: ....

If applicable, the time range of the data for which production is requested:

....

☐ Additional information if needed: ....

SECTION F: Electronic evidence to be produced

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

(a) ☐ subscriber data:

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

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

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

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

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

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

☐ PUK-codes

☐ other: .....

(b) ☐ data requested for the sole purpose of identifying the user as defined in Article 3, point (10), of Regulation (EU) 2023/1543:

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

☐ time range of the data for which production is requested (if different from Section E): .....

☐ other: .....

(c) ☐ traffic data:

(i) for (mobile) telephony:

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

☐ time and duration of connection(s)

☐ call attempt(s)

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

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

☐ other: .....

(ii) for internet:

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

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

☐ volume of data

☐ date and time of connection(s)

☐ duration of connection or access session(s)

☐ other: .....

(iii) for hosting:

☐ logfiles

☐ tickets

☐ other: .....

(iv) other:

☐ purchase history

☐ prepaid balance charging history

☐ other: .....

(d) ☐ content data:

☐ (web)mailbox dump

☐ online storage dump (user-generated data)

☐ pagedump

☐ message log/backup

☐ voicemail dump

☐ server contents

☐ device backup

☐ contact list

☐ other: .....

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

SECTION G: Information on the underlying conditions

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

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

☐ execution of a custodial sentence or a detention order of at least four months following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.

(b) Nature and legal classification of the offence(s) in relation to which the EPOC is issued and the applicable statutory provision ([4]):

....

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

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

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

☐ one or more of the following offences, if wholly or partly committed by means of an information system:

☐ offence(s) as defined in Articles 3 to 8 of Directive (EU) 2019/713 of the European Parliament and of the Council ([5]);

☐ offence(s) as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council ([6]);

☐ offence(s) as defined in Articles 3 to 8 of Directive 2013/40/EU of the European Parliament and of the Council ([7]);

☐ criminal offences as defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council ([8]).

(d) Controller/processor:

European Production Orders shall be addressed to service providers acting as controllers. By way of exception, the European Production Order may be addressed directly to the service provider that processes the data on behalf of the controller.

Tick where appropriate:

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

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

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

☐ addressing the controller might be detrimental to the investigation

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

☐ the processor shall inform the controller about the data production

☐ the processor shall not inform the controller about the data production until further notice, as it would be detrimental to the investigation. Please provide a short justification ([9]): .....

(e) Any other relevant information: ....

SECTION H: Information to the user

The addressee shall in any event refrain from informing the person whose data are being requested. It is the responsibility of the issuing authority to inform that person, without undue delay, about the data production.

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

([6]) 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).

([7]) 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).

([8]) 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).

([9]) The issuing authority must indicate the reasons for the delay in the case file, only a short justification must be added in the EPOC.

Please note that (tick where appropriate):

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

☐ it is necessary to avoid obstructing official or legal inquiries, investigations or procedures;

☐ it is necessary to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

☐ it is necessary to protect public security;

☐ it is necessary to protect national security;

☐ it is necessary to protect the rights and freedoms of others.

SECTION I: Details of the issuing authority

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

☐ judge, court, or investigating judge

☐ public prosecutor

☐ other competent authority as defined by the issuing State

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

Please note that (tick if applicable):

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

Details of the issuing authority, or its representative, or both, certifying the contents of the EPOC as accurate and correct:

Name of authority: ....

Name of its representative: ....

Post held (title/grade): ....

File number: ....

Address: ....

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

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

Email: ....

Language(s) spoken: ....

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

Name of the authority/name: ....

Address: ....

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

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

Email: ....

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

Date: ....

Signature ([10]): ....

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

The type of validating authority

☐ judge, court or investigating judge

☐ public prosecutor

Details of the validating authority, or its representative, or both, certifying the contents of the EPOC as accurate and correct:

Name of the authority: ....

Name of its representative: ....

Post held (title/grade): ....

File number: ....

Address: ....

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

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

Email: ....

