

321DT32e

Background Documentation



With the support of the Justice Programme
2014-2020 of the European Union

This publication has been produced with the financial support of the Justice Programme 2014-2020 of the European Union. The content of this publication reflects only the ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

Work carried out by the European Union on e-evidence

1	Proposal for a Regulation of the European Parliament and the Council on the European Production and Preservation Orders for electronic evidence in criminal matters (<i>Strasbourg, 17.4.2018 COM(2018) 225 final</i>)
2	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (<i>Strasbourg, 17.4.2018 COM(2018) 226 final</i>)
3	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings - General approach (<i>Council of the EU, Interinstitutional File: 2018/0107(COD) 6946/19 Brussels, 28 February 2019</i>)

A) European Criminal Law: the institutional framework

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A2-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union (<i>OJ C115/47; 9.5.2008</i>) – <i>Title V (pages. 27-38)</i>
A1-04	Consolidated Version of the Treaty on the European Union (<i>OJ C321 E/1; 29.12.2006, P. 5</i>) – <i>Title VI (pages 23-31)</i>
A1-05	Charter of fundamental rights of the European Union (<i>OJ. C 364/1; 18.12.2000</i>)
A1-06	Explanations relating to the Charter of Fundamental Rights (<i>2007/C 303/02</i>)
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 (<i>OJ L 239; 22.9.2000, P. 19</i>)

A2) Court of Justice of the European Union

A2-01	Consolidated Version of the Statute of the Court of Justice of the European Union (01.07.2013)
A2-02	Consolidated version of the Rules of Procedure of the Court of Justice of 25 September 2012

A3) The EU's competence in criminal matters

A3-01	Case C-440/05, ship-source pollution, <i>Commission v. Council</i> [2007] ECR I-0000, <i>Judgement of 23 October 2007</i>
A3-02	Case C-176/03 <i>Commission v. Council</i> [2005] ECR I-07879, <i>Judgement of 13 September 2005</i>

A4) European Convention on Human Rights (ECHR)

A4-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocol and protocols no. 4, 6, 7, 12 and 13, Council of Europe
A4-02	Case of <i>Salduz v. Turkey</i> (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

B) From mutual legal assistance to mutual recognition

B1) Main instruments

B1-01	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (<i>OJ L 328/42; 15.12.2009, P.42</i>)
B1-02	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (<i>2001/C 326/01</i>), (<i>OJ C 326/01; 21.11.2001, P. 1</i>)
B1-03	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 (<i>OJ C 197/1; 12.7.2000, P. 1</i>)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (<i>Strasbourg, 8.XI.2001</i>)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (<i>Strasbourg, 17.III.1978</i>)
B1-06	European Convention on Mutual Assistance in Criminal Matters (<i>Strasbourg, 20.IV.1959</i>)
B1-07	Third Additional Protocol to the European Convention on Extradition (<i>Strasbourg, 10.XI.2010</i>)
B1-08	Second Additional Protocol to the European Convention on Extradition (<i>Strasbourg, 17.III.1978</i>)
B1-09	Additional Protocol to the European Convention on Extradition (<i>Strasbourg, 15.X.1975</i>)
B1-10	European Convention on Extradition (<i>Strasbourg, 13.XII.1957</i>)

B2) Mutual recognition in practice: the European Arrest Warrant

B2-01	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (<i>OJ L 81/24; 27.3.2009</i>)
B2-02	Council Framework Decision of 13 June 2002 on the European arrest warrant

	and the surrender procedures between Member States (<i>OJ L 190/1; 18.7.2002, P. 1</i>)
B2-03	Case C-399/11 Stefano Melloni v Ministerio Fiscal, Judgment of of 26 February 2013
B2-04	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-05	C-261/09 Mantello, Judgement of 16 November 2010
B2-06	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-07	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-08	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-09	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008
B2-10	C-303/05 Wereld/Ministerraad, Judgment of the Court of 3 May 2007

B3) Mutual recognition in practice: sanctions

B3-01	Proposal for a Directive on the freezing and confiscation of proceeds of crime in the European Union (COM(2012) 85 final; 12.3.2012)
B3-02	Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (<i>OJ L 294/20; 11.11.2009</i>)
B3-03	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions (<i>OJ L 337/102; 16.12.2008</i>)
B3-04	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union (<i>OJ L 327/27; 5.12.2008</i>)
B3-05	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings (<i>OJ L 220/32; 15.08.2008</i>)
B3-06	Council Framework Decision of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (<i>OJ L 328/59, 24.11.2006, P.59</i>)
B3-07	Council Framework Decision of 24 February 2005 on the application of the principle of mutual recognition to financial penalties (<i>OJ L 76/16, 22.3.2005, P.16</i>)
B3-08	Council Framework Decision of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property (<i>OJ L 68/49, 1.3.2005, P. 49</i>)

B4) Mutual recognition in practice: evidence

B4-01	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (<i>OJ L 130/1; 1.5.2014</i>)
B4-02	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (<i>OJ L, 350/72, 30.12.2008</i>)
B4-03	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (<i>OJ L 196/45; 2.8.2003</i>)

B5) Criminal records

B5-01	Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (<i>OJ L 93/33; 7.4.2009, P. 33</i>)
B5-02	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (<i>OJ L 93/23; 07.4.2009</i>)
B5-03	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure (<i>6397/5/06 REV 5; 15.1.2007</i>)
B5-04	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record (<i>OJ L 322/33; 9.12.2005</i>)

C) Procedural guarantees in the EU

C-01	Proposal for a Directive on provisional legal aid for suspects or accused persons deprived of liberty and legal aid in European arrest warrant proceedings (<i>COM(2013) 824 final; 27.11.2013</i>)
C-02	Proposal for a Directive on procedural safeguards for children suspected or accused in criminal proceedings (<i>COM(2013) 822 final; 27.11.2013</i>)
C-03	Proposal for a Directive on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings (<i>COM(2013) 821 final; 27.11.2013</i>)
C-04	Directive 2013/48/EU 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 (<i>OJ L 294/1; 6.11.2013</i>)
C-05	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (<i>1.6.2012; OJ L 142/1</i>)
C-06	Strengthening mutual trust in the European judicial area – A Green Paper on the application of EU criminal justice legislation in the field of detention (<i>COM(2011) 327 final; 14.6.2011</i>)
C-07	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 (<i>OJ L 280/1; 26.10.2010</i>)
C-08	Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings (<i>OJ C 295/1; 4.12.2009</i>)

D) Victims' rights

D-01	Regulation (EU) No 606/2013 of 12 June 2013 on mutual recognition of protection measures in civil matters (<i>OJ L 181/4; 29.6.2013</i>)
D-02	Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (<i>14.11.2012; OJ L 315/57</i>)
D-03	Directive 2011/99/EU of 13 December 2011 on the European protection order (<i>OJ L 338/2; 21.12.2011</i>)
D-04	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims (<i>OJ L 261/15; 6.8.2004</i>)

D-05	Council Framework Decision of 15 March 2001 on the standing of victims in criminal procedures (<i>OJ L 82/1; 22.03.2001</i>)
------	--------------------------------------------------------------------------------------------------------------------------------

E) Cybercrime - Council of Europe

E-01	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (<i>Strasbourg, 28.I.2003</i>)
E-02	Convention on Cybercrime (<i>Budapest, 23.XI.2001</i>)

F) Cybercrime – European Union

F-01	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 (Official Journal L 218/8 of 14.08.2013)
F-02	Directive 2011/92/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 (<i>Official Journal L 335/1 of 17.12.2011</i>)

- For a comprehensive overview of the legal instruments in the field of cybercrime please consult the ERA e-library at the following address: <http://www.era-comm.eu/Cybercrime/library.html>

G) Electronic Evidence

G-01	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
G-02	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014)
G-03	ACPO Good Practice Guide for Digital Evidence (March 2012)
G-04	Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (Official Journal L 130/1 01.05.2014)
G-05	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (Official Journal L 350/72, 30.12.2008)
G-06	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (Official Journal L 178/1, 17.7.2000)
G-07	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption (COM (97) 503), October 1997



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 crime¹, 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 ago². 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 jurisdiction³ in cyberspace⁴. 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 concerned⁵.

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 EU⁶.

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 matters⁷ (EIO Directive), the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union⁸, Council Decision 2002/187/JHA setting up Eurojust⁹, Regulation (EU) 2016/794 on Europol¹⁰, Council Framework Decision 2002/465/JHA on joint investigation teams¹¹, 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 US¹² and the Agreement on MLA between the EU and Japan¹³.

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 measure¹⁴. This includes access to electronic evidence but the EIO Directive does not contain any specific provisions on this type of evidence¹⁵. 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 cybercrime¹⁸. 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 consideration¹⁹.

