EUROPEAN
COMMISSION

Strasbourg, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Proposal for a

# REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## on European Production and Preservation Orders for electronic evidence in criminal matters

{SWD(2018) 118 final} - {SWD(2018) 119 final}

# EXPLANATORY MEMORANDUM

## 1. CONTEXT OF THE PROPOSAL

### • Reasons for and objectives of the proposal

Today, using social media, webmail, messaging services and applications (‘apps’) to communicate, work, socialise and obtain information has become commonplace in many parts of the world. These services connect hundreds of millions of users to one another. They generate significant benefits for the users’ economic and social wellbeing across the Union and beyond. However, they can also be misused as tools to commit or facilitate crimes, including serious crimes such as terrorist attacks. When that happens, these services and apps are often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in court.

Given the borderless nature of the internet, such services can be provided from anywhere in the world and do not necessarily require physical infrastructure, a corporate presence or staff in Member States where the services are offered or in the internal market as a whole. They also do not require a specific location for the storage of data, which is often chosen by the service provider on the basis of legitimate considerations such as data security, economies of scale and swiftness of access. As a result, in a growing number of criminal cases involving all types of crime[1], Member State authorities require access to data that might serve as evidence and that is stored outside their country and/or by service providers in other Member States or third countries.

For situations where either the evidence or the service provider is located elsewhere, mechanisms for cooperation between countries were developed several decades ago[2]. Despite regular reforms, these cooperation mechanisms are under increasing pressure from the growing need for timely cross-border access to electronic evidence. In response, a number of Member States and third countries have resorted to expanding their national tools. The resulting fragmentation generates legal uncertainty and conflicting obligations and raises questions about the protection of fundamental rights and procedural safeguards for persons affected by such requests.

In 2016, the Council called for concrete action based on a common EU approach to make mutual legal assistance more efficient; to improve cooperation between Member State authorities and service providers based in non-EU countries; and to propose solutions to the problem of determining and enforcing jurisdiction[3] in cyberspace[4]. The European Parliament similarly highlighted the challenges that the currently fragmented legal framework can create for service providers seeking to comply with law enforcement requests and called for a European legal framework, including safeguards for the rights and freedoms of all concerned[5].

---

1 See Sections 2.1.1 and 2.3 of the impact assessment.

2 In the Union, mutual recognition mechanisms, now based on the European Investigation Order Directive; with third countries, mutual legal assistance (MLA) mechanisms.

3 In this document, the term ‘enforcement jurisdiction’ makes reference to the competence of the relevant authorities to undertake an investigative measure.

4 Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16.

5 P8_TA(2017)0366.

The present proposal targets the specific problem created by the volatile nature of electronic evidence and its international dimension. It seeks to adapt cooperation mechanisms to the digital age, giving the judiciary and law enforcement tools to address the way criminals communicate today and to counter modern forms of criminality. Such tools are conditional on their being subject to strong protection mechanisms for fundamental rights. This proposal aims to improve legal certainty for authorities, service providers and persons affected and to maintain a high standard for law enforcement requests, thus ensuring protection of fundamental rights, transparency and accountability. It also speeds up the process to secure and obtain electronic evidence that is stored and/or held by service providers established in another jurisdiction. This instrument will co-exist with the current judicial cooperation instruments that are still relevant and can be used as appropriate by the competent authorities. In parallel, the Commission is working to strengthen the existing judicial cooperation mechanisms through measures such as the creation of a secure platform for the swift exchange of requests between judicial authorities within the EU and the investment of EUR 1 million to train practitioners from all EU Member States in mutual legal assistance and cooperation, with a focus on the United States as the third country receiving the largest number of requests from the EU[6].

For the serving and execution of orders under this instrument, authorities should rely on the legal representative designated by the service providers. The Commission presents today a proposal to ensure that such legal representatives are effectively designated. It provides a common, EU-wide solution for addressing legal orders to service providers by way of a legal representative.

- **Consistency with existing EU legal framework in the policy area and the Council of Europe Budapest Convention**

The current EU legal framework consists of Union cooperation instruments in criminal matters, such as the Directive 2014/41/EU regarding the European Investigation Order in criminal matters[7] (EIO Directive), the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[8], Council Decision 2002/187/JHA setting up Eurojust[9], Regulation (EU) 2016/794 on Europol[10], Council Framework Decision 2002/465/JHA on joint investigation teams[11], as well as bilateral agreements between the

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

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

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

9 Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. In 2013, the Commission adopted a proposal for a Regulation to reform Eurojust (Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM/2013/0535 final).

10 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

11 Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.

Union and non-EU countries, such as the Agreement on Mutual Legal Assistance ('MLA') between the EU and the US[12] and the Agreement on MLA between the EU and Japan[13].

By introducing European Production Orders and European Preservation Orders, the proposal makes it easier to secure and gather electronic evidence for criminal proceedings stored or held by service providers in another jurisdiction. The EIO Directive, which has to a large extent replaced the Convention on Mutual Assistance in Criminal Matters, covers any investigative measure[14]. This includes access to electronic evidence but the EIO Directive does not contain any specific provisions on this type of evidence[15]. The new instrument will not replace the EIO for obtaining electronic evidence but provides an additional tool for authorities. There may be situations, for example when several investigative measures need to be carried out in the executing Member State, where the EIO may be the preferred choice for public authorities. Creating a new instrument for electronic evidence is a better alternative than amending the EIO Directive because of the specific challenges inherent in obtaining electronic evidence which do not affect the other investigative measures covered by the EIO Directive.

To facilitate cross-border gathering of electronic evidence, the new instrument will build on the principles of mutual recognition. An authority in the country where the addressee of the Order is located will not have to be involved in serving and executing the Order directly, except if there is non-compliance, in which case enforcement will be required and the competent authority in the country where the representative is located will intervene. The instrument therefore requires a set of robust safeguards and provisions, such as validation by a judicial authority in each case. For instance, European Production Orders to produce transactional or content data (as opposed to subscriber and access data) may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or for specific cyber-dependent, cyber-enabled or terrorism-related crimes as referred to in the proposal.

Personal data covered by this proposal is protected and may only be processed in accordance with the General Data Protection Regulation (GDPR)[16] and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive)[17]. The GDPR will enter into application on 25 May 2018, while the Law Enforcement Data Protection Directive has to be transposed by the Member States by 6 May 2018.

---

12 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

13 Council Decision 2010/616/EU of 7 October 2010 on the conclusion of the Agreement between the European Union and Japan on mutual legal assistance in criminal matters.

14 Except for joint investigation teams (See Art. 3 EIO Directive); not all Member State participate in the EIO Directive (Ireland, Denmark).

15 Except for a reference to the identification of a person holding an IP address in Art. 10(2)(e), for which double criminality cannot be invoked as a ground for refusal to recognise and execute the request.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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

The Council of Europe's Budapest Convention on Cybercrime (CETS No 185), ratified by most EU Member States, establishes international mechanisms for cooperation against cybercrime[18]. The Convention deals with crimes committed via the internet and other computer networks. It also requires Parties to establish powers and procedures to obtain electronic evidence and to provide each other mutual legal assistance, not limited to cybercrimes. In particular, the Convention requires Parties to put in place production orders to obtain computer data from service providers in their territory and subscriber data from service providers offering services in their territory. Moreover, the Convention provides for preservation orders where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. The service and enforceability of national production orders against providers established outside the territory of a Party to the Convention raises further issues. In that regard, further measures to improve cross-border access to electronic evidence are currently under consideration[19].

- **Summary of the proposed Regulation**

The proposed Regulation introduces binding European Production and Preservation Orders. Both Orders need to be issued or validated by a judicial authority of a Member State. An order can be issued to seek preservation or production of data that is stored by a service provider located in another jurisdiction and that are necessary as evidence in criminal investigations or criminal proceedings. Such Orders may only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State. Both Orders can be served on providers of electronic communication services, social networks, online marketplaces, other hosting service providers and providers of internet infrastructure such as IP address and domain name registries, or on their legal representatives where they exist. The European Preservation Order, similarly to the European Production Order, is addressed to the legal representative outside of the issuing Member State's jurisdiction to preserve the data in view of a subsequent request to produce this data, for example via MLA channels in case of third countries or via an EIO between participating Member States. Unlike surveillance measures or data retention obligations set out by law, which are not provided for by this Regulation, the European Preservation Order is an Order issued or validated by a judicial authority in a concrete criminal procedure after an individual evaluation of the proportionality and necessity in every single case. Like the European Production Order, it refers to the specific known or unknown perpetrators of a criminal offence that has already taken place. The European Preservation Order only allows preserving data that is already stored at the time of receipt of the Order, not the access to data at a future point in time after the receipt of the European Preservation Order.

Both Orders can be used only in criminal proceedings, from the initial pre-trial investigative phase until the closure of the proceedings by judgment or other decision. The Orders to produce subscriber and access data can be issued for any criminal offence whilst the Order for producing transactional or content data may only be issued for criminal offences punishable in

[18] In the 2013 Cybersecurity Strategy of the European Union, the Budapest Convention was recognised as the main multilateral framework for the fight against cybercrime - Joint Communication of the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final.

[19] At its 17th Plenary (June 2017), the Cybercrime Convention Committee (T-CY) adopted the Terms of Reference of the preparation of a second additional protocol to the Convention ('Second Additional Protocol') to be prepared and finalised by the T-CY by December 2019. The aim is to move away from data storage location as a decisive factor.

the issuing State by a custodial sentence of a maximum of at least 3 years, or for specific crimes which are referred to in the proposal and where there is a specific link to electronic tools and offences covered by the Terrorism Directive 2017/541/EU.