Language(s) spoken: ....

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

Date: ....

Signature ([11]): ....

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

☐ This EPOC is notified to the following enforcing authority:
....

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

Name of the enforcing authority: ....

Address: ....

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

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

Email: ....

SECTION L: Transfer of data

(a) Authority to whom the data have to be transferred

☐ issuing authority,

☐ validating authority

☐ other competent authority (e.g. central authority)

Name and contact details: ....

(b) Preferred format in which or means by which the data have to be transferred (if applicable): .....

SECTION M: Further information to be included (not to be sent to the addressee – to be provided to the enforcing authority in the event that notification to the enforcing authority is required)

The grounds for determining that the European Preservation Order fulfils the conditions of necessity and proportionality:

....

A summary description of the case:

....

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

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

☐ participation in a criminal organisation;

☐ terrorism;

☐ trafficking in human beings;

☐ sexual exploitation of children and child pornography;

☐ illicit trafficking in narcotic drugs and psychotropic substances;

☐ illicit trafficking in weapons, munitions and explosives;

☐ corruption;

☐ fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council ([12]);

☐ laundering of the proceeds of crime;

☐ counterfeiting currency, including the euro;

☐ computer-related crime;

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

☐ facilitation of unauthorised entry and residence;

☐ murder or grievous bodily injury;

☐ illicit trade in human organs and tissue;

☐ kidnapping, illegal restraint or hostage-taking;

☐ racism and xenophobia;

☐ organised or armed robbery;

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

☐ swindling;

☐ racketeering and extortion;

☐ counterfeiting and piracy of products;

☐ forgery of administrative documents and trafficking therein;

☐ forgery of means of payment;

☐ illicit trafficking in hormonal substances and other growth promoters;

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

☐ illicit trafficking in nuclear or radioactive materials;

☐ trafficking in stolen vehicles;

☐ rape;

☐ arson;

☐ crimes within the jurisdiction of the International Criminal Court;

☐ unlawful seizure of aircraft or ships;

☐ sabotage.

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

… ....

ANNEX II

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

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council [1] the addressee of this European Preservation Order Certificate (EPOC-PR) must, without undue delay after receiving the EPOC-PR, preserve the data requested. The preservation must cease after 60 days, unless extended by the issuing authority by an additional 30 days, or the issuing authority confirms that a subsequent request for production has been issued. If the issuing authority confirms within those time periods that a subsequent request for production has been issued, the addressee must preserve the data for as long as necessary to produce the data once the subsequent request for production is received.

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

SECTION A: Issuing/validating authority:

Issuing State: ....

Issuing authority: ....

Validating authority (where applicable): ....

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

File number of the issuing authority: ....

File number of the validating authority: ....

SECTION B: Addressee

Addressee: ....

☐ Designated establishment

☐ Legal representative

☐ This order is issued in an emergency case to the specified addressee because the designated establishment or the legal representative of a service provider did not react to the EPOC-PR within the deadlines or has not been designated or appointed within the deadlines set out in Directive (EU) 2023/1544 of the European Parliament and of the Council [2]

[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

[2] Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28.7.2023, p. 181).

Address: .....

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

Contact person (if known): .....

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

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

Any other relevant information: .....

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

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

☐ Tel. No: .....

☐ Email address(es): .....

☐ IMEI number(s): .....

☐ MAC address(es): .....

☐ The user(s) of the service or other unique identifier(s) such as user name(s), login ID(s) or account name(s) ....

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

☐ Other: .....

If applicable, the time range of the data for which preservation is requested: .....

☐ Additional information if needed: .....

SECTION D: Electronic evidence to be preserved

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

(a) ☐ subscriber data:

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

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

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

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

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

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

☐ PUK-codes

☐ other:..... .....

(b) ☐ data requested for the sole purpose of identifying the user as defined in Article 3, point (10) of Regulation (EU) 2023/1543:

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

☐ time range of the data for which preservation is requested (if different from Section C):.....