- **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 proposal²⁰ and made various suggestions for improvement²¹. 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 practical 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 Act²³, 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**

	<i>REGULATION</i>	
	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 Order 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 considerations²⁴.

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 2016²⁵. 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.

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 Committee²⁶,

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 2017²⁷, 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 2017²⁸, 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/JHA²⁹.
- (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/EU³⁰, 2012/13/EU³¹, 2013/48/EU³², 2016/343³³, 2016/800³⁴ and 2016/1919³⁵ 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 unknown 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) 2018/302³⁷ 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 availability 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) 2016/679³⁸. 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) 2016/680³⁹.
- (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 standardised 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-Making⁴⁰. 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 Council⁴¹ 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 Council⁴² 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 Council⁴⁴ 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 constitutes 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 Council⁴⁵;
- (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/EC⁴⁶.

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/JHA⁴⁷;
 - offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council⁴⁸;
 - 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 Council⁴⁹.
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 2016⁵⁰.
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/JHA⁵¹.

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
The President

For the Council
The President



EUROPEAN
COMMISSION

Strasbourg, 17.4.2018
COM(2018) 226 final

2018/0107 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**laying down harmonised rules on the appointment of legal representatives for the
purpose of gathering evidence in criminal proceedings**

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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Online service providers such as electronic communications services or social networks, online marketplaces and other hosting service providers are important drivers of innovation and growth in the digital economy. They facilitate an unprecedented access to information and make it easier for individuals to communicate with one another. These services connect hundreds of millions of users and provide innovative services to individuals and businesses. They generate significant benefits for the digital single market and the economic and social wellbeing of users across the Union and beyond. The growing importance and presence of the internet and of communication and information society services in our daily lives and societies are reflected in the exponential growth of usage. However, these services can also be misused as tools to commit or facilitate crimes, including serious crimes such as terrorist attacks. When that happens, these services and applications ('apps') often are the only place where investigators can find leads to determine who committed a crime and to obtain evidence which can be used in court.

Given the borderless nature of the internet, such services can in principle be provided from anywhere in the world and do not necessarily require a physical infrastructure, corporate presence or staff in Member States where the services are offered or in the internal market as a whole. The cross-border offering of such services is encouraged and supported within the EU in particular by the freedom to provide services.

Service providers active in the internal market can be divided into three main categories: (1) service providers headquartered in a Member State offering services in the territory of only that Member State; (2) service providers headquartered in a Member State offering services in several Member States; and (3) service providers headquartered outside the EU offering services in one or several EU Member States, with or without an establishment in one or more of these Member States.

In the absence of a general requirement for service providers to ensure a physical presence within the territory of the Union, Member States have taken steps at national level to ensure compliance with national legal obligations that they consider to be essential and in line with Art. 3(4) of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market¹ (e-Commerce Directive). Such steps include requiring access to evidence or other types of information when requested by judicial authorities in criminal matters. These national approaches vary widely across Member States and include measures ranging from expanded enforcement jurisdiction² to the obligation to designate a legal representative on the relevant Member State's territory for certain service providers offering services within that territory. For example, Germany has recently passed the 'Network Enforcement Act'³, obliging providers of social networks⁴ to designate a person

¹ [Directive 2000/31/EC](#) of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

² The term 'enforcement jurisdiction' refers to the competence of the relevant authorities to undertake an investigative measure.

³ http://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html.

⁴ The Act applies 'to telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such

in Germany authorised to receive law enforcement requests. The law imposes sanctions of up to EUR 500 000 for failure to name a representative or to respond to requests for information when acting as the person authorised to receive service. Discussions on similar measures are under way in Italy⁵. Other Member States, such as Belgium, do not require local representation but instead seek to enforce national obligations directly against providers based abroad through domestic proceedings⁶.

Member States also apply a number of different connecting factors to assert jurisdiction over a service provider, such as its main seat, the place where services are offered, the location of the data or a combination of factors. In addition, there are disparate cooperation mechanisms and informal agreements between the authorities of some Member States and some service providers. Some of the larger service providers estimated, for the purposes of the impact assessment, that their annual costs of compliance with national legal obligations are in the high seven digits. The cost of complying with diverging national requirements, while presumably proportionate to market presence, can prove prohibitive to smaller service providers.

When it comes to the enforceability of requests sent in the context of such arrangements, there are differences between Member States as to whether service providers are under an obligation to cooperate or not. The sanctions and enforcement in case of non-compliance are also fragmented. Even in cases where the service provider complies with the order imposing the sanction, it is still difficult to enforce the original order to provide the data.

Member States have highlighted these challenges as key issues to be tackled jointly on several occasions:

- On 22 March 2016, a joint statement of Ministers of Justice and Home Affairs and representatives of the EU institutions on the terrorist attacks in Brussels⁷, stressed the need, as a matter of priority, to find ways to secure and obtain electronic evidence more quickly and effectively by intensifying cooperation with third countries and with service providers that are active on European territory, in order to enhance compliance with EU and Member States' legislation.
- In Council Conclusions adopted on 9 June 2016⁸, the Member States reiterated their determination to act to uphold the rule of law in cyberspace and called on the Commission to develop a common EU approach on improving criminal justice in cyberspace as a matter of priority.

A two-fold legislative approach is necessary to address these challenges. This proposal lays down rules on the legal representation in the Union of certain service providers for the purposes of gathering evidence in criminal proceedings. In addition, an instrument adopted on the basis of Article 82(1) TFEU, is needed to provide for the direct serving of orders on the service provider in cross-border situations. Thus, the foregoing challenges are dealt with

content available to the public (social networks)(...) The same shall apply to platforms which are designed to enable individual communication or the dissemination of specific content.'

⁵ <http://www.publicpolicy.it/wp-content/uploads/2016/03/Relazione-Franco-Roberti-Dna.pdf>.

⁶ Court of Appeals of Antwerp, judgment of 15 November 2017, <http://www.lesoir.be/124825/article/2017-11-17/la-justice-belge-condamne-skype-payer-une-amende-de-30000-euros>.

⁷ [Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016](#).

⁸ [Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16](#).

through a combination of these two proposals. But it is important to keep in mind that this proposal clearly and foremost aims to identify the addressee of the orders of Member States' authorities to obtain evidence in criminal matters held by service providers. Therefore, this proposal aims to remove some of the obstacles to addressing the service providers by offering a common, EU-wide solution for addressing legal orders to service providers by way of a legal representative. This removes the need for individualised and uncoordinated national approaches and provides legal certainty at EU level. To that end, this proposal sets obligations for the Member States to ensure that service providers designate empowered legal representatives legally responsible for complying with judicial orders and decisions on behalf of these service providers.

In addition, a harmonised approach creates a level playing field for all companies offering the same type of services in the EU, regardless of where they are established or act from, while respecting the country of origin principle set out in Art. 3 of the e-Commerce Directive. That principle applies only to providers of information society services which are established in the EU and is moreover subject to a number of exceptions and possible exemptions. Harmonised rules at EU level are not only necessary to eliminate obstacles to the provision of services and to ensure a better functioning of the internal market but also to ensure a more coherent approach to criminal law in the Union. A level playing field is also necessary for other fundamental premises for the good functioning of the internal market, such as the protection of fundamental rights of citizens and the respect of sovereignty and public authority when it comes to the effective implementation and enforcement of national and European legislation.

- **Consistency with existing EU legal framework in the policy area**

The obligation to designate a legal representative for service providers not established in the EU but offering services in the EU already exists in certain acts of EU law applicable in particular fields. This is the case, for instance, in the General Data Protection Regulation (EU) 2016/679 (Article 27)⁹ and in Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (Article 18)¹⁰. The Commission proposal for an ePrivacy Regulation also contains such an obligation (Article 3)¹¹.

As noted above, this proposal is consistent with the e-Commerce Directive and in particular with the country of origin principle laid down in the Directive's Article 3. It leaves the provisions of that Directive, including the requirements on providing information pursuant to Article 5, unaffected.

- **Summary of the proposed Directive (how it improves current framework)**

There are currently varying approaches across Member States when it comes to obligations imposed on service providers, especially in criminal proceedings. Fragmentation has appeared in particular in electronic evidence, as certain service providers store information that can be relevant for the investigation and prosecution of criminal offences. This fragmentation creates

⁹ [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

¹⁰ [Directive \(EU\) 2016/1148](#) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

¹¹ [Proposal for a Regulation](#) of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

legal uncertainty for those involved and can put service providers under different and sometimes conflicting obligations and sanctioning regimes in that regard, depending on whether they provide their services nationally, cross-border within the Union or from outside the Union. To reduce obstacles to the freedom to provide services, this Directive makes it mandatory for service providers to designate a legal representative in the Union to receive, comply with and enforce decisions aimed at gathering evidence by competent national authorities in criminal proceedings. The ensuing reduction of obstacles would ensure a better functioning of the internal market in a way which is coherent with the development of a common area of freedom, security and justice.