Given the different levels of intrusiveness of the measures imposed in relation to the data pursued, the proposal sets out a number of conditions and safeguards. These include the obligation to obtain ex-ante validation of orders by a judicial authority. The proposal applies only to stored data. Real-time interception of telecommunication is not covered by this proposal. The measure is limited to what is necessary and proportionate for the purposes of relevant criminal proceedings. It also allows service providers to seek clarifications from issuing authorities where necessary. If these issues cannot be solved and the issuing authority decides to pursue enforcement, service providers may use the same reasons to oppose enforcement by its own authorities. In addition, a specific procedure is set up for situations where the obligation to provide data conflicts with a competing obligation arising from a third country law.

EU legislation protects the rights of the suspects and the accused in criminal proceedings, and there are already rules to protect personal data. However, for the persons whose data is being sought, these additional safeguards in the proposal provide procedural rights for these persons in or outside of the criminal proceedings. This includes the possibility to challenge the legality, necessity or the proportionality of the Order without restricting the grounds for the challenge in accordance with national law. The rights under the law of the enforcing State are fully respected by ensuring that immunities and privileges which protect the data sought in the Member State of the service provider are taken into account in the issuing State. This is especially the case where they provide for a higher protection than the law of the issuing State.

The Orders under the proposed Regulation are enforceable in the same manner as comparable domestic orders in the jurisdiction where the service provider receives the order. The Regulation provides that Member States should have effective and proportionate sanctions in place.

## 2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

### • Legal basis

The legal basis to support action in the field is Article 82(1) of the Treaty on the Functioning of the European Union. Article 82(1) provides that measures may be adopted in accordance with the ordinary legislative procedure to lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions. Measures may also be adopted to facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions.

This legal basis applies to the mechanisms covered by this Regulation. Article 82(1) ensures mutual recognition of judicial decisions by which a judicial authority in the issuing State addresses a legal person in another Member State and even imposes obligations on it, without prior intervention of a judicial authority in that other Member State. The European Production or Preservation Order can lead to the intervention of a judicial authority of the executing State when necessary to enforce the decision.

- **Choice of the instrument**

Article 82(1) TFEU gives the Union's legislator the possibility to adopt regulations and directives.

As the proposal concerns cross-border procedures, where uniform rules are required, there is no need to leave a margin to Member States to transpose such rules. A regulation is directly applicable, provides clarity and greater legal certainty and avoids divergent interpretation in the Member States and other transposition problems that the Framework Decisions on mutual recognition of judgments and judicial decisions have encountered. Furthermore, a regulation allows for the same obligation to be imposed in a uniform manner in the Union. For these reasons the most appropriate form to be used for this mutual recognition instrument is considered to be a regulation.

- **Subsidiarity**

Given the cross-border dimension of the problems addressed, the measures included in the proposal need to be adopted at Union level in order to achieve the objectives. The crimes for which electronic evidence exists frequently involve situations where the infrastructure in which the electronic evidence is stored and the service provider running the infrastructure are under a different national legal framework, within the Union or beyond, than the national legal framework of the victim and perpetrator of the crime. As a result, it can be very time-consuming and challenging for the competent country to effectively access electronic evidence across borders without common minimum rules. In particular, Member States acting alone would have difficulty addressing the following issues:

- Fragmentation of legal frameworks in Member States, which was identified as a major challenge by service providers seeking to comply with requests based on different national laws;
- Better expediency of judicial cooperation on the basis of existing Union legislation, notably via the EIO.

Given the diversity of legal approaches, the number of policy areas concerned (security, fundamental rights including procedural rights and protection of personal data, economic issues), and the large range of stakeholders, Union-level legislation is the most appropriate means to address the identified problems.

- **Proportionality**

The proposal lays down rules under which a competent authority in the Union may order a service provider offering services in the Union and not established in the same Member State, to produce or preserve electronic evidence. Key features of the proposal, such as the material scope of the European Production Order, conditions ensuring comity, the sanctioning mechanism and the system of safeguards and legal remedies, limit the proposal to what is necessary to achieve its main objectives. In particular, the proposal is limited to requests for stored data (data from real-time interception of telecommunications is not covered) and to orders issued in criminal proceedings for a specific criminal offence under investigation. It therefore does not cover crime prevention or other types of proceedings or infringements (such as administrative proceedings for infringements of the rules of law) and does not require providers to systematically collect or store more data than they do for business reasons or for compliance with other legal requirements. Moreover, while the Orders to produce subscriber and access data can be issued for any criminal offence, the Order for producing transactional

or content data may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or for specific cyber-dependent and cyber-enabled offences defined in the proposal and terrorism related crimes. Finally, the proposal clarifies the procedural rules and safeguards applicable to cross-border access to electronic evidence but does not go as far as harmonising domestic measures. It is limited to what is necessary and proportionate to address the needs of law enforcement and judicial authorities in the digital age.

## 3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

Over a year and a half the Commission consulted all relevant stakeholders to identify problems and ways forward. This was done through surveys, ranging from an open public consultation to targeted surveys with the relevant public authorities. Group expert meetings and bilateral meetings were also organised to discuss the potential effects of EU legislation. Conferences discussing cross-border access to electronic evidence were also used to gather feedback on the initiative.

By and large, survey respondents perceived the increased use of information services to be a challenge for law enforcement, as the relevant authorities are often ill equipped to deal with evidence online. The lengthy process to obtain evidence is also recognised as one of the main obstacles. Other key issues public authorities highlighted include the lack of reliable cooperation with service providers, lack of transparency, and legal uncertainty surrounding jurisdiction for investigative measures. Direct cross-border cooperation between law enforcement and digital service providers was considered to add value in a criminal investigation. Service providers and some civil society organisations indicated the need to ensure legal certainty when cooperating with public authorities and to avoid conflicts of law. On concerns about how new EU legislation could affect rights, stakeholders felt specific safeguards should be guaranteed as a necessary condition for any cross-border instrument.

Feedback gathered from the inception impact assessment showed that stakeholders believed addressing the shortcomings of the current MLA system would make it more effective and improve legal certainty. Some civil society organisations were against EU-level legislation on direct cooperation. They preferred to limit EU action to improving mutual legal assistance procedures. This idea will be taken forward as part of the practical measures endorsed by the Council in June 2016.

Through a targeted survey to public authorities in the Member States, it was also revealed that there was no common approach on obtaining cross-border access to electronic evidence, as each Member State has its own domestic practice. Service providers also react differently to requests from foreign law enforcement authorities, and response times vary depending on the requesting Member State. This creates legal uncertainty for all stakeholders involved.

In general, the stakeholder consultation indicated that the current legal framework is fragmented and complex. This can lead to delays during the execution phase and a lack of effective investigation and prosecution of crimes involving cross-border access to electronic evidence.

- **Impact assessment**

The Regulatory Scrutiny Board issued a positive opinion on the impact assessment supporting this proposal[20] and made various suggestions for improvement[21]. Following this opinion, the impact assessment was amended to further discuss fundamental rights issues associated with the cross-border sharing of data, in particular the links between the various measures that are part of the preferred option. The assessment was also modified to better reflect the views of stakeholders and Member States and how they were taken into account. Moreover, the policy context was reviewed to include additional references to various aspects, such as discussions in expert groups that helped to shape the initiative. The complementarity between different measures (in particular the EIO Directive, negotiations of an additional protocol to the Budapest Convention and the joint review of the EU-US MLA Agreement) was clarified in terms of scope, timing and depth, and the baseline scenario was revised to better reflect developments that are likely to occur independently from the adoption of the proposed measures. Finally, flowcharts were added to better describe the workflows for data sharing.

Four main policy options were considered besides the baseline scenario (Option O): a number of practical measures to improve both judicial cooperation procedures and direct cooperation between public authorities and service providers (Option A: non-legislative); an option combining the practial measures of Option A with international solutions at bilateral or multilateral level (Option B: legislative); an option combining the previous measures contained in Option B with a European Production Order and a measure to improve access to databases that provide subscriber information on a query basis, such as the Domain Name Whois (Option C: legislative); and an option combining all previous measures contained in Option C with legislation on direct access to remotely stored data (Option D: legislative)[22].

If no measure is taken (Option O), an increasing number of requests will worsen the situation. All other options help to achieve the objectives of the initiative but to varying degrees. Option A would improve the efficiency of current processes, for example by improving the quality of requests, but the room for improvement would be limited by the structural shortcomings of the current system.

Option B would lead to more improvements by providing for internationally accepted solutions, but the outcome of these international solutions would to a large extent depend on third States. The solutions are therefore uncertain and unlikely to be as effective and offer as many safeguards as a Union solution.

Option C would clearly add value compared to the previous options by also providing for an intra-EU instrument on direct cooperation with service providers that would address most of the issues identified when there is a service provider that holds the data concerned.

---

20 Commission Staff Working Document – Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118.

21 European Commission Regulatory Scrutiny Board – Opinion on the Impact Assessment – Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SEC(2018) 199.

22 For details, cf. the Commission Staff Working Document – Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD(2018) 118.

Option D is the most comprehensive package of solutions. In addition to the previous measures, it involves a legislative measure on direct access for situations where the involvement of a service provider is not needed.

The present legislative initiative that the Commission is proposing is based on the findings of the impact assessment. This legislation will be complemented by the practical measures as described in the impact assessment and by continued work towards an additional protocol to the Budapest Convention. Based on its legislative proposal, the Commission will also discuss with the US and other third countries the possibility of future bilateral or multilateral agreements on cross-border access to electronic evidence with accompanying safeguards. For measures on direct access and the access to databases, which form part of Option D, the Commission is at the moment not proposing any legislation, but will reflect further on the best way forward on these two issues.