☐ other:..... .....

(c) ☐ traffic data:

(i) for (mobile) telephony:

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

☐ time and duration of connection(s)

☐ call attempt(s)

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

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

☐ other:..... .....

(ii) for internet:

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

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

☐ volume of data

☐ date and time of connection(s)

☐ duration of connection or access session(s)

☐ other:..... .....

(iii) for hosting:

☐ logfiles

☐ tickets

☐ other:..... .....

(iv) other:

☐ purchase history

☐ prepaid balance charging history

☐ other:..... .....

(d) ☐ content data:

☐ (web)mailbox dump

☐ online storage dump (user-generated data)

☐ pagedump

☐ message log/backup

☐ voicemail dump

☐ server contents

☐ device backup

☐ contact list

☐ other:..... .....

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

SECTION E: Information on the underlying conditions

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

☐ criminal proceedings in respect of a criminal offence;

☐ execution of a custodial sentence or a detention order of at least four months following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.

(b) Nature and legal classification of the offence(s) for which the EPOC-PR is issued and the applicable statutory provision ([3]) ....

SECTION F: Details of the issuing authority

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

☐ judge, court, or investigating judge

☐ public prosecutor

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

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

Please note that (tick if applicable):

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

This emergency case refers to an imminent threat to the life, physical integrity or safety of a person or an imminent threat to a critical infrastructure as defined in Article 2, point (a), of Council Directive 2008/114/EC ([4]), where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State.

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

Name of authority: ....

Name of its representative: ....

Post held (title/grade): ....

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

([4]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures (OJ L 345, 23.12.2008, p. 75).

File number: .....

Address: .....

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

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

Email: .....

Language(s) spoken: .....

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

Name of authority/name: .....

Address: .....

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

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

Email: .....

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

Date: .....

Signature ([5]): .....

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

The type of validating authority:

☐ judge, court or investigating judge

☐ public prosecutor

Details of the validating authority or its representative, or both, certifying the contents of the EPOC-PR as accurate and correct:

Name of the authority: .....

Name of its representative: .....

Post held (title/grade): .....

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

File number: .....

Address: .....

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

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

Email: .....

Language(s) spoken: .....

Date: .....

Signature ([6]): .....

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

ANNEX III

INFORMATION ON THE IMPOSSIBILITY OF EXECUTING AN EPOC / EPOC-PR

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council [1], in cases where the addressee cannot comply with its obligation to preserve the requested data under an EPOC-PR or to produce it under an EPOC, cannot respect the specified deadline or does not provide the data exhaustively, this form should be completed by the addressee and sent back to the issuing authority as well as, where a notification took place and in other cases where applicable, to the enforcing authority referred to in the EPOC, without undue delay.

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

SECTION A: Certificate concerned

The following information concerns:

☐ a European Production Order Certificate (EPOC)

☐ a European Preservation Order Certificate (EPOC-PR)

SECTION B: Relevant authority(ies)

Issuing authority: .....

File number of the issuing authority: .....

If applicable, validating authority: .....

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

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

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

If applicable, enforcing authority: .....

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

SECTION C: Addressee of the EPOC/EPOC-PR

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

File number of the addressee: .....

[1] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

SECTION D: Reasons for non-execution

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

☐ it is incomplete

☐ it contains manifest errors

☐ it does not contain sufficient information

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

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

☐ the European Production Order/European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4 of Regulation (EU) 2023/1543.

☐ the European Production Order to obtain traffic data which are not requested for the sole purpose of identifying the user as defined in Article 3, point (10), of Regulation (EU) 2023/1543, or to obtain content data, has been issued for an offence not covered by Article 5(4) of Regulation (EU) 2023/1543.

☐ the service is not covered by Regulation (EU) 2023/1543.

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

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

(b) Please explain further the reasons for non-execution referred to in point (a), and, where necessary, indicate and explain any other reasons not listed under point (a):

… ....