The obligation of designating a legal representative for all service providers that are operating in the Union would ensure that there is always a clear addressee of orders aiming at gathering evidence in criminal proceedings. This would in turn make it easier for service providers to comply with those orders, as the legal representative would be responsible for receiving, complying with and enforcing those orders on behalf of the service provider.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis to support action in the field is found in Articles 53 and 62 of the Treaty on the Functioning of the European Union, which provide for the adoption of measures to coordinate the provisions laid down by law, regulation or administrative action in Member States on establishing and providing services.

In the present case, an obligation to appoint a legal representative in the Union would help in particular to eliminate obstacles to the freedom to provide services enshrined in Article 56 Treaty on the Functioning of the European Union, as outlined above.

- **Choice of the instrument**

Under Articles 53 and 62 of the Treaty on the Functioning of the European Union, the Commission can propose directives and non-binding instruments such as recommendations. Given the need to provide legal certainty and remove obstacles to the free provision of services, which cannot be achieved by adopting a non-binding instrument, the form of a directive was chosen.

- **Subsidiarity**

This proposal covers service providers offering services in the EU, regardless of their place of establishment, which may be in the EU or outside the EU. In the absence of a common EU approach, uncoordinated national solutions related to the receipt of, compliance with or the enforcement of decisions for gathering evidence in criminal proceedings are liable to lead to fragmentation, creating a patchwork of diverse and possibly conflicting national obligations for service providers active in several markets. This hampers the provision of services across the EU. Given the diversity of legal approaches and the large range of stakeholders, Union-level legislation is the most appropriate means to address the identified problems.

- **Proportionality**

The proposal seeks to put forward a harmonised approach to remove existing and emerging obstacles to the provision of services as regards the issue of the receipt of, compliance with or the enforcement of decisions for gathering evidence in criminal proceedings. The chosen approach is considered proportionate to the burden imposed. In view of the increasing

importance and presence of the internet and information society services, there are a number of possible options to address the current obstacles. Of these options, as discussed in more detail in the Impact Assessment¹² accompanying the legislative proposal, the mandatory appointment of a legal representative for certain service providers active in the EU achieves the objective of providing an effective mechanism to allow legal orders to be served without imposing an undue burden on service providers.

The obligation to designate a legal representative represents a higher burden for companies not established in the EU, as they could not rely on an existing corporate presence in the EU. On the other hand, this legal representative could be a third party, which could be shared between several service providers, in particular small and medium-sized businesses ('SMEs'), and the legal representative may accumulate different functions (e.g. the General Data Protection Regulation or ePrivacy representatives in addition to the legal representative provided for by this instrument). It will only apply to SMEs who offer their services in the EU, and not in case of occasional data processing in the EU.

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, including on the possibilities for improvement in the channels for interaction between authorities and service providers. 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.

Through a targeted survey to public authorities in the Member States, it was 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.

Throughout the consultation, service providers and some civil society organisations indicated the need to ensure legal certainty in direct cooperation with public authorities and to avoid conflicts of law. Key issues highlighted by public authorities included the lack of reliable cooperation with service providers, lack of transparency, and legal uncertainty surrounding jurisdiction for investigative measures. Some civil society organisations considered that EU-level legislation in this area was not desirable and indicated a preference for limiting EU action to improving mutual legal assistance procedures, which will be taken forward in parallel.

¹² 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.

- **Impact assessment**

The Regulatory Scrutiny Board issued a positive opinion on the impact assessment¹³ and made various suggestions for improvement¹⁴. 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, which helped shape the initiative. The complementarity between different measures 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 practical measures of Option A with international solutions (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 (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). The Impact Assessment also identified the need for service providers offering services in the EU to nominate a legal representative in the Union, and this was included in Options C and D.

The Impact Assessment revealed that options including the legal representative (C and D) would add clear value compared to the other options. Although service providers would have to incur in additional costs in the short term due to the appointment of a legal representative, a harmonised framework at EU level is likely to reduce the burden on those providers currently responding to requests for data from law enforcement on a voluntary basis, which have to assess them under the different laws of all Member States. The cost model established and validated in cooperation with relevant service providers indicated that the initiative would generate significant savings in the medium and long term and remove obstacles to the internal market. Furthermore, legal certainty and standardisation of procedures should also have a positive impact on SMEs, since they would alleviate administrative burden. Overall, the initiative is also expected to generate savings for them.

- **Fundamental rights**

The obligation to appoint a legal representative seeks to eliminate obstacles to and hence facilitate the exercise of the freedom to provide services. In particular, the proposal allows service providers established in the Union to designate an existing establishment as its legal

¹³ 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.

¹⁴ 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.

representative, with an exception only when this establishment is in a Member State not participating in judicial cooperation instruments adopted under Title V of the Treaty. This exception is meant to address the particular situation created by Title V of the Treaty, which needs to be taken into account.

4. BUDGETARY IMPLICATIONS

The legislative proposal does not have an impact on the Union budget.

5. OTHER ELEMENTS

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

The Directive has to be implemented by the Member States. The Commission will support this implementation process by creating a contact committee to ensure a harmonised and coherent implementation and avoid different systems for service providers. The Commission will, if necessary, issue guidance for service providers. The Commission will submit a report on its application, building on a detailed review of its functioning, to the European Parliament and the Council at the latest 5 years after the entry into application. If necessary, the report will be accompanied by proposals adapting this Directive.

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

Article 1 Subject matter and scope

Article 1 establishes the subject matter of the Directive, which is to lay down rules on the legal representation in the Union of certain service providers for the purpose of gathering evidence in criminal proceedings.

The type of obligations requested from service providers may take several forms, such as receiving an order in criminal proceedings from a prosecutor or a judge with legal consequences, providing data needed in those criminal proceedings, taking certain measures for data preservation in criminal proceedings or being addressed with an enforcement procedure in case of non-compliance. Due to their commercial and territorial policies, service providers may have difficulty in complying with these different types of increasingly frequent requests. On the other hand, competent authorities need to know whom and how to address service providers established or offering services on the territory of the Union.

Member States shall not put additional obligations to those deriving from this Directive on service providers under the scope of this Directive, such as obliging them to establish a legal representative in their own territory instead of anywhere in the Union where they offer services.

Harmonised rules on legal representation should not limit the powers given under Union and national law to competent authorities to address service providers established on their territory. In such cases, if national authorities decide to address their orders directly to the establishment of the service provider, the responsibility of the legal representative as set out in this Directive does not apply.

Article 2 Definitions

Article 2 sets out definitions which apply in this instrument.

The legal representative can be a legal or natural person designated by the service provider to act on its behalf to comply with any decisions of competent law enforcement and judicial authorities for the purpose of gathering evidence in criminal matters. Service providers should

be able to choose to designate an existing establishment in a Member State, including their main seat or headquarters, and also to designate several legal representatives.

The following types of service providers fall under the scope of the Directive: providers of electronic communications services, providers of information society services that store data as part of the service provided to the user, including social networks, online marketplaces and other hosting service providers, and providers of names and numbering services for the internet.

The scope of this Directive covers providers of electronic communication services, as defined [in the Directive establishing the European Electronic Communications Code]. Traditional telecommunication services, consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and email services, instead of traditional communications services. These services, along with social networks, such as Twitter and Facebook, which allow users to share content, are therefore covered by this proposal.

In many cases, data is no longer stored on a user's device but is 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 centralised systems to provide their services. To take into account this development, the definition covers cloud 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 traders to conclude transactions via online sales or service contracts with traders. 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 usually 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 nowadays 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 distance.

Data held by providers of internet infrastructure services, such as domain name registrars and registries and privacy and proxy service providers, or by 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 possibly involved in criminal activity.

For the purposes of defining those service providers falling into the ambit of application of this Directive, there should be a sufficient link between the provider and the Union. In that regard it should be assessed whether the service provider enables legal or natural persons in the Union 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 applying this Directive. Therefore, a substantial connection to the Union should be required. Such a substantial connection would certainly exist where the service provider has an establishment in the Union. 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 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 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.

Article 3 Legal representative

Article 3(1) and (2) establish the obligation that has to be imposed upon service providers providing services in the Union to designate a legal representative in the Union. In principle, service providers should be free to choose in which Member State they designate their legal representative, and in accordance with Article 1(2), Member States may not restrict this free choice, for example by imposing an obligation to designate the legal representative on their territory. However, Article 3(1) to (3) contains certain restrictions with regard to this free choice of service providers, notably that the legal representative should be established in a Member State where the service provider provides services or is established. This restriction, which requires a pre-existing connection between the service provider and the Member State where the legal representative is to be designated, limits the possibility of service providers to select the Member State based on considerations which would run counter to the aims of this Directive, such as the level of fines. Article 3(1) to (3) also defines which Member States are responsible for imposing the obligation to service providers.