The initiative is expected to enable more effective and efficient investigations and prosecutions while improving transparency and accountability and ensuring respect of fundamental rights. It is also expected to foster trust in the digital single market by improving security and reducing the perception of impunity for crimes committed on or through networked devices.

For public authorities, the initiative is expected to generate initial implementation costs, which in the long term would be offset by savings in recurrent costs. National authorities would have to adapt to new procedures and undergo training. However, after that authorities would benefit from the streamlining and centralisation and the clear legal framework governing requests for access to data, as these should generate efficiency gains. Similarly, as the preferred option would take pressure off judicial cooperation channels, countries receiving requests should see a reduction in the number of requests they are required to process.

Service providers would need to adapt to a new legislative framework by putting (new) procedures in place and training their staff. On the other hand, a harmonised framework could reduce the burden on those providers currently responding to requests for non-content data which have to assess them under the different laws of all Member States. Legal certainty and standardisation of procedures should also have a positive impact on small and medium-sized businesses, since they would alleviate administrative burden and favour competitiveness. Overall, the initiative is also expected to generate savings for them.

- **Fundamental rights**

The proposal could potentially affect a number of fundamental rights:

- rights of the individual whose data is accessed: right to protection of personal data; right to respect of private and family life; right to freedom of expression; right of defence; right to an effective remedy and to a fair trial;
- rights of the service provider: right to freedom to conduct a business; right to an effective remedy;
- rights of all citizens: right to liberty and security.

Taking into account the relevant data protection *acquis,* sufficient and important safeguards are included in the proposed Regulation to ensure that the rights of these persons are protected.

Since the Orders can only be issued in criminal proceedings and if there are comparable national situations, both during the pre-trial and trial phase, all criminal law procedural safeguards are applicable. This includes in particular the right to a fair trial enshrined in Article 6 ECHR and Articles 47 and 48 of the Charter of Fundamental Rights. It also includes the relevant legislation at EU level on procedural rights in criminal proceedings: Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, Directive 2012/13/EU on the right to information about rights and charges and access to the case file, Directive 2013/48/EU on the right of access to a lawyer and communication with relatives when arrested and detained, Directive 2016/343 on the strengthening of certain aspects of the presumption of innocence and the right to be present at one's trial, Directive 2016/800 on the procedural safeguards for children and Directive 2016/1919 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings.

More specifically, the prior intervention of a judicial authority when the Order is issued ensures that the legality of the measure and its necessity and proportionality to the case in question has been checked. This also ensures that the Order does not unduly impinge on fundamental rights, including the effects of legal principles such as the lawyer-client privilege. The issuing authority is required to ensure in the individual case that the measure is necessary and proportionate, including in view of the gravity of the offence under investigation. The proposal also includes thresholds for transactional and content data, ensuring that the European Production Order will only be used for more serious forms of crimes in relation to such data.

The right to an effective remedy for persons whose data is being requested is also explicitly addressed. Immunities and privileges of certain professions such as lawyers granted as well as fundamental interests of national security or defence in the State of the addressee must also be taken into account during trial in the issuing State. The review by a judicial authority serves as a further safeguard here.

As the Order is a binding measure, it also affects the rights of service providers, in particular the freedom to conduct a business. The proposal includes a right for the service provider to raise certain claims in the issuing Member State, for example if the Order has not been issued or validated by a judicial authority. If the Order is transmitted for enforcement to the enforcing state, the enforcing authority may decide not to recognise or enforce the Order if upon receipt any of the limited grounds for opposition are apparent, and after consulting with the issuing authority. In addition, should the procedure for enforcement be initiated, the addressee itself will be able to oppose the Order before the enforcing authority on the basis of any of such limited grounds. This includes, for example, cases where it is apparent that the Order was not issued or validated by a competent authority or where compliance would manifestly violate the Charter or be manifestly abusive. This does not preclude the right of the addressee to an effective judicial remedy against a decision imposing a sanction.

A potential issue related to EU measures in this area is the possibility that it could lead to third countries introducing reciprocal obligations for EU service providers which are not consistent with EU fundamental rights conditions, including the high level of data protection ensured by the EU acquis. The proposal addresses this situation in two ways: first, by providing a measure that contains strong safeguards and explicit references to the conditions and safeguards already inherent in the EU *acquis*, thus serving as a model for foreign legislation; and secondly, by including a specific 'conflicts of obligations' clause that allows service providers to identify and raise conflicting obligations they face, triggering a judicial

review. This clause is designed to ensure respect both for general blocking statutes, such as for example the U.S. Electronic Communications Privacy Act (ECPA), which prohibits disclosure in relation to content data within its geographic scope except in limited circumstances, as well as for laws that do not generally prohibit the disclosure but may do so in individual cases. For cases relating to ECPA, access to content data might be prevented in certain situations at present, and MLA should therefore remain the main tool to access such data. However, with the changes brought about by the adoption of the U.S. CLOUD Act[23], the blocking statute could be lifted if the EU were to conclude an agreement with the US. Additional international agreements with other key partners may further reduce conflicts-of-law situations.

In view of the above, the measures in this proposal are compatible with fundamental rights.

## 4. BUDGETARY IMPLICATIONS

The legislative proposal for a Regulation does not have an impact on the Union's budget.

## 5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Regulation is directly applicable in the Union. It will be directly applied by practitioners, without the need to modify internal legal systems.

The Regulation will be evaluated and the Commission will submit a report to the European Parliament and the Council at the latest 5 years after its entry into force. Based on the findings of the report, in particular on whether the Regulation leaves any gaps which are relevant in practice, and taking into account technological developments, the Commission will assess the need to enlarge the scope of the Regulation. If necessary, the Commission will submit proposals to adapt this Regulation. Member States will provide the Commission with the information necessary for the preparation of the report. Member States will gather the data necessary for the yearly monitoring of the Regulation.

The Commission will, if necessary, issue guidance for service providers to comply with obligations under the Regulation.

- **Detailed explanation of the specific provisions of the proposal**

| | ***REGULATION*** | |
|---|---|---|
| | **Article** | **Recital** |
| I. Subject matter, definitions and scope | 1. Subject matter | 1-15 |
| | 2. Definitions | 16-23 |
| | 3. Scope | 24-27 |

[23] On 23 March 2018, the Clarifying Lawful Overseas Use of Data (CLOUD) Act was adopted in the United States. The CLOUD Act is available here.

| | | |
|---|---|---|
| II. European Production Order, European Preservation Order and Certificates, legal representative | 4. Issuing authority | 30 |
| | 5. Conditions for issuing a European Production Order | 28-29, 31-35 |
| | 6. Conditions for issuing a European Preservation Order | 36 |
| | 7. Addressee of a European Production Order and a European Preservation Order | 37 |
| | 8. European Production Order Certificate and European Preservation Oder Certificate | 38-39 |
| | 9. Execution of an EPOC | 40-41 |
| | 10. Execution of an EPOC-PR | 42 |
| | 11. Confidentiality and user information | 43 |
| | 12. Reimbursement of costs | None |
| III. Sanctions and enforcement | 13. Sanctions | None |
| | 14. Procedure for enforcement | 44-45, 55 |
| IV. Remedies | 15. and 16. Review procedure in case of conflicting obligations from the law of a third country | 47-53 |
| | 17. Effective remedies | 54 |
| | 18. Ensuring privileges and immunities under the law of the enforcing State | 35 |
| V. Final provisions | 19. Monitoring and reporting | 58 |
| | 20. Amendments to the Certificates and the Forms | 59-60 |
| | 21. Exercise of delegation | 60 |
| | 22. Notifications | None |
| | 23. Relationship to European Investigation Orders | 61 |
| | 24. Evaluation | 62 |
| | 25. Entry into force | None |

***Chapter 1: Subject matter, definitions and scope***

*Article 1: Subject matter*

This Article sets out the general scope and purpose of the proposal, which is to lay down the rules under which a competent judicial authority in the European Union may order a service provider offering services in the Union to produce or preserve electronic evidence through a European Production or Preservation Order. These instruments can only be used in cross-border situations, that is, in situations where the service provider is established or represented in another Member State.

This Regulation shall give additional tools to investigating authorities to obtain electronic evidence without limiting the powers already set out by national law to compel service providers established or represented on their territory. If the service provider is established or represented in the same Member State, authorities of that Member State shall therefore use national measures to compel the service provider.

The data ordered through a European Production Order should be provided directly to the authorities without the involvement of authorities in the Member State where the service provider is established or represented. The Regulation also moves away from data location as a determining connecting factor, as data storage normally does not result in any control by the state on whose territory data is stored. Such storage is determined in most cases by the provider alone, on the basis of business considerations[24].

Moreover, the Regulation is also applicable if the service providers are not established or represented in the Union, but offer services in the Union. This is mirrored in Article 3(1).

When the proposal refers to a service provider established or represented in a Member State via a designated legal representative, the sole designation of a legal representative does not create an establishment of the service provider for the purpose of this Regulation.

Article 1(2) recalls that this Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU.

*Article 2: Definitions*

This Article sets out definitions which apply throughout the instrument.

The following types of service providers fall under the scope of the Regulation: providers of electronic communications services, providers of information society services for which the storage of data is a defining component of the service provided to the user, including social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and other hosting service providers, and providers of internet domain name and numbering services.

The scope of the Regulation covers providers of electronic communications services as defined [in the Directive establishing the European Electronic Communications Code]. Traditional telecommunication services, consumers and businesses increasingly rely on new

[24] The impact assessment contains further explanations.

internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and e-mail services, instead of traditional communications services. These services, along with social networks, such as Twitter and Facebook, which allow users to share content, should thus be covered by this proposal.