SECTION E: Conflicting obligations arising from the law of a third country

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

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

… ....

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

… ....

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

☐ fundamental rights of individuals (please specify):

… ....

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

… ....

☐ other interests (please specify):

… ....

— explain why the law is applicable in this case:

… ....

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

… ....

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

… ....

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

… ....

Please add any relevant additional information: ....

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

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

… ....

SECTION G: Preservation of data

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

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

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

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

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

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

Post held: .....

Address: .....

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

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

Email: .....

Name of the authorised person:.....

Date .....

Signature ([2]): .....

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

ANNEX IV

CATEGORIES OF OFFENCES REFERRED TO IN ARTICLE 12(1), POINT (D)

(1) participation in a criminal organisation;

(2) terrorism;

(3) trafficking in human beings;

(4) sexual exploitation of children and child pornography;

(5) illicit trafficking in narcotic drugs and psychotropic substances;

(6) illicit trafficking in weapons, munitions and explosives;

(7) corruption;

(8) fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council ([1]);

(9) laundering of the proceeds of crime;

(10) counterfeiting currency, including the euro;

(11) computer-related crime;

(12) environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties;

(13) facilitation of unauthorised entry and residence;

(14) murder or grievous bodily injury;

(15) illicit trade in human organs and tissue;

(16) kidnapping, illegal restraint or hostage-taking;

(17) racism and xenophobia;

(18) organised or armed robbery;

(19) illicit trafficking in cultural goods, including antiques and works of art;

(20) swindling;

(21) racketeering and extortion;

(22) counterfeiting and piracy of products;

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

(23) forgery of administrative documents and trafficking therein;

(24) forgery of means of payment;

(25) illicit trafficking in hormonal substances and other growth promoters;

(26) illicit trafficking in nuclear or radioactive materials;

(27) trafficking in stolen vehicles;

(28) rape;

(29) arson;

(30) crimes within the jurisdiction of the International Criminal Court;

(31) unlawful seizure of aircraft or ships;

(32) sabotage.

ANNEX V

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

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council ([1]), upon receipt of the European Preservation Order Certificate (EPOC-PR) the addressee must, without undue delay, preserve the data requested. The preservation must cease after 60 days, unless extended by the issuing authority by an additional 30 days, or the issuing authority confirms that the subsequent request for production has been issued, using the form set out in this Annex.

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

SECTION A: Issuing authority of the EPOC-PR

Issuing State: ....

Issuing authority: ....

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

Name and contact details: ....

SECTION B: Addressee of the EPOC-PR

Addressee: ....

Address: ....

Phone/fax/email (if known): ....

Contact person (if known): ....

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

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

Any other relevant information: ....

([1]) Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

SECTION C: Information about the EPOC-PR

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

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

SECTION D: Confirmation

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

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

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

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

Signature of the issuing authority and/or its representative

Name:.....

Date:.....

Signature ([2]):.....

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

ANNEX VI

EXTENSION OF THE PRESERVATION OF ELECTRONIC EVIDENCE

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council ([1]), upon receipt of the European Preservation Order Certificate (EPOC-PR) the addressee must, without undue delay, preserve the data requested. The preservation must cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been issued. Within the 60 days, the issuing authority may extend the duration of the preservation by an additional 30 days where necessary, to allow for the issuing of the subsequent request for production, using the form set out in this Annex.

SECTION A: Issuing authority of the EPOC-PR

Issuing State: … .....

Issuing authority: … .....

File number of the issuing authority: … .....

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

Name and contact details: … .....

SECTION B: Addressee of the EPOC-PR

Addressee: … .....

Address: … .....

Phone/fax/email (if known): … .....

Contact person (if known): … .....

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

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

Any other relevant information: … .....

SECTION C: Information on prior EPOC-PR

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

([1]) Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28.7.2023, p. 118).

SECTION D: Extension of the prior preservation order

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

Signature of the issuing authority and/or its representative

Name: ….....

Date: ….....

Signature ([2]): ….....

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