Article 3(1) applies to service providers established in the Union. They have to designate at least one legal representative in the Union, more specifically in a Member State where they offer services or are established. The Member States where service providers are established are responsible for imposing this obligation.

Article 3(2) applies to service providers that are not established in the Union. In that case, they should designate a legal representative in one of the Member States where they offer services. The Member States where the service provider offers services are responsible for imposing this obligation.

Article 3(3) applies in both cases covered by Article 3(1) and 3(2) and imposes additional requirements to address the problem inherent to the interplay between an internal market instrument and judicial cooperation instruments adopted under Title V of the Treaty. A legal representative designated in a Member State not participating in a relevant judicial cooperation instrument would not fully fulfil its role, as it could not be addressed with an order under this instrument. This is why Article 3(3) requires service providers offering services in Member States participating in such instruments to designate a legal representative in one of them. As a result, a service provider establishing a legal representative in a Member State participating in a judicial cooperation instrument under Title V would fulfil its obligations both under paragraph 1 or 2, depending on the case, and under paragraph 3. On the other hand, a service provider designating a legal representative in a Member State not participating in a judicial cooperation instrument under Title V would thereby fulfil its obligation under paragraph 1 or 2, but in order to also fulfil its obligation under paragraph 3, it would have to nominate another legal representative in one of the Member States participating

in a judicial cooperation instrument under Title V. The Member States taking part in a relevant instrument and where the service provider offers services are responsible for imposing this obligation.

Because of the ‘variable geometry’ that exists in the area of criminal law, with Denmark not participating in any Union legislation under Title V, and a right to opt-in for the United Kingdom and Ireland, there are currently different instruments that apply in the relationships between Member States when gathering evidence in criminal proceedings. These instruments include the Directive regarding the European Investigation Order and the 2000 Mutual Legal Assistance Convention. The European Production Order will add to this multifaceted legal regime. The resulting complexity is likely to lead to an increased risk that the Member States participating in the Regulation on European Production Orders may develop uncoordinated national solutions, which would in turn lead to further fragmentation and legal uncertainty for all stakeholders concerned. This is why all Member States should be required to ensure that service providers not established in the Union but offering services in the Union designate a legal representative in the Union, which would be the addressee of direct requests in cross-border situations, and of requests based on judicial cooperation between judicial authorities. In addition, to avoid the risk of weakening the effectiveness of the EU legal instruments adopted under Title V, Chapter 4, of the Treaty on the Functioning of the EU for gathering evidence in criminal matters, to which only some Member States participate, a legal representative should be designated in one of those Member States taking part in those legal instruments.

Service providers should be free to designate one of their establishments within the Union, including their main seat or headquarters, as their legal representative, subject to the conditions set out in the Directive.

Article 3(6) clarifies that Member States have to ensure in national law that a designated legal representative can be held liable for non-compliance, without prejudice to the liability of service provider itself. Service providers should not be able to claim they are not responsible for example for the non-compliance of their legal representative. Neither can they exculpate themselves due to missing or ineffective internal procedure, as they are responsible for providing the necessary resources and powers to guarantee compliance with orders and national decisions. Nor should the legal representative be able to exculpate himself by claiming for example he is not empowered to deliver data.

Article 4 Notifications and languages

Article 4 sets out the obligation for Member States to ensure that service providers designate one or more legal representatives and provide their contact details.

The notification should also include information on the language(s) in which the service provider can be addressed. The official language of the Member State in which the legal representative is located will be the one used by default. If there are several official languages, the service provider can choose one or more of them. Moreover, service providers will be able to choose additional official languages of the Union to be addressed in by competent authorities of all Member States. This will allow service providers to choose a language used, for example, in internal communications with headquarters or which is currently frequently used in requests and thus bring about more consistency and certainty for both competent authorities and service providers.

Where a service provider designates several legal representatives, they may also notify considerations to determine which one should be addressed. These are not binding for Member States’ authorities, but should be followed except in duly justified cases.

The service providers are responsible for making this information publicly available, e.g. on their website, and for keeping this information up to date. Additionally, the Member States should make available the relevant information on dedicated websites to help judicial authorities identify the correct addressee.

Article 5 Sanctions

For the cases where service providers covered by this Directive do not comply with the national provisions adopted pursuant to this Directive, Member States should provide in their national law effective, proportionate and dissuasive sanctions which can be imposed on service providers for not establishing a legal representative as set out in this Directive and not providing the necessary powers, resources and conditions such as infrastructure for the legal representative for generally complying with decisions by national authorities and deliver the requested evidence.

Penalties or fines for the non-compliance by the legal representative with a specific decision such as an order in concrete proceedings, on the other hand, are the matter of other specific instruments, such as the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters or the national law.

Article 6 Coordination mechanism

To ensure a coherent approach, the Directive provides for a coordination mechanism on the basis of central authorities designated by Member States. This coordination mechanism will enable Member States to exchange information, provide for assistance and cooperate in their enforcement approach, e.g. by identifying the most appropriate Member State to take action in a given case of non-compliance.

Articles 7, 8, 9 and 10

These Articles contain further provisions on transposition by Member States, review by the Commission, entry into force of the Directive and the addressees of the Directive. The proposed Directive will enter into force the twentieth day after its publication in the Official Journal. Member States will have 6 months to transpose the provisions of the proposed Directive into national law. The Commission shall carry out an evaluation of this Directive in line with the Commission's Better Regulation Guidelines and pursuant to paragraph 22 of the Interinstitutional Agreement of 13 April 2016¹⁵.

¹⁵ 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.

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 53 and 62 thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee¹⁶,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Network-based services can in principle be provided from anywhere and do not require a physical infrastructure, corporate presence, or staff in the country where the services are offered, nor in the internal market itself. As a consequence, it can be difficult to apply and enforce obligations laid down in national and Union law which apply to the service providers concerned, in particular the obligation to comply with an order or a decision by a judicial authority. This is the case in particular in criminal law, where Member States' authorities face difficulties with serving, ensuring compliance and enforcing their decisions, in particular where relevant services are provided from outside their territory.
- (2) Against that background, Member States have taken a variety of disparate measures to more effectively apply and enforce their legislation. This includes measures for addressing service providers to obtain electronic evidence that is of relevance to criminal proceedings.
- (3) To that end, some Member States have adopted, or are considering adopting, legislation imposing mandatory legal representation within their own territory, for a number of service providers offering services in that territory. Such requirements create obstacles to the free provision of services within the internal market.
- (4) There is a significant risk that other Member States will try to overcome existing shortcomings related to gathering evidence in criminal proceedings by means of imposing disparate national obligations in the absence of a Union-wide approach. This is bound to create further obstacles to the free provision of services within the internal market.
- (5) Under the current circumstances, the resulting legal uncertainty affects both service providers and national authorities. Disparate and possibly conflicting obligations are

¹⁶ OJ C , , p. .

set out for service providers established or offering services in different Member States, which also subject them to different sanction regimes in case of violations. This divergence in the framework of criminal proceedings will likely further expand because of the growing importance of communication and information society services in our daily lives and societies. The foregoing not only represents an obstacle to the proper functioning of the internal market but also entails problems for the establishment and correct functioning of the Union's area of freedom, security and justice.

- (6) To avoid such fragmentation and to ensure that undertakings active in the internal market are subject to the same or similar obligations, the Union has adopted a number of legal acts in related fields such as data protection¹⁷. To increase the level of protection for the data subjects, the rules of the General Data Protection Regulation¹⁸ provide for the designation of a legal representative in the Union by controllers or processors not established in the Union but offering goods or services to individuals in the Union or monitoring their behaviour if their behaviour takes place within the Union, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body.
- (7) By setting out harmonised rules on the legal representation of certain service providers in the Union for receipt of, compliance with and enforcement of decisions issued by competent authorities in the Member States for the purposes of gathering evidence in criminal proceedings, the existing obstacles to the free provision of services should be removed, as well as the future imposition of divergent national approaches in that regard should be prevented. Level playing field for service providers should be established. Moreover, more effective criminal law enforcement in the common area of freedom, security and justice should be facilitated.
- (8) The legal representative at issue should serve as an addressee for domestic orders and decisions and for orders and decisions pursuant to Union legal instruments adopted within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal matters. This includes both instruments that permit the direct serving of orders in cross-border situations on the service provider, and instruments based on judicial cooperation between judicial authorities under Title V, Chapter 4.
- (9) Member States shall ensure that the obligation to designate a legal representative is immediate, that is from the date of transposition set out in Article 7 for service

¹⁷ [Directive 95/46/EC](#) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31); [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1); [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

¹⁸ [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

providers that offer services in the Union at that date, or from the moment service providers start offering services in the Union for those service providers that will start offering services after the date of transposition.