In many cases, data is no longer stored on a user's device but made available on a cloud-based infrastructure allowing in principle access from anywhere. Service providers do not need to be established or to have servers in every jurisdiction but rather use a centralised administration and decentralised systems to store data and provide their services. They do so to optimise load balancing and shorten delays in responding to users' requests for data. Content delivery networks (CDNs) are usually deployed to speed up content delivery by copying content in several servers distributed throughout the globe. This enables companies to serve content from the server which is closest to the user or which can route communication through a less congested network. To take into account this development, the definition covers cloud and other hosting services that provide a variety of computing resources such as networks, servers or other infrastructure, storage, apps and services that make it possible to store data for different purposes. The instrument also applies to digital marketplaces that allow consumers and/or businesses to conclude transactions via online sales or service contracts. Such transactions are made either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace. It is therefore this marketplace that is in possession of electronic evidence that may be needed in the course of criminal proceedings.

Services for which the storage of data is not a defining component are not covered by the proposal. Although most services delivered by providers involve some kind of storage of data, especially where they are delivered online at a distance, services for which the storage of data is not a main characteristic and is thus only of an ancillary nature may be discerned, including legal, architectural, engineering and accounting services provided online at a distance.

Data held by providers of internet infrastructure services, such as domain name registrars and registries and privacy and proxy service providers, or regional internet registries for internet protocol addresses, may be of relevance for criminal proceedings as they can provide traces allowing for identification of an individual or entity involved in criminal activity.

The categories of data that can be obtained with a European Production Order by the competent authorities include subscriber data, access data, transactional data (the three categories commonly referred to jointly as 'non-content data') and stored content data. This distinction, apart from the access data, exists in the legal orders of many Member States and also in non-EU legal frameworks.

All categories contain personal data and are thus covered by the safeguards under the EU data protection *acquis*. The intensity of the impact on fundamental rights varies between them, in particular between subscriber data on the one hand and transactional and content data on the other hand. It is essential that all these categories are covered by the instrument: subscriber and access data are often the starting point to obtain leads in an investigation about the identity of a suspect. While transactional and content data can be the most relevant as probative material. Because of the different levels of interference with fundamental rights, it is justified to attach different conditions to subscriber data on the one hand and transactional and content data on the other, as is done in several provisions in the Regulation.

It is appropriate to single out access data as a specific data category used in this Regulation. Access data as defined here is pursued for the same objective as subscriber data, i.e. to identify the user, and the level of interference with fundamental rights is similar. It should therefore be subject to the same conditions as subscriber data. Hence this proposal introduces a new category of data, which is to be treated like subscriber data if the same aim is pursued.

Article 2 defines the Member States and authorities that could be involved in the procedure. A definition of the issuing authority is included in Article 4.

Emergency cases are exceptional situations that regularly require a timely reaction by service providers and for which special conditions will be applicable. They are therefore defined separately in this Article.

*Article 3: Scope*

This Article sets out the scope of the proposal. The Regulation applies to all service providers that offer services in the Union, including service providers that are not established in the Union. The active offering of services in the Union, with all the benefits deriving from it, justifies that these service providers are also made subject to the Regulation and creates a level playing field between participants on the same markets. Moreover, not covering these service providers would create a gap and make it easy for criminals to circumvent the scope of the Regulation.

In order to ascertain whether services are being offered, authorities need to assess whether the service provider enables legal or natural persons in one or more Member States to use its services. However, the mere accessibility of the service (which could also derive from the accessibility of the service provider's or an intermediary's website or of an email address and of other contact details) should not be a sufficient condition for the application of this Regulation. Therefore, a substantial connection to those Member States is required to ascertain a sufficient conjunction between the provider and the territory where it is offering its services. Such a substantial connection exists where a service provider has an establishment in one or more Member States. In the absence of an establishment in the Union, the criterion of a substantial connection to the Union should be assessed on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in a Member State. The targeting of activities towards a Member State could also be derived from the availability of an app in the relevant national app store from providing local advertising or advertising in the language used in a Member State, from making use of any information originating from persons in Member States in the course of its activities, or from the handling of customer relations such as by providing customer service in the language generally used in a Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.

The European Production Order and the European Preservation Order are investigative measures that can be issued only in criminal investigations or criminal proceedings for concrete criminal offences. The link to a concrete investigation distinguishes it from preventive measures or data retention obligations set out by law and ensures the application of

the procedural rights applicable to criminal proceedings. The competence to open investigations for a specific offence is therefore a prerequisite to use the Regulation.

As an additional requirement, the data sought must be related to services offered by the service provider in the Union.

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

*Article 4: Issuing authority*

When issuing a European Production or Preservation Order, a judicial authority always needs to be involved as either an issuing or a validating authority. For Orders to produce transactional and content data, a judge or court is required. For subscriber or access data, this can be done also by a prosecutor.

*Article 5: Conditions for issuing a European Production Order*

Article 5 sets out the conditions for issuing a European Production Order. They have to be assessed by the issuing judicial authority.

The European Production Order may only be issued if this is necessary and proportionate in the individual case. Moreover, it should only be issued if a similar measure would be available in a comparable domestic situation in the issuing State.

Orders to produce subscriber data and access data can be issued for any criminal offence. Transactional and content data should be subject to stricter requirements to reflect the more sensitive nature of such data and the correspondingly higher degree of invasiveness of Orders for such data, as compared to subscriber and access data. Orders can therefore only be issued for offences which carry a maximum custodial sentence of at least 3 years or more. Setting a threshold based on the maximum custodial sentence allows for a more 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, a threshold should not undermine the effectiveness of the instrument and its use by practitioners. Member States apply various maxima for sentences that relate to their national system. National criminal codes vary and are not harmonised. This is the case for the criminal offences and for the sanctions applicable to them. National procedural codes also differ regarding the thresholds for obtaining transactional or content data: some Member States do not set out any specific threshold; others provide for a list of offences. A three-year threshold limits the scope of the instrument to more serious crimes, without excessively limiting the possibilities of its use by practitioners. This threshold excludes from the scope a wide range of crimes depending on the criminal code of the Member State (for example in some Member States participation in the activity of an organised criminal group and abduction, but also offences such as petty theft, fraud and assault for which the use of a cross-border production order for more sensitive data may be considered disproportionate). On the other hand, a three-year threshold includes crimes that require a more effective approach, such as membership in a criminal organisation, financing of terrorist groups, supporting or advertising a criminal organisation, training for the commission of terrorist offences, certain offences made with terrorist intent and preparation of an offence to be committed with terrorist intent, or preparation of hostage taking, which would otherwise be excluded if a higher threshold was applied, depending on the Member State. This threshold has been chosen to ensure a balance for all Member States between efficiency of criminal investigations and

protection of rights and proportionality. A threshold also has the advantage of being easily applicable in practice.

In addition, Orders for producing transactional or content data may also be issued for specific harmonised offences listed in the provision for which evidence will typically be available mostly only in electronic form. This justifies the application of the Regulation also in cases where the maximum custodial sentence is less than the above threshold; otherwise those offences could not be investigated properly, which might lead to impunity. The offences are specific provisions of: (i) Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment, (ii) Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA and (iii) Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Orders may also be issued for offences listed in Directive 2017/541/EU on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. Some of these offences have minimum maximum thresholds of at least 1 year, others of 2 years, but none goes below a maximum threshold of 1 year.

The Article also sets out mandatory information that must be part of the European Production Order to enable the service provider to identify and produce the requested data. The reasoning with the grounds for the necessity and proportionality of this measure are also part of the European Production Order.

The European Production Order is implemented by issuing a European Production Order Certificate (EPOC) (see Article 8), which is translated and sent to the service provider. The EPOC contains the same mandatory information as the Order, except for the grounds for the necessity and proportionality of the measure or further details about the case.

In situations where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company, typically in case of hosting or software services, the company itself should be the primary addressee of a request by the investigating authorities. This may require an EIO or MLA procedure where the company would not be a service provider covered by the scope of this Regulation. The service provider can only be addressed by a European Production Order if it would not be appropriate to address the request to the company, in particular where this would create a risk of jeopardising the investigation, for example where the company itself is under investigation.

Before issuing a European Production Order, the issuing authority also has to take into account potential immunities and privileges under the law of the Member State of the service provider or any impact on fundamental interests of that Member State such as national security and defence. The aim of this provision is to ensure that immunities and privileges which protect the data sought in the Member State of the service provider are taken into account in the issuing State, in particular where they provide for a higher protection than the law of the issuing State.

*Article 6: Conditions for issuing a European Preservation Order*

A European Preservation Order is subject to similar conditions as the European Production Order. It can be issued for any offence in line with the other conditions set out in Article 6. Its aim is to prevent the removal, deletion or alteration of relevant data in situations where it may take more time to obtain the production of this data, for example because judicial cooperation

channels will be used. Given, for example, that the EIO in general can be issued for any offence without limiting it to any thresholds, the European Preservation Order shall not be limited either. Otherwise, this instrument would not be effective. To enable investigating authorities to act fast and given that the relevant request to produce the data will be the subsequent request where all the conditions will again be scrutinised, European Preservation Orders may also be issued or validated by a prosecutor.

*Article 7: Addressee of a European Production Order or a European Preservation Order*

European Production Orders and European Preservation Orders should be addressed to a legal representative designated by the service provider for the purpose of gathering evidence in criminal proceedings in accordance with the Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. The transmission will be in form of a European Production Order Certificate ('EPOC') or a European Preservation Order Certificate ('EPOC-PR') as referred to in Article 8. This legal representative will be responsible for their reception and timely and complete execution. This leaves service providers the choice of how to organise themselves to produce the data ordered by Member State authorities.