- (10) The obligation to designate a legal representative should apply to service providers that offer services in the Union, meaning in one or more Member States. Situations where a service provider is established on the territory of a Member State and offers services exclusively on the territory of that Member State, should not be covered by this Directive.
- (11) Notwithstanding the designation of a legal representative, Member States should be able to continue addressing service providers established on their territory, be it in purely domestic situations, be it after receipt of a request for assistance under legal instruments on mutual legal assistance and on mutual recognition in criminal matters.
- (12) The determination whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in the Union to use its services. However, the mere accessibility of an online interface (for instance the accessibility of the service provider's or an intermediary's website or of an email address and of other contact details) taken in isolation should not be a sufficient condition for the application of this Directive.
- (13) A substantial connection to the Union should also be relevant to determine the ambit of application of this Directive. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be 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. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302¹⁹ cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union. The same considerations should apply to determine whether a service provider offers services in a Member State.
- (14) Service providers obliged to designate a legal representative should be able to choose to that effect an existing establishment in a Member State, be it a corporate body or a branch, agency, office or a main seat or headquarters, and also more than one legal

¹⁹ [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).

representative. Nevertheless, a corporate group should not be forced to designate multiple representatives, one for each undertaking part of that group. Different instruments adopted within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union apply in the relationships between Member States when gathering evidence in criminal proceedings. As a consequence of this ‘variable geometry’ that exists in the common area of criminal law, there is a need to ensure that the Directive does not facilitate the creation of further disparities or obstacles to the provision of services in the internal market by allowing service providers offering services on their territory to designate legal representatives within Member States that do not take part in relevant legal instruments, which would fall short of addressing the problem. Therefore, at least one representative should be designated in a Member State that participates in the relevant Union legal instruments to avoid the risk of weakening the effectiveness of the designation provided for in this Directive and to make use of the synergies of having a legal representative for the receipt of, compliance with and enforcement of decisions and orders issued in the context of gathering evidence in criminal proceedings, including under the [Regulation] or the 2000 Mutual Legal Assistance Convention. In addition, designating a legal representative, which could also be utilised to ensure compliance with national legal obligations, makes use of the synergies of having a clear point of access to address the service providers for the purpose of gathering evidence in criminal matters.

- (15) Service providers should be free to choose in which Member State they designate their legal representative, and Member States may not restrict this free choice, e.g. by imposing an obligation to designate the legal representative on their territory. However, the Directive also contains certain restrictions with regard to this free choice of service providers, notably that the legal representative should be established in a Member State where the service provider provides services or is established, as well as the obligation to designate a legal representative in one of the Member States participating in judicial cooperation instruments adopted under Title V of the Treaty.
- (16) The service providers most relevant for gathering evidence in criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Directive. Providers of electronic communication services are defined in 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, and for which it is only of an ancillary nature, such as legal, architectural, engineering and accounting services provided online at distance, should be excluded from the scope of this Directive, even where they may fall within the definition of information society services as per Directive (EU) 2015/1535.
- (17) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and privacy and proxy service providers or regional internet registries for internet protocol (‘IP’) addresses, are of particular relevance when it comes to the identification of actors behind malicious or

compromised web sites. They hold data that is of particular relevance for criminal investigations 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.

- (18) The legal representative should be able to comply with decisions and orders addressed to them by Member States' authorities on behalf of the service provider, which should take the appropriate measures to ensure this result, including sufficient resources and powers. The absence of such measures or their shortcomings should not serve as grounds to justify non-compliance with decisions or orders falling into the ambit of application of by this Directive, neither for the service provider nor its legal representative.
- (19) Service providers should notify the Member State in which the legal representative resides or is established of the identity and contact details of their legal representative, as well as related changes and updates of information. The notification should also provide information about the languages in which the legal representative can be addressed, which should include at least one of the official languages of the Member State where the legal representative resides or is established, but may include other official languages of the Union, such as the language of its headquarters. When the service provider designates more than one legal representative, it may also notify considerations to determine which one should be addressed. These considerations are not binding for Member States' authorities, but should be followed except in duly justified cases. All this information, which is of particular relevance for Member States' authorities, should be made publicly available by the service provider, for example on its website, in a manner comparable to the requirements for making available general information pursuant to Article 5 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market²⁰(e-Commerce Directive). For those service providers subject to the e-Commerce Directive, Article 3(3) complements but does not replace these requirements. Furthermore, Member States should also publish the relevant information for their country on a dedicated site of the e-Justice portal to facilitate coordination between Member States and use of the legal representative by authorities from another Member State.
- (20) The infringement of the obligations to designate a legal representative and to notify and make publicly available the information related thereto should be subject to effective, proportionate and dissuasive sanctions. Under no circumstances should the sanctions determine a ban, permanent or temporary, of service provision. Member States should coordinate their enforcement action where a service provider offers services in several Member States. To ensure a coherent and proportionate approach, a coordination mechanism is provided. The Commission could facilitate such coordination if necessary, but needs to be informed of cases of infringement. This Directive does not govern the contractual arrangements for transfer or shifting of financial consequences between service providers and legal representatives of sanctions imposed upon them.

²⁰ [Directive 2000/31/EC](#) of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

- (21) This Directive is without prejudice to the investigative powers of authorities in civil or administrative proceedings, including where such proceedings can lead to sanctions.
- (22) In order to ensure the application of the Directive in a consistent manner, additional mechanisms for the coordination between Member States should be put in place. For that purpose, Member States should designate a central authority that can provide central authorities in other Member States with information and assistance in the application of the Directive, in particular where enforcement actions under the Directive are considered. This coordination mechanism should ensure that relevant Member States are informed of the intent of a Member State to undertake an enforcement action. In addition, Member States should ensure that central authorities can provide each other with assistance in those circumstances, and cooperate with each other where relevant. Cooperation amongst central authorities in the case of an enforcement action may entail the coordination of an enforcement action between competent authorities in different Member States. For the coordination of an enforcement action, central authorities shall also involve the Commission where relevant. The existence of the coordination mechanism does not prejudice the right of an individual Member State to impose sanctions on service providers that fail to comply with their obligations under the Directive. The designation and publication of information about central authorities will facilitate the notification by service providers of the designation and contact details of its legal representative to the Member State where its legal representative resides or is established of the designation and contact details.
- (23) Since the objective of this Directive, namely to remove obstacles to the free provision of services in the framework of gathering evidence in criminal proceedings, cannot be sufficiently achieved by the Member States, but can rather, by reason of the borderless nature of such services, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.
- (24) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council²¹ and delivered an opinion on (...) ²²,
- (25) The Commission should carry out an evaluation of this Directive that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU value added and should provide the basis for impact assessments of possible further measures. The evaluation should be completed 5 years after entry into application, to allow for the gathering of sufficient data on its practical implementation. Information should be collected regularly and in order to inform the evaluation of this Directive.

²¹ [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).

²² OJ C , , p. .

HAVE ADOPTED THIS DIRECTIVE:

Article 1
Subject matter and scope

1. This Directive lays down rules on the legal representation in the Union of certain service providers for receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings.
2. Member States may not impose additional obligations to those deriving from this Directive on service providers covered by this Directive for the purposes set out in paragraph 1.
3. This Directive is without prejudice to the powers of national authorities in accordance with Union and national law to address service providers established on their territory for the purposes referred to in in paragraph 1.
4. This Directive shall apply to the service providers defined in Article 2(2) offering their services in the Union. It shall not apply where those service providers are established on the territory of a single Member State and offer services exclusively on the territory of that Member State.

Article 2
Definitions

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

- (1) ‘legal representative’ means a legal or natural person, designated in writing by a service provider for the purpose of Articles 1(1), 3(1), 3(2) and 3(3);
- (2) ‘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 Council²³ 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;
- (3) ‘offering services in a Member State’ means:
 - (a) enabling legal or natural persons in a Member State to use the services referred to in point (2); and

²³ [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).

- (b) having a substantial connection to the Member State referred to in point (a);
- (4) ‘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;
- (5) ‘group’ means a group as defined in Article 3(15) of Directive (EU) 2015/849 of the European Parliament and of the Council²⁴.

Article 3
Legal representative

1. Member States where a service provider offering services in the Union is established shall ensure that it designates at least one legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider is established or offers the services.
2. Where a service provider is not established in the Union, Member States shall ensure that such service provider offering services on their territory designates at least one legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.
3. As regards the receipt of, compliance with and enforcement of decisions and orders issued by the competent authorities of Member States under Union legal instruments adopted within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal proceedings, the Member States taking part in those legal instruments shall ensure that service providers offering services on their territory designate at least one representative in one of them. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.
4. Service providers shall be free to designate additional legal representatives, resident or established in other Member States, including those where the service providers offer their services. Service providers which are part of a group shall be allowed to collectively designate one legal representative.
5. Member States shall ensure that the decisions and orders by their competent authorities for evidence gathering in criminal proceedings are addressed to the legal representative designated by the service provider to that effect. That representative shall be entrusted with the receipt, compliance and enforcement of those decisions and orders on behalf of the service provider concerned.
6. To this end, Member States shall ensure that the legal representative residing or established on their territory cooperates with the competent authorities when

²⁴ [Directive \(EU\) 2015/849](#) of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

receiving those decisions and orders, in accordance with the applicable legal framework.

7. Member States shall ensure that service providers established or offering services in their territory provide their legal representative with the necessary powers and resources to comply with those decisions and orders.
8. Member States shall ensure that the designated legal representative can be held liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders, without prejudice to the liability and legal actions that could be initiated against the service provider. In particular, the lack of appropriate internal procedures between the service provider and the legal representatives cannot be used as a justification for non-compliance with those obligations.
9. Member States shall ensure that the obligation to designate a legal representative applies from the date of transposition set out in Article 7 for service providers that offer services in the Union at that date, or from the moment service providers start offering services in the Union for those service providers that will start offering services after the date of transposition of the Directive.

Article 4 *Notifications and languages*

1. Member States shall ensure that, upon designation of its legal representative in accordance with Article 3(1), (2) and (3), each service provider established or offering services in their territory notifies in writing the central authority of the Member State where its legal representative resides or is established of the designation and contact details of its legal representative as well as any changes thereof.
2. The notification shall specify the official language(s) of the Union, as referred to in Regulation 1/58, in which the legal representative can be addressed. This shall include, at least, one of the official languages of the Member State where the legal representative resides or is established.
3. When a service provider designates several representatives, the notification shall specify the official language(s) of the Union or Member States covered by each of them or any other considerations to determine the appropriate legal representative to be addressed. In duly justified cases, Member States' authorities may depart from those considerations.
4. Member States shall ensure that the service provider makes the information notified to them in accordance with this Article publicly available. Member States shall publish that information on a dedicated page of the e-Justice portal.

Article 5 *Sanctions*

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

2. Member States shall, by the date set out in Article 7, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. Member States shall also inform the Commission on an annual basis about non-compliant service providers and relevant enforcement action taken against them.

Article 6
Coordination mechanism

1. Member States shall designate a central authority or, where its legal system so provides, more than one central authority, to ensure the application of this Directive in a consistent and proportionate manner.
2. Member States shall inform the Commission of their designated central authority, or central authorities, referred to in paragraph 1. The Commission shall forward a list of designated central authorities to the Member States. The Commission will also make publicly available a list of designated central authorities to facilitate the notifications by a service provider to the Member States where its legal representative resides or is established.
3. Member States shall ensure that central authorities shall provide each other with relevant information and mutual assistance relevant to application of this Directive in a consistent and proportionate manner. The provisioning of information and mutual assistance shall cover, in particular, enforcement actions.
4. Member States shall ensure that the central authorities shall cooperate with each other and, where relevant, with the Commission to ensure the application of this Directive in a consistent and proportionate manner. Cooperation shall cover, in particular, enforcement actions.

Article 7
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 6 months after entry into force. They shall immediately inform the Commission thereof.
2. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.
3. Member States shall communicate to the Commission the text of the measures of national law which they adopt in the field covered by this Directive.

Article 8
Evaluation

By [5 years from the date of application of this Directive] at the latest, the Commission shall carry out an evaluation of the Directive and present a report to the European Parliament and to the Council on the application of this Directive, which shall include an assessment of the need to enlarge its scope. Where appropriate, the report shall be accompanied by a proposal for the amendment of this Directive. The evaluation shall be conducted according to the

Commission's Better Regulation Guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

Article 9
Entry into force

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

Article 10
Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament
The President

For the Council
The President



Brussels, 28 February 2019
(OR. en)

6946/19

**Interinstitutional File:
2018/0107(COD)**

JAI 226
COPEN 80
CYBER 62
ENFOPOL 105
DROIPEN 28
JAIEX 31
DAPIX 82
EJUSTICE 32
MI 209
TELECOM 98
DATAPROTECT 66
CODEC 557

NOTE

From:	Presidency
To:	Council
No. prev. doc.:	6284/19
No. Cion doc.:	8115/18
Subject:	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings - General approach

INTRODUCTION

1. On 17 April 2018, the Commission adopted and transmitted to the Council and to the European Parliament the above-mentioned proposal with Articles 53 and 62 TFEU as a legal basis. The draft Directive serves as a tool to overcome the risk of diverging national approaches evidence in criminal proceedings, as it sets out the rules for the appointment of service providers' legal representatives.

2. The proposal aims at harmonising the various national approaches, that currently include: asserting national jurisdiction over a service provider on the basis of its seat, the place where it offers services or the location of its data; extending enforcement jurisdiction (extra-territoriality); or requesting that a special representative be designated for some service providers for that Member State.
3. The legal representative should reside or be established in one of the MS where the service provider is established or is offering services, and its obligations are strictly limited to the receipt of and compliance with decisions and orders issued by the MS competent authorities, and they can be subject to enforcement procedures.
4. On 18 October 2018, the European Council¹ called for a solution to be found to ensure swift and efficient cross-border access to e-evidence in order to effectively fight terrorism and other serious and organised crime, both within the EU and at international level. It stressed that the Commission proposals on e-evidence should be agreed on by the end of the current legislature.
5. In the European Parliament, Ms Birgit Sippel (LIBE, S&D) was appointed as rapporteur on 24 May 2018. The LIBE Committee discussed the proposal on 11 June 2018 and has held several meetings and hearings, including a public hearing on 27 November 2018. No timeline has been set for the adoption of the report.
6. The European Economic and Social Committee adopted its opinion on 12 July 2018².

II. WORK WITHIN THE COUNCIL

7. The Commission presented this proposal to the COPEN Working Party on 27 April 2018, followed by an article-by-article examination of the draft directive and an exchange of views on the impact assessment in the Working Party on 7-8 May 2018. In general, both the impact assessment and the proposal were positively received by delegations.

¹ EUCO 13/18, paragraph 9.

² 11533/18.

8. Discussions were centered mainly around the selection criteria proposed by the Commission for the designation of a legal representative in the Union by the service provider for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States, as well as the sanctions for non-compliance with the obligations under the directive.
9. The examination of the proposal by the Working Party were conducted under the Bulgarian, Austrian and Romanian Presidencies. Six meetings were held which resulted in three revised versions of the proposed Directive. The outcome of those discussions together with the written input received from delegations and their reservations on the text are reflected in the revised Presidency compromise text as set out in the Annex. The recitals have been adapted to reflect changes in substantive provisions. All changes compared to the Commission proposal are indicated in **bold** (new text) or ~~strikethrough~~-(deleted text).
10. Discussions were concluded on 18 February 2019 with a view to submitting the compromise text as set out in the Annex for adoption as a general approach at the forthcoming Council (Justice and Home Affairs) to be held on 7 and 8 March 2019.

III. CONCLUSION

11. The text, as set out in the Annex, reflects the efforts of the Presidency and Member States to strike a compromise.
12. On 27 February the Permanent Representatives Committee reached an agreement on the Presidency compromise text as set out in the Annex to this note with only one technical amendment as suggested by the CZ delegation.
13. The Council is therefore invited to reach a general approach on this text, which will constitute the basis for the negotiations with the European Parliament in the framework of the ordinary legislative procedure (Art. 294 TFEU).

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 53 and 62 thereof,

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee³,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Network-based services can in principle be provided from anywhere and do not require a physical infrastructure, corporate presence, or staff in the country where the services are offered, nor in the internal market itself. As a consequence, it can be difficult to apply and enforce obligations laid down in national and Union law which apply to the service providers concerned, in particular the obligation to comply with an order or a decision by a judicial authority. This is the case in particular in criminal law, where Member States' authorities face difficulties with serving, ensuring compliance and enforcing their decisions, in particular where relevant services are provided from outside their territory.

³ OJ C , , p. .