Where no legal representative has been appointed, Orders may be addressed to any establishment of the service provider in the Union. This fall-back option serves to ensure effectiveness of the system in case the service provider has not (yet) nominated a dedicated representative, for example where there is no obligation to nominate a legal representative in accordance with the Directive, because service providers are established and active only in one Member State or in cases where an obligation to nominate a legal representative is not yet in force, before the transposition deadline of the Directive.

In case of non-compliance by the legal representative, there are two situations where the issuing authority may address any establishment of the service provider in the Union: in emergency cases as defined in Article 9(2), and in cases where the legal representative does not comply with its obligations under Article 9 and 10, and where the issuing authority believes that there are clear risks of loss of data.

*Article 8: European Production and Preservation Order Certificate*

The EPOC and EPOC-PR serve to transmit the Orders to the addressee defined in Article 7. Templates for both Certificates are provided in Annex I and II of the Regulation; they need to be translated into one of the official languages of the Member State where the addressee is located. The service provider may declare that Orders will be accepted also in other official languages of the Union. The aim of the Certificates is to provide all the necessary information to be transmitted to the addressee in a standardised format, minimising sources of error, allowing an easy identification of the data and avoiding as much as possible free text and therefore reducing translation costs. The full reasoning with the grounds for necessity and proportionality or further details about the case shall not be included in the Certificate to avoid jeopardising the investigations. It is therefore only needed as part of the Order itself to later allow the suspect to challenge it during the criminal proceedings.

Some service providers have already established platforms for the submission of requests by law enforcement. The use of these platforms shall not be prevented by the Regulation, as it offers many advantages, including the possibility of an easy authentication and a secure transmission of the data. However, these platforms have to allow for the submission of the

EPOC and the EPOC-PR in the format as provided for in Annexes I and II, without requesting additional data pertaining to the Order.

Platforms established by Member States or Union bodies may also provide secure means of transmission and facilitate authentication of the Orders and the gathering of statistics. Consideration should be given to a possible expansion of the eCodex and SIRIUS platforms to include a secure connection to service providers for the purposes of the transmission of the EPOC and EPOC-PR and, where appropriate, responses from the service providers.

*Article 9: Execution of an EPOC*

Article 9 obliges addressees to reply to EPOCs, and introduces mandatory deadlines. The normal deadline is 10 days, while authorities may set a shorter deadline where justified. Moreover, in emergency cases, defined as a situation where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure, the deadline is 6 hours.

The provision also ensures the possibility of a dialogue between addressee and issuing authority. If the EPOC is incomplete, manifestly incorrect or does not contain sufficient information for the service provider to execute the EPOC, the addressee shall contact the issuing authority and seek clarification, using the form in Annex III. It shall also inform the issuing authority in cases where it cannot provide the data due to *force majeure*, or a de facto impossibility. This is the case if, for example, the person whose data is sought was neither a customer of this service or — for example under other privacy obligations — the data has lawfully been deleted by the service provider before it or its legal representative received the Order. The issuing authority would need to be aware of these circumstances to react fast, to perhaps gather the electronic evidence from another service provider and to prevent the issuing authority from initiating an enforcement procedure where this would not make any sense.

If the addressee does not provide the information at all, or not in an exhaustive or timely manner, for reasons other than those mentioned above, it has to inform the issuing authority of the reasons in the form included in Annex III. Addressees can therefore raise any issue related to the execution of the EPOC with the issuing authority. This allows the issuing authority to correct or reconsider the EPOC at an early stage, before the enforcement phase.

Where the data is not produced immediately, in particular where a dialogue is launched between the addressee and the issuing authority, meaning that the deadlines of Article 9(1) will no longer be kept, the service provider has an obligation to preserve the data to avoid losing it, upon receipt of the EPOC, provided that the data can be identified. The preservation may be for the clarified EPOC or a subsequent MLA or EIO request that will be sent instead of the original EPOC.

*Article 10: Execution of an EPOC-PR*

Execution of an EPOC-PR requires preserving the data available at the time of receipt of the Order. Service providers should preserve the data as long as necessary to produce the data upon request, provided that the issuing authority confirms within 60 days after having issued the Order that it has launched the subsequent request for production. This requires that at least some formal steps have been taken, such as sending a mutual legal assistance request for translation.

On the other hand, preservation requests should only be made or maintained as long as necessary to enable a subsequent request to be made to produce this data. To avoid unnecessary or overly long preservation, the authority that issued the European Preservation Order shall inform the addressee as soon as a decision is taken to refrain from issuing, or to withdraw a production order or a judicial cooperation request.

This provision also ensures the possibility of a dialogue between addressee and issuing authority, similar to the provisions of Article 9. If the EPOC-PR is incomplete, manifestly incorrect or does not contain sufficient information for the service provider to execute the EPOC-PR, the addressee shall contact the issuing authority and seek clarification, using the Form in Annex III. It shall also inform the issuing authority in cases where it cannot provide the data for circumstances that are considered as *force majeure*, or de facto impossibility, or for other reasons.

*Article 11: Confidentiality and user information*

The confidentiality of the ongoing investigation, including the fact that there has been an Order to obtain relevant data, has to be protected. This Article is inspired by Article 19 of the EIO Directive. It provides for the obligation of the addressee and if different, the service provider, to preserve the confidentiality of the EPOC or EPOC-PR, in particular by refraining from informing the person whose data is being sought where requested by the issuing authority in order to safeguard the investigation of criminal offences, in compliance with Article 23 GDPR.

On the other hand, it is important, including for exercising legal remedies, that the person whose data was sought is informed. Where this is not done by the service provider upon request of the issuing authority, the issuing authority shall inform the person in accordance with Article 13 of the Law Enforcement Data Protection Directive once there is no longer a risk of jeopardising the investigation and include information about available legal remedies. Because of the lesser interference with rights involved, such information is not provided for in case of a European Preservation Order, but only for European Production Orders.

*Article 12: Reimbursement of costs*

If this is provided by the national law of the issuing State for domestic orders in similar domestic cases, service providers may also claim reimbursement of their costs from the issuing State in accordance with the national law of the issuing State. This ensures equal treatment of service providers addressed by a domestic order and those addressed by an EPOC by the same Member State, if that Member State has made the choice to reimburse certain service providers. On the other hand, the proposed Regulation does not harmonise the reimbursement of costs, as Member States have made diverging choices in that respect.

The costs can be claimed either directly by the service provider, or via its legal representative. They can only be reimbursed once.

***Chapter 3: Sanctions and enforcement***

*Article 13: Sanctions*

Member States shall ensure that there are effective, proportionate and deterrent pecuniary fines available when service providers do not comply with their obligations under Article 9,

10 or 11. This shall be without prejudice to national laws providing for the imposition of criminal sanctions for such situations.

*Article 14: Procedure for enforcement*

Article 14 provides for a procedure to enforce the Orders in case of non-compliance with the help of the Member State where the addressee of the transmitted Certificate is located. Depending on the initial addressee, this is either the Member State of the service provider or of the legal representative. The issuing authority transfers the full Order including the reasoning on necessity and proportionality, accompanied by the Certificate, to the competent authority in the enforcing State, which shall enforce it in accordance with its national law using, if necessary, the sanctions mentioned in Article 13. If the Order is transmitted for enforcement to the enforcing State, the enforcing authority may decide not to recognise and enforce the Order if upon receipt it considers that one of the limited grounds for opposition apply, and after consulting with the issuing authority. In addition, should the procedure for enforcement be initiated, the addressee itself will be able to oppose the Order before the enforcing authority. The addressee may do this on the basis of any of such grounds, excluding immunities and privileges but including cases where it is apparent that the Order was not issued or validated by a competent authority or that compliance would manifestly violate the Charter of Fundamental Rights of the European Union or be manifestly abusive. For example, an Order requesting the production of content data pertaining to an undefined class of people in a geographical area or with no link to concrete criminal proceedings would ignore in a manifest way the conditions for issuing a European Production Order set out in this Regulation and would be apparent already from the content of the Certificate itself. Other grounds can only be invoked by the person whose data is being sought, in the framework of their own legal remedies in the issuing State (see Article 17 below). In addition, service providers shall have a legal remedy against the decision of the enforcing authority imposing a penalty on them.

The enforcement procedure contains several deadlines for the enforcing and issuing authority to avoid further delays during this procedure.

***Chapter 4: Remedies***

*Articles 15 and 16: Review procedure in case of conflicting obligations deriving from the law of a third country*

Articles 15 and 16 provide for a review procedure in case service providers headquartered in third countries are faced with conflicting obligations. These provisions are also of great importance to ensure the protection of individual rights and international comity. By setting a high standard, they aim to encourage third countries to provide for a similar level of protection. In the opposite situation, where authorities of a third country seek to obtain data of an EU citizen from an EU service provider, Union or Member States laws protecting fundamental rights, such as the data protection *acquis*, may similarly prevent disclosure. The European Union expects third countries to respect such prohibitions as this proposal does.

The procedure in Article 15 can be triggered by the addressee if compliance with a European Production Order would cause infringement of the law(s) of a third country that prohibits disclosure of the data on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence. The addressee is required to inform the issuing authority by reasoned objection of the grounds for its conclusion that there are conflicting obligations.

Such reasoned objection cannot be based on the mere fact that similar provisions do not exist in the law of the third country nor on the only circumstance that the data is stored in a third country. The reasoned objection shall be raised pursuant to the procedure set out in Article 9(5) for notifying intent not to comply, using the form provided in Annex III.

On the basis of this reasoned objection, the issuing authority shall review its own Order. If the issuing authority chooses to withdraw the Order, the procedure ends. If the issuing authority would like to uphold the Order, the case is transferred to the competent court of its Member State. The court then assesses, on the basis of the reasoned objection and taking into account all relevant facts of the case, whether the third country law applies to the specific case at hand and — if it does apply — whether a conflict exists in the specific case at hand. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations.