- (2) Against that background, Member States have taken a variety of disparate measures to more effectively apply and enforce their legislation. This includes measures for addressing service providers to obtain electronic evidence that is of relevance to criminal proceedings.
- (3) To that end, some Member States have adopted, or are considering adopting, legislation imposing mandatory legal representation within their own territory, for a number of service providers offering services in that territory. Such requirements create obstacles to the free provision of services within the internal market.
- (4) There is a significant risk that other Member States will try to overcome existing shortcomings related to gathering evidence in criminal proceedings by means of imposing disparate national obligations in the absence of a Union-wide approach. This is bound to create further obstacles to the free provision of services within the internal market.
- (5) Under the current circumstances, the resulting legal uncertainty affects both service providers and national authorities. Disparate and possibly conflicting obligations are set out for service providers established or offering services in different Member States, which also subject them to different sanction regimes in case of violations. This divergence in the framework of criminal proceedings will likely further expand because of the growing importance of communication and information society services in our daily lives and societies. The foregoing not only represents an obstacle to the proper functioning of the internal market but also entails problems for the establishment and correct functioning of the Union's area of freedom, security and justice.

- (6) To avoid such fragmentation and to ensure that undertakings active in the internal market are subject to the same or similar obligations, the Union has adopted a number of legal acts in related fields such as data protection⁴. To increase the level of protection for the data subjects, the rules of the General Data Protection Regulation⁵ provide for the designation of a legal representative in the Union by controllers or processors not established in the Union but offering goods or services to individuals in the Union or monitoring their behaviour if their behaviour takes place within the Union, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body.
- (7) By setting out harmonised rules on the legal representation of certain service providers in the Union for receipt of, compliance with and enforcement of decisions issued by competent authorities in the Member States for the purposes of gathering evidence in criminal proceedings, the existing obstacles to the free provision of services should be removed, as well as the future imposition of divergent national approaches in that regard should be prevented. Level playing field for service providers should be established. **This should not affect obligations on service providers deriving from other EU legislation.** Moreover, more effective criminal law enforcement in the common area of freedom, security and justice should be facilitated.

⁴ [Directive 95/46/EC](#) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31); [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1); [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

⁵ [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

- (8) The legal representative at issue should serve as an addressee for domestic orders and decisions and for orders and decisions pursuant to Union legal instruments ~~adopted~~ **falling** within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal matters, **including where those orders and decisions are transmitted in form of a certificate**. This includes both instruments that permit the direct serving of orders in cross-border situations on the service provider **or its legal representative, such as the [Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (“Regulation”)⁶**], and other instruments ~~based on~~ **for judicial cooperation applicable between the judicial authorities Member States, notably those falling within the scope of under** Title V, Chapter 4, such as the Directive on the European Investigation Order⁷ and the 2000 Mutual Legal Assistance Convention⁸. **Recourse to the legal representative should be in accordance with the procedures set out in the instruments and legislation applicable to the judicial proceedings. The competent authorities of the Member State where the legal representative resides or is established should act in accordance with the role set out for them in the respective instrument if and where an involvement is foreseen.**

⁶ **Regulation of the European Parliament and of the Council on European Production and preservation orders for electronic evidence in criminal matters**

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, OJ C 197, 12.7.2000, p. 1 and its Protocol, OJ C 326, 21.11.2001, p. 2.**

- (9) Member States shall ensure that **service providers have** the obligation to designate a legal representative ~~is immediate that is from the date of transposition set out in Article 7 for service providers that offer services in the Union at that date~~ **by [6 months from the transposition deadline of this Directive]** or from the moment service providers start offering services in the Union for those service providers that will start offering services after **[6 months from the date of transposition deadline of this Directive]**.
- (10) The obligation to designate a legal representative should apply to service providers that offer services in the Union, meaning in one or more Member States. Situations where a service provider is established on the territory of a Member State and offers services exclusively on the territory of that Member State, should not be covered by this Directive.
- (11) Notwithstanding the designation of a legal representative, Member States should be able to continue addressing service providers established on their territory, be it in purely domestic situations, be it after receipt of a request for assistance under legal instruments on mutual legal assistance and on mutual recognition in criminal matters. **Likewise Member States should be able to continue addressing the Member States where service providers are established with instruments falling within the scope of Title V, Chapter 4, such as the Directive on the European Investigation Order and the 2000 Mutual Legal Assistance Convention.**
- (12) The determination whether a service provider offers services in the Union requires an assessment whether the service provider enables legal or natural persons in the Union to use its services. However, the mere accessibility of an online interface (for instance the accessibility of the service provider's or an intermediary's website or of an email address and of other contact details) taken in isolation should not be a sufficient condition for the application of this Directive.

(13) A substantial connection to the Union should also be relevant to determine the ambit of application of this Directive. Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be ~~assessed on the basis of the existence of~~ **based on specific factual criteria such as** a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302⁹ cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union. The same considerations should apply to determine whether a service provider offers services in a Member State.

⁹ [Regulation \(EU\) 2018/302](#) of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (OJ L 601, 2.3.2018, p. 1).

(14) Service providers obliged to designate a legal representative should be able to choose to that effect an existing establishment in a Member State, be it a corporate body or a branch, agency, office or a main seat or headquarters, and also more than one legal representative.

This legal representative could also be a third party, which could be shared between several service providers, in particular small and medium-sized enterprises.

Nevertheless, a corporate group should not be forced to designate multiple representatives, one for each undertaking part of that group, **but can designate one legal representative for the group**. Different instruments ~~adopted~~ **falling** within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union apply in the relationships between Member States when gathering evidence in criminal proceedings. As a consequence of this ‘variable geometry’ that exists in the common area of criminal law, there is a need to ensure that the Directive does not facilitate the creation of further disparities or obstacles to the provision of services in the internal market by allowing service providers offering services on their territory to designate legal representatives within Member States that do not take part in relevant legal instruments, which would fall short of addressing the problem.

Therefore, at least one representative should be designated in a Member State that participates in the relevant Union legal instruments to avoid the risk of weakening the effectiveness of the designation provided for in this Directive and to make use of the synergies of having a legal representative for the receipt of, compliance with and enforcement of decisions and orders issued in the context of gathering evidence in criminal proceedings, including under the [Regulation], **the Directive on the European Investigation Order** or the 2000 Mutual Legal Assistance Convention. In addition, designating a legal representative, which could also be utilised to ensure compliance with national legal obligations, makes use of the synergies of having a clear point of access to address the service providers for the purpose of gathering evidence in criminal matters.

- (15) Service providers should be free to choose in which Member State they designate their legal representative, and Member States may not restrict this free choice, e.g. by imposing an obligation to designate the legal representative on their territory. However, the Directive also contains certain restrictions with regard to this free choice of service providers, notably that the legal representative should be established in a Member State where the service provider provides services or is established, as well as the obligation to designate a legal representative in one of the Member States participating in judicial cooperation instruments ~~adopted under~~ **falling within** Title V of the Treaty. **The sole designation of a legal representative should not be considered to constitute an establishment of the service provider.**
- (16) The service providers most relevant for gathering evidence in criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Directive. Providers of electronic communication services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. **This Directive should also be applicable to other** ~~The categories of~~ information society services **providers within the meaning of Directive (EU) 2015/1535 that 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** ~~providers,~~ **but offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf. This should be in line with the terms used in the Budapest Convention on Cybercrime. Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, i.e. technical operations to produce or alter data by means of computer processing power.**

The categories of service providers included here are, for example online marketplaces facilitating transactions between their users (such as providing consumers or and businesses) the ability to communicate with each other and other hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms. Where an information society service provider does not provide its users the ability to communicate with each other, but only with the service provider, or does not provide the ability to process or to store data, or where the ability to store/process data is not an essential part of the service provided to users, such as legal, architectural engineering and accounting services provided online at a distance, it would not fall within the scope of the definition, even if within the definition of information society services pursuant to Directive (EU) 2015/1535. Information society services for which the storage of data is not a defining component, and for which it is only of an ancillary nature, such as legal, architectural, engineering and accounting services provided online at distance, should be excluded from the scope of this Directive, even where they may fall within the definition of information society services as per Directive (EU) 2015/1535.

- (17) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and privacy and proxy service providers or regional internet registries for internet protocol ('IP') addresses, are of particular relevance when it comes to the identification of actors behind malicious or compromised web sites. They hold data that is of particular relevance for criminal investigations 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.