If the court determines that there is in fact a conflict with obligations arising from laws protecting fundamental rights of individuals or fundamental interests of the third country related to national security or defence, the court must request an opinion of the relevant third country via the national central authorities of the third country. If the third country consulted confirms the existence of the conflict and objects to the execution of the Order, the court must withdraw the Order.

If the conflict arises on the basis of other third country legislation that does not serve to protect either the fundamental rights of individuals or fundamental interests of the third country related to national security or defence, then the court shall take its decision based on a balancing of the interests in favour of and against upholding the Order.

The conditions set out in Article 9, especially the preservation obligations described in Article 9(6), are also applicable in situations where conflicting obligations deriving from the law of a third country occur. Where the court comes to the determination that the Order is to be upheld, the issuing authority and the service provider are informed with a view to proceeding to its execution. Where the Order is lifted, a separate European Preservation Order may be issued to ensure availability of the data where it might be obtained through a mutual legal assistance request.

Given that the European Preservation Order itself does not result in data disclosure and therefore does not give rise to similar concerns, the review procedure is limited to the European Production Order.

*Article 17: Effective remedies*

This provision ensures that persons affected by the European Production Order have effective remedies. These remedies are exercised in the issuing State in accordance with national law. For suspects and accused persons, remedies are normally exercised during the criminal proceedings. No specific remedies are made available for the European Preservation Order, which in and of itself does not allow for data disclosure, other than in those cases where it is followed by a European Production Order or another instrument leading to disclosure, which then give rise to specific remedies.

Persons whose data was sought without them being suspects or accused persons in criminal proceedings shall also have a right to a legal remedy in the issuing State. All these rights are

without prejudice to any remedies available under the Law Enforcement Data Protection Directive and the GDPR.

Unlike what is provided for service providers, the Regulation does not limit the possible grounds for all these persons to challenge the legality of the Order. These grounds include the necessity and proportionality of the Order.

The exercise of remedies in the issuing State does not burden affected persons in a disproportionate manner. As is the case with Orders that are enforced through other forms of judicial cooperation, the courts in the issuing State are best-placed to review the legality of European Production Orders issued by their own authorities and to assess the compatibility with their own national law. In addition, during the enforcement stage, addressees can separately oppose the enforcement of the EPOC or of the EPOC-PR in their host Member State on the basis of a list of grounds enumerated in the Regulation (see Article 14 above).

*Article 18: Ensuring privileges and immunities under law of receiving State*

This provision pursues the same objective as Article 5(7) to ensure that immunities and privileges which protect the data sought in the Member State of the service provider are taken into account in the issuing State, in particular where there are differences between those Member States, as well as fundamental interests of that Member State such as national security and defence. Article 18 provides that the court in the issuing State has to take them into account as if they were provided for under their national law. Because of the differences between Member States when assessing the relevance and admissibility of evidence, the provision leaves some flexibility to the courts as to how to take them into account.

***Chapter 5: Final provisions***

*Article 19: Monitoring and reporting*

This article requires the Member States to report specific information related to the application of the Regulation with a view to assist the Commission in the exercise of its duties under Article 24. The Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation.

*Article 20: Amendments to the Certificates and the Forms*

The Certificates and the forms contained in Annexes I, II, and III of this proposal will make it easier to execute an EPOC and an EPOC-PR. For this reason, it is necessary in the future to be able to address a possible need to improve the content of the Certificate and the form as quickly as possible. Amending the three annexes through the ordinary legislative procedure does not correspond to this requirement, and they constitute non-essential elements of the legislative acts, the main elements being defined in Article 8. Therefore, a faster and more flexible procedure for amendments through delegated acts is laid down in Article 20.

*Article 21: Exercise of delegation*

This article lays down the conditions under which the Commission has the power to adopt delegated acts to provide for necessary amendments to the Certificate and the forms annexed to the proposal. It lays down a standard procedure for adopting such delegated acts.

*Article 22: Notifications*

Member States are required to notify to the Commission who the competent issuing and enforcing authorities are, and which courts are competent to deal with reasoned objections of service providers in case of a conflict of law.

*Article 23: Relationship to European Investigation Orders*

This provision clarifies that the Regulation does not prevent Member State authorities from issuing European Investigation Orders in accordance with Directive 2014/41/EU to obtain electronic evidence.

*Article 24: Evaluation*

This provision sets out that the Commission shall carry out an evaluation of this Regulation in line with the Commission's Better Regulation Guidelines and pursuant to paragraph 22 of the Interinstitutional Agreement of 13 April 2016[25]. The Commission will report to the European Parliament and the Council on the findings of the evaluation, including an assessment of the need to enlarge its scope to services not yet covered but which may become more relevant for investigations, 5 years after the entry into force of the proposed Regulation.

*Article 25: Entry into force*

The proposed Regulation will enter into force the twentieth day after its publication in the Official Journal. The Regulation will then apply 6 months after its date of entry into force.

[25] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016; OJ L 123, 12.5.2016, p. 1–14.

2018/0108 (COD)

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**on European Production and Preservation Orders for electronic evidence in criminal matters**

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[26],

Acting in accordance with the ordinary legislative procedure,

Whereas:

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

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

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

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

(5) In the Joint Communication on Resilience, Deterrence and Defence of 13 September 2017[27], the Commission emphasised that effective investigation and prosecution of

[26] OJ C , , p. .

cyber-enabled crime was a key deterrent to cyber-attacks, and that today's procedural framework needed to be better adapted to the internet age. Current procedures at times could not match the speed of cyber-attacks, which create particular need for swift cooperation across borders.

(6) The European Parliament echoed these concerns in its Resolution on the fight against cybercrime of 3 October 2017[28], highlighting the challenges that the currently fragmented legal framework can create for service providers seeking to comply with law enforcement requests and calling on the Commission to put forward a Union legal framework for electronic evidence with sufficient safeguards for the rights and freedoms of all concerned.

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

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

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

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

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

---

27 JOIN(2017) 450 final.

28 2017/2068(INI).

(12) This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. These include the right to liberty and security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of the legality and proportionality, as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence. In case the issuing Member State has indications that parallel criminal proceedings may be ongoing in another Member State, it shall consult the authorities of this Member State in accordance with Council Framework Decision 2009/948/JHA[29].

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

(14) This Regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in Directives 2010/64/EU[30], 2012/13/EU[31], 2013/48/EU[32], 2016/343[33], 2016/800[34] and 2016/1919[35] of the European Parliament and of the Council.

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

(16) The service providers most relevant for criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered

---

29 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).

30 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).

31 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).

32 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).

33 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).

34 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).

35 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).

by this Regulation. Providers of electronic communications services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. The categories of information society services included here are those for which the storage of data is a defining component of the service provided to the user, and refer in particular to social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and other hosting services, including where the service is provided via cloud computing. Information society services for which the storage of data is not a defining component of the service provided to the user, and for which it is only of an ancillary nature, such as legal, architectural, engineering and accounting services provided online at a distance, should be excluded from the scope of this Regulation, even where they may fall within the definition of information society services as per Directive (EU) 2015/1535.

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

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

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

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

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

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

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

(24) The European Production Order and the European Preservation Order are investigative measures that should be issued only in the framework of specific criminal proceedings against the specific known or still unknow perpetrators of a concrete criminal offence that has already taken place, after an individual evaluation of the proportionality and necessity in every single case.

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

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

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

(28) A substantial connection to the Union should also be relevant to determine the ambit of application of the present Regulation. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be assessed on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial

connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.[36] On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302[37] cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.

(29) A European Production Order should only be issued if it is necessary and proportionate. The assessment should take into account whether the Order is limited to what is necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the individual case only.

(30) When a European Production or Preservation Order is issued, there should always be a judicial authority involved either in the process of issuing or validating the Order. In view of the more sensitive character of transactional and content data, the issuing or validation of European Production Orders for production of these categories requires review by a judge. As subscriber and access data are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent prosecutors.

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

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

---

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

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

described in the Directive 2017/541/EU do not require the minimum maximum threshold of 3 years.

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

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

(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege), are referred to in other mutual recognition instruments such as the European Investigation Order. Their range and impact differ according to the applicable national law that should be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order if a similar order would be available in a comparable domestic situation. In addition to this basic principle, immunities and privileges which protect access, transactional or content data in the Member State of the service provider should be taken into account as far as possible in the issuing State in the same way as if they were provided for under the national law of the issuing State. This is relevant in particular should the law of the Member State where the service provider or its legal representative is addressed provide for a higher protection than the law of the issuing State. The provision also ensures respect for cases where the disclosure of the data may impact fundamental interests of that Member State such as national security and defence. As an additional safeguard, these aspects should be taken into account not only when the Order is issued, but also later, when assessing the relevance and admissibility of the data concerned at the relevant stage of the criminal proceedings, and if an enforcement procedure takes place, by the enforcing authority.

(36) The European Preservation Order may be issued for any offence. Its aim is to prevent the removal, deletion or alteration of relevant data in situations where it may take more time to obtain the production of this data, for example because judicial cooperation channels will be used.

(37) European Production and Preservation Orders should be addressed to the legal representative designated by the service provider. In the absence of a designated legal representative, Orders can be addressed to an establishment of the service provider in the Union. This can be the case where there is no legal obligation for the service provider to nominate a legal representative. In case of non-compliance by the legal

representative in emergency situations, the European Production or Preservation Order may also be addressed to the service provider alongside or instead of pursuing enforcement of the original Order according to Article 14. In case of non-compliance by the legal representative in non-emergency situations, but where there are clear risks of loss of data, a European Production or Preservation Order may also be addressed to any establishment of the service provider in the Union. Because of these various possible scenarios, the general term 'addressee' is used in the provisions. Where an obligation, such as on confidentiality, applies not only to the addressee, but also to the service provider if it is not the addressee, this is specified in the respective provision.

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

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

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

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

(42) Upon receipt of a European Preservation Order Certificate ('EPOC-PR'), the service provider should preserve requested data for a maximum of 60 days unless the issuing authority informs the service provider that it has launched the procedure for issuing a

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

(43) Service providers and their legal representatives should ensure confidentiality and when requested by the issuing authority refrain from informing the person whose data is being sought in order to safeguard the investigation of criminal offences, in compliance with Article 23 of Regulation (EU) 2016/679[38]. However, user information is an essential element in enabling review and judicial redress and should be provided by the authority if the service provider was asked not to inform the user, where there is no risk of jeopardising ongoing investigations, in accordance with the national measure implementing Article 13 of Directive (EU) 2016/680[39].

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

(45) The enforcement procedure is a procedure where the addressee can oppose the enforcement based on certain restricted grounds. The enforcing authority can refuse to recognise and enforce the Order based on the same grounds, or if immunities and privileges under its national law apply or the disclosure may impact its fundamental interests such as national security and defence. The enforcing authority should consult the issuing authority before refusing to recognise or enforce the order, based on these grounds. In case of non-compliance, authorities can impose sanctions. These sanctions should be proportionate also in view of specific circumstances such as repeated or systemic non-compliance.

(46) Notwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with an EPOC or an EPOC-PR.

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

---

38 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).

39 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).

Order would prevent service providers from complying with legal obligation deriving from a third State's law.

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

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

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

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

(52) In all other cases of conflicting obligations, unrelated to fundamental rights of the individual or fundamental interests of the third country related to national security or defence, the court should take its decision on whether to uphold the European Production Order by weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible

consequences for the service provider of having to comply with the Order. Importantly for cyber-related offences, the place where the crime was committed covers both the place(s) where the action was taken and the place(s) where the effects of the offence materialised.

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

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

(55) In addition, during the enforcement procedure and subsequent legal remedy, the addressee may oppose the enforcement of a European Production or Preservation Order on a number of limited grounds, including it not being issued or validated by a competent authority or it being apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or is manifestly abusive. For example, an Order requesting the production of content data pertaining to an undefined class of people in a geographical area or with no link to concrete criminal proceedings would ignore in a manifest way the conditions for issuing a European Production Order.

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

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

be considered, such as notified national electronic identification systems or trust services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

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

(60) In order to effectively address a possible need for improvement regarding the content of the EPOCs and EPOC-PRs and of the Form to be used to provide information on the impossibility to execute the EPOC or EPOC-PR, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[40]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

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

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

(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic evidence across borders, cannot be sufficiently achieved by the Member States given its cross-border nature, but can rather be better achieved at Union level,

---

40 OJ L 123, 12.5.2016, p. 1.

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

the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(64) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, *[the United Kingdom /Ireland has notified its wish to take part in the adoption and application of this Regulation] or [and without prejudice to Article 4 of that Protocol, the United Kingdom/Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]*.

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

(66) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[42] and delivered an opinion on (…)[43],

HAVE ADOPTED THIS REGULATION:

# Chapter 1: Subject matter, definitions and scope

*Article 1*
*Subject matter*

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

2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities in this respect shall remain unaffected.

---

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

43 OJ C , , p. .

*Article 2*
*Definitions*

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

(1) ‘European Production Order’ means a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence;

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

(3) ‘service provider’ means any natural or legal person that provides one or more of the following categories of services:

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

  (b) information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[44] for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers;

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

(4) ‘offering services in the Union’ means:

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

  (b) having a substantial connection to the Member State(s) referred to in point (a);

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

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

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

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

  (b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber

[44] 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).

or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;

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

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

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

(11) 'information system' means information system as defined in point (a) of Article 2 of Directive 2013/40/EU of the European Parliament and of the Council[45];

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

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

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

(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC[46].

---

45 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).

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

*Article 3*
*Scope*

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

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

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

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

*Article 4*
*Issuing authority*

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

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

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

2. A European Production Order for transactional and content data may be issued only by:

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

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

3. A European Preservation Order may be issued by:

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

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

Preservation Order under this Regulation, by a judge, a court, an investigating judge or a prosecutor in the issuing State.

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

*Article 5*
*Conditions for issuing a European Production Order*

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

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

3. European Production Orders to produce subscriber data or access data may be issued for all criminal offences.

4. European Production Orders to produce transactional data or content data may only be issued

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

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

– offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA[47];

– offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[48];

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

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[49].

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

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

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

---

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

48 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).

49 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).

(c) the persons whose data is being requested, except where the sole purpose of the order is to identify a person;

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

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

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

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

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

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

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

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

*Article 6*
*Conditions for issuing a European Preservation Order*

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

2. It may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order. European Preservation Orders to preserve data may be issued for all criminal offences.

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

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

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

(c) the persons whose data shall be preserved, except where the sole purpose of the order is to identify a person;

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

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

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

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

*Article 7*

*Addressee of a European Production Order and a European Preservation Order*

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

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

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

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

*Article 8*

*European Production and Preservation Order Certificate*

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

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

2. The EPOC or the EPOC-PR shall be directly transmitted by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity.

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

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

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

authority. The grounds for the necessity and proportionality of the measure or further details about the investigations shall not be included.

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

*Article 9*
*Execution of an EPOC*

1. Upon receipt of the EPOC, the addressee shall ensure that the requested data is transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure.

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

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

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

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

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

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

*Article 10*
*Execution of an EPOC-PR*

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

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

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

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

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

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

*Article 11*
*Confidentiality and user information*

1. Addressees and, if different, service providers shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and where requested by the issuing authority, shall refrain from informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings.

2. Where the issuing authority requested the addressee to refrain from informing the person whose data is being sought, the issuing authority shall inform the person whose data is being sought by the EPOC without undue delay about the data production. This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings.

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

*Article 12*
*Reimbursement of costs*

The service provider may claim reimbursement of their costs by the issuing State, if this is provided by the national law of the issuing State for domestic orders in similar situations, in accordance with these national provisions.

# Chapter 3: Sanctions and enforcement

*Article 13*
*Sanctions*

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

*Article 14*
*Procedure for enforcement*

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

2. Upon receipt, the enforcing authority shall without further formalities recognise a European Production Order or European Preservation Order transmitted in accordance with paragraph 1 and shall take the necessary measures for its enforcement, unless the enforcing authority considers that one of the grounds provided for in paragraphs 4 or 5 apply or that the data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its

fundamental interests such as national security and defence. The enforcing authority shall take the decision to recognise the Order without undue delay and no later than 5 working days after the receipt of the Order.

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

4. The addressee may only oppose the enforcement of the European Production Order on the basis of the following grounds:

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

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

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

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

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

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

5. The addressee may only oppose the enforcement of the European Preservation Order on the basis of the following grounds:

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

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

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

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

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

6. In case of an objection by the addressee, the enforcing authority shall decide whether to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority in accordance with paragraph 7.

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

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

9. If the enforcing authority obtains the data from the addressee, it shall transmit it to the issuing authority within 2 working days, unless the data concerned is protected by an immunity or privilege under its own domestic law or it impacts its fundamental interests such as national security and defence. In such case, it shall inform the issuing authority of the reasons for not transmitting the data.

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

# Chapter 4: Remedies

*Article 15*
*Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country*

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

2. The reasoned objection shall include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country.

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

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

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

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

4. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks

to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations.

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

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

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

*Article 16*

*Review procedure in case of conflicting obligations based on other grounds*

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

2. The reasoned objection must include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country.

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

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

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

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

5. If the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. If the competent court establishes that the third country law, when applied to the specific circumstances of the case under examination, prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or withdraw the Order in particular on the basis of the following factors:

(a) the interest protected by the relevant law of the third country, including the third country's interest in preventing disclosure of the data;

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

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

the place where the criminal offence in question was committed;

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

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

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

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

*Article 17*
*Effective remedies*

1. Suspects and accused persons whose data was obtained via a European Production Order shall have the right to effective remedies against the European Production Order during the criminal proceedings for which the Order was issued, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

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

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

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

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

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

*Article 18*
*Ensuring privileges and immunities under the law of the enforcing State*

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

# Chapter 5: Final provisions

*Article 19*
*Monitoring and reporting*

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

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

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

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

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

   (d) the number of European Production Orders transmitted and received for enforcement to an enforcing State by type of data requested, service providers

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

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

*Article 20*
*Amendments to the Certificates and the Forms*

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

*Article 21*
*Exercise of delegation*

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

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

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

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[50].

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

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

*Article 22*
*Notifications*

1. By *[date of application of this Regulation]* each Member State shall notify the Commission of the following:

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

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

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

(c) the courts competent to deal with reasoned objections by addressees in accordance with Articles 15 and 16.

2. The Commission shall make the information received under this Article publicly available, either on a dedicated website or on the website of the European Judicial Network referred to in Article 9 of the Council Decision 2008/976/JHA[51].

*Article 23*
*Relationship to European Investigation Orders*

Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for the gathering of evidence that would also fall within the scope of this Regulation.

*Article 24*
*Evaluation*

By *[5 years from the date of application of this Regulation]* at the latest, the Commission shall carry out an evaluation of the Regulation and present a report to the European Parliament and to the Council on the functioning of this Regulation, which shall include an assessment of the need to enlarge its scope. If necessary, the report shall be accompanied by legislative proposals. The evaluation shall be conducted according to the Commission's better regulation guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

*Article 25*
*Entry into force*

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

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

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

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

Done at Strasbourg,

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

EUROPEAN
COMMISSION

Brussels, 17.4.2018
COM(2018) 225 final

ANNEXES 1 to 3

**ANNEXES**

**to the**

**Proposal for a Regulation of the European Parliament and of the Council**

**on European Production and Preservation Orders for electronic evidence in criminal matters**

{SWD(2018) 118 final} - {SWD(2018) 119 final}

**ANNEX I**

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

Under Regulation (EU)….[1] the addressee of the European Production Order Certificate (EPOC) must execute the EPOC and must transmit the requested data to the authority indicated under point (i) of Section G of the EPOC. If the data is not produced, the addressee must, upon receipt of the EPOC, preserve the data requested, unless the information in the EPOC does not allow it to identify this data. Preservation shall be upheld until the data is produced or until the issuing authority or where applicable the enforcing authority,indicates that it is no longer neccessary to preserve and produce data.

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

SECTION A:

Issuing State: ……..

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

Addressee:……

SECTION B: Deadlines

The data requested must be produced (tick the appropriate box and complete, if necessary):

□ within 10 days at the latest

□ within 6 hours at the latest in the event of an emergency involving:

□ an imminent threat to a person's life or physical integrity. Justification, if necessary: …….

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

□ within another time period (specify): ……..……..….. because of :

□ an imminent danger that the requested data will be deleted
□ other urgent investigative measures
□ an imminent trial date
□ a suspect / accused in custody
□ other reasons: …….....

[1] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (*OJ L …*)

SECTION C: User information

Please note that (tick, if applicable):

□ the addresee **must refrain from informing the person** whose data is being sought of the EPOC.

SECTION D: Electronic evidence to be produced

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

□ subscriber data, including but not limited to:

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

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

□ type of service, including identifier (phone number, IP address, SIM-card number, MAC address) and associated device(s)

□ profile information (user name, profile photo)

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

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

□ PUK-codes

□ access data, including but not limited to:

□ IP connection records / logs for identification purposes

□ transactional data:

□ traffic data, including but not limited to:

(a) for (mobile) telephony:

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

□ time and duration of connections

□ call attempts

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

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

(b) for internet:

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

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

□ volume of data

(c) for hosting:

□ logfiles

□ tickets

□ purchase history

□ other transactional data, including but not limited to:

□ prepaid balance charging history
□ contacts list

□ content data, including but not limited to:

□ (web)mailbox dump
□ online storage dump (user generated data)
□ pagedump
□ message log/backup
□ voicemail dump
□ server contents
□ device backup

(ii) The information below is made available to you to allow executing the EPOC:

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

(iii) If applicable, the time range requested to be produced:

……..…….

(iv) Please note that (tick and complete if applicable):

□ the requested data was preserved in accordance with an earlier request for preservation issued by…….……..……
(indicate the authority, and, if available, the date of transmission of request and reference number) and transmitted to ……..……
(indicate the service provider/ legal representative/ public authority to which it was transmitted and, if available, the reference number given by the addressee)

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

……..…….……

The current EPOC is issued for transactional and / or content data and concerns (tick the relevant box(es), if applicable):

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

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

□ offence(s) as defined in Articles 3, 4 and 5 of Council Framework Decision 2001/413/JHA;

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

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

□ offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council.

(vi) Please note that (tick, if applicable):

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

(vii) Any other relevant information:

……

SECTION E: Details of the authority which issued the EPOC

The type of authority which issued this EPOC (tick the relevant box):

□ judge, court, or investigating judge

□ public prosecutor (for subscriber and access data)

□ public prosecutor (for transactional and content data) → please complete also Section (F)

□ any other competent authority as defined by the issuing State → please complete also Section (F)

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

Name of authority:……..……..

Name of its representative:…….……...……

Post held (title/grade):……...……

File No:….……..……..

Address:……..……..

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

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

Email:……...…….

Date: ……..……

Official stamp (if available) and signature:……...……

SECTION F: Details of the authority which validated the EPOC

The type of authority which has validated this EPOC (tick the relevant box, if applicable):

□ judge, court or investigating judge
□ public prosecutor (for subscriber and access data)

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

Name of authority:……

Name of its representative:……...……

Post held (title/grade):……..……..……

File No:…….……..…….

Address: ……...……..……..

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

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

Email:…….…..…….

Date: …….…….

Official stamp (if available) and signature:……..……

SECTION G: Transfer of data and contact details

(i) Authority to whom the data has to be transferred (tick and complete, if neccessary):

□ issuing authority,
□ validating authority
□ other competent authority as defined by the issuing State:.....

(ii) Auhority/contact point which can be contacted for any question related to the execution of the EPOC:…….……

_____

## ANNEX II

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

Under Regulation (EU) ...[2] the addressee of the European Preservation Order Certificate (EPOC-PR) must, without undue delay after receiving the EPOC-PR preserve the data requested. The preservation will cease after 60 days, unless the issuing authority confirms that a subsequent request for production has been launched. If the issuing authority confirms within those 60 days that a subsequent request for production has been launched, the addressee must preserve the data for as long as necessary to produce the data once the subsequent request for production is served.

The addressee must take necessary measures to ensure the **confidentiality** of the EPOC-PR and of the data preserved or produced.

SECTION A:

Issuing State: ……

NB: details of issuing authority to be provided at the end (Sections D and E)

Addressee:……...……..……..…

SECTION B: User information

Please note that (tick, if applicable):

□ the addresee **must refrain from informing the person** whose data is being sought of the EPOC-PR.

SECTION C: Electronic evidence to be preserved

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

□ subscriber data, including but not limited to:

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

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

□ type of service, including identifier (phone number, IP-address, SIM-card number, MAC-address) and associated device(s)

□ profile information (user name, profile photo)

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

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

[2] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (*OJ L …*)

□ PUK-codes

□ access data, including but not limited to:

□ IP connection records / logs for identification purposes

□ transactional data:

□ traffic data, including but not limited to:

(a) for (mobile) telephony:

□ outgoing (A) and incoming (B) identifiers (phone number, IMSI, IMEI)
□ time and duration of connections
□ call attempts
□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection
□ bearer / teleservice used (e.g. UMTS, GPRS)

(b) for internet:

□ routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID)
□ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection
□ volume of data

(c) for hosting:

□ logfiles
□ tickets

□ purchase history

□ other transactional data, including but not limited to:

□ prepaid balance charging history
□ contacts list

□ content data, including but not limited to:

□ (web)mailbox dump
□ online storage dump (user generated data)
□ pagedump
□ message log/backup
□ voicemail dump
□ server contents
□ device backup

(ii) Information below is made available to you to allow executing the EPOC-PR:

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

□ Other: ……

(iii) If applicable, the time range requested to be preserved:

……..……

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

……..……..……

(v) Any other relevant information:

……..

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

The type of authority which issued this EPOC-PR (tick the relevant box):

□ judge, court, or investigating judge

□ public prosecutor

□ any other competent authority as defined by the law of the issuing State → please complete also Section (E)

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

Name of authority:……

Name of its representative:……..……

Post held (title/grade):…….…….

File No:.…….……..

Address:.…….……..

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

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

Email:…….…….

Date: ……

Official stamp (if available) and signature:……...……

SECTION E: Details of the authority which validated the EPOC-PR

The type of authority which has validated this EPOC-PR (tick the relevant box):

□ judge, court or investigating judge

□ public prosecutor

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

Name of authority:……..…

Name of its representative:……..……

Post held (title/grade):……

File No:……..……..

Address: ……..

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

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

Email:……..……

Date: ……..

Official stamp (if available) and signature:……...……

SECTION F: Contact details

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

**ANNEX III**

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

SECTION A:

The following information concerns:

□ the European Production Order (EPOC)

□ the European Preservation Order (EPOC-PR)

SECTION B:

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

Authority which issued the EPOC / EPOC-PR: ……..……

If applicable, authority which validated the EPOC / EPOC-PR: …….

SECTION C:

File reference of the addressee of the EPOC / EPOC-PR: …….…….

File reference of the issuing authority: ……

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

If available, date of transmission of the EPOC / EPOC-PR: ……...……

SECTION D: Reasons for non-execution

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

□ the EPOC / EPOC-PR is incomplete

□ the EPOC / EPOC-PR contains manifest errors

□ the EPOC / EPOC-PR does not contain sufficient information

□ *force majeure* or de facto impossibility not attributable to the addressee or the service provider

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

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

□ the European Production Order has not been issued for an offence provided for by Article 5(4) of Regulation (EU)…

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

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

□ based on the sole information contained in the EPOC / EPOC-PR, it is apparent that the EPOC / EPOC-PR manifestly violates the Charter or is manifestly abusive

□ compliance with the European Production Order would conflict with the applicable law(s) of a third country prohibiting disclosure of the data concerned.

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

…….

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

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

- title of the law(s) of the third country, including the relevant provision(s):

…….

- text of the relevant provision(s):

……..……..…….

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

□ fundamental rights of individuals (please specify):

…….……..

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

……..

□ other interests (please specify):

……..…….

- explain why the law is applicable in this case:

……..……..……..

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

……..……

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

…….……..

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

……...……..…...

SECTION F: Information that is requested

Further information is required from the issuing authority for the EPOC/ EPOC-PR to be executed (complete, if applicable):

……..……..

SECTION G: Preservation of data

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

□ will be preserved until data is produced or until the issuing authority or where applicable the enforcing authority informs that it is no longer necessary to preserve and produce data

□ will not be preserved since the information provided in the EPOC / EPOC-PR does not allow to identify it.

SECTION H: Details of the service provider / its legal representative

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

Name of the authorised person:……

Official stamp (if available) and signature:……..