- (18) The legal representative should be able to comply with decisions and orders addressed to them by Member States' authorities on behalf of the service provider, which should take the appropriate measures to ensure this result, including sufficient resources and powers. The absence of such measures or their shortcomings should not serve as grounds to justify non-compliance with decisions or orders falling into the ambit of application of by this Directive, neither for the service provider nor its legal representative. **Neither should service providers be able to exculpate themselves due to missing or ineffective internal procedure, as they are responsible for providing the necessary resources and powers to guarantee compliance with orders and national decisions. Nor should the legal representative be able to exculpate himself by claiming for example he is not empowered to deliver data. The service provider and its legal representative(s) should remain free to allocate among themselves the tasks of identifying and accessing the requested evidence as long as decisions and orders addressed to them are complied with.**
- (19) Service providers should notify the Member State in which the legal representative resides or is established of the identity and contact details of their legal representative, as well as related changes and updates of information. The notification should also provide information about the languages in which the legal representative can be addressed, which should include ~~at least one~~ **or more** of the official languages **in accordance with the national law** of the Member State where the legal representative resides or is established, but may include other official languages of the Union, such as the language of its headquarters.

When the service provider designates more than one legal representative, it may also notify considerations to determine which one should be addressed. ~~These considerations are not binding for Member States' authorities, but should be followed except in duly justified~~ **where the competent authorities consider it is necessary to depart from those considerations on a case-by-cases basis e.g. when the legal representative is unavailable or uncooperative. Where the competent authorities, by way of exception, depart from these considerations they should only address a legal representative established in a Member State participating in the respective instrument. All this information, which is of particular relevance for Member States' authorities, should be made publicly available by the service provider, for example on its website, in a manner comparable to the requirements for making available general information pursuant to Article 5 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market¹⁰ (e-Commerce Directive). For those service providers subject to the e-Commerce Directive, Article 3(3) complements but does not replace these requirements.** Furthermore, Member States should **also publish and keep up-to-date** the relevant information for their country on a dedicated ~~site~~ **internet page** of the ~~e-Justice Portal~~ **European Judicial Network in criminal matters** to facilitate coordination between Member States and use of the legal representative by authorities from another Member State. **The data may also be further disseminated to facilitate access to this data by competent authorities, such as via dedicated intranet sites or forums and platforms.**

¹⁰ ~~Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).~~

(20) **The service provider should be subject to effective, proportionate and dissuasive sanctions for the infringement of its obligations to designate a legal representative, to entrust the legal representative with the necessary powers and resources to comply with decisions and orders, establish the appropriate procedures and to notify and make publicly available the information related thereto should be subject to effective, proportionate and dissuasive sanctions. The service provider and the legal representative should be subject to effective, proportionate and dissuasive sanctions for the systematic infringement by the legal representative of the obligation to cooperate with the competent authorities when receiving decisions and orders. Member States should ensure that both the designated legal representative and the service provider can be held jointly and severally liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders. Jointly and severally liable means that either the legal representative or the service provider may be sanctioned for non-compliance by either of them with any of the obligations under this Directive. Joint and several liability should not apply for actions or omissions of either the service provider or the legal representative which constitute a criminal offence under the law of the Member State imposing the sanction.** Under no circumstances should the sanctions determine a ban, permanent or temporary, of service provision. Member States should coordinate their enforcement action where a service provider offers services in several Member States. **Central authorities should coordinate** to ensure a coherent and proportionate approach, ~~a coordination mechanism is provided~~. The Commission could facilitate such coordination if necessary, but needs to be informed of cases of infringement. This Directive does not govern the contractual arrangements for transfer or shifting of financial consequences between service providers and legal representatives of sanctions imposed upon them.

- (20a) **When determining in the individual case the appropriate and proportionate sanction, the competent authorities should also take into account the financial capacity of the service provider.**
- (21) This Directive is without prejudice to the investigative powers of authorities in civil or administrative proceedings, including where such proceedings can lead to sanctions.
- (22) In order to ensure the application of the Directive in a consistent manner, additional mechanisms for the coordination between Member States should be put in place. For that purpose, Member States should designate a central authority that can provide central authorities in other Member States with information and assistance in the application of the Directive, in particular where enforcement actions under the Directive are considered. This coordination mechanism should ensure that relevant Member States are informed of the intent of a Member State to undertake an enforcement action. In addition, Member States should ensure that central authorities can provide each other **any relevant information and** with assistance in those circumstances, and cooperate with each other where relevant. Cooperation amongst central authorities in the case of an enforcement action may entail the coordination of an enforcement action between competent authorities in different Member States. **It should aim to avoid positive or negative conflicts of competence.** For the coordination of an enforcement action, central authorities **should** ~~shall~~ also involve the Commission where relevant. The existence of the **obligation of these authorities to cooperate** ~~coordination mechanism~~ does not prejudice the right of an individual Member State to impose sanctions on service providers that fail to comply with their obligations under the Directive. The designation and publication of information about central authorities will facilitate the notification by service providers of the designation and contact details of its legal representative to the Member State where its legal representative resides or is established of the designation and contact details.

- (23) Since the objective of this Directive, namely to remove obstacles to the free provision of services in the framework of gathering evidence in criminal proceedings, cannot be sufficiently achieved by the Member States, but can rather, by reason of the borderless nature of such services, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.
- (24) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council¹¹ and delivered an opinion on (...) ¹²,
- (25) The Commission should carry out an evaluation of this Directive that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU value added and should provide the basis for impact assessments of possible further measures. The evaluation should be completed 5 years after entry into application, to allow for the gathering of sufficient data on its practical implementation. Information should be collected regularly and in order to inform the evaluation of this Directive.

¹¹ [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).

¹² OJ C , , p. .

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive lays down rules on the legal representation in the Union of certain service providers for receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings.
2. Member States ~~may~~ **shall** not impose additional obligations to those deriving from this Directive on service providers covered by this Directive for the purposes set out in paragraph 1.
3. This Directive is without prejudice to the powers of national authorities in accordance with Union and national law to address **directly** service providers established on their territory for the purposes referred to ~~in~~ in paragraph 1.
4. This Directive shall apply to the service providers defined in Article 2(2) offering their services in the Union. It shall not apply where those service providers are established on the territory of a single Member State and offer services exclusively on the territory of that Member State.

Article 2
Definitions

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

- (1) ‘legal representative’ means a legal or natural person, designated in writing by a service provider for the purpose of Articles 1(1), 3(1), 3(2) and 3(3);
- (2) ‘service provider’ means any natural or legal person that provides one or more of the following categories of services, **with the exception of financial services referred to in Article 2(2)(b) of Directive 2006/123/EC**:
 - (a) electronic communications service as defined in Article 2(4) of ~~{~~Directive (EU) 2018/1972 establishing the European Electronic Communications Code¹³~~}~~;
 - (b) **internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and related privacy and proxy services**;
 - (c) **other** information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council¹⁴ **that provide**:
 - **the ability to its users to communicate with each other; or**
 - **to process or store data on behalf of the users to whom the service is provided for which the storage of data is a defining component of the service provided to the user, including social networks, online marketplaces facilitating transactions between their users, and other hosting service providers;**

¹³ **Directive (EU) 2018/1972 of the European Parliament and Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36.)**

¹⁴ [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).

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

- (3) ‘offering services in a Member State’ means:
- (a) enabling legal or natural persons in a Member State to use the services referred to in point (2); and
 - (b) having a substantial connection **based on specific factual criteria** to the Member State referred to in point (a);
- (4) ‘establishment’ or ‘**being established**’ means ~~either~~ the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or ~~a stable infrastructure from where~~ the business is managed;
- (5) ‘group’ means a group as defined in Article 3(15) of Directive (EU) 2015/849 of the European Parliament and of the Council¹⁵.

Article 3

Legal representative

1. Member States where a service provider offering services in the Union is established shall ensure that it designates at least one legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider is established or offers the services.

¹⁵ [Directive \(EU\) 2015/849](#) of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

2. Where a service provider is not established in the Union, Member States shall ensure that such service provider offering services on their territory designates at least one legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.
3. As regards the receipt of, compliance with and enforcement of decisions and orders issued by the competent authorities of Member States under Union legal instruments ~~adopted~~ **falling** within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal proceedings, the Member States taking part in those legal instruments shall ensure that service providers offering services on their territory designate at least one representative in one of them. The legal representative shall reside or be established in one of the Member States where the service provider offers the services.
4. Service providers ~~shall be free to~~ **may** designate additional legal representatives, ~~resident or established in other Member States, including those where the service providers are~~ **established or** offer their services. Service providers ~~which are part of a group~~ shall be allowed to collectively designate one legal representative.
5. Member States shall ensure that the decisions and orders by ~~the their~~ competent authorities for evidence gathering in criminal proceedings are addressed to the legal representative designated by the service provider to that effect. That **legal** representative shall be entrusted with the receipt, **of and** compliance **with and enforcement** of those decisions and orders on behalf of the service provider concerned, **and can be subject to enforcement measures.**

6. Member States shall ensure that service providers established or offering services in their territory provide their legal representative with the necessary powers and resources to comply with ~~these~~ decisions and orders **received from any Member State**.
- 7.¹⁶ ~~To this end, The~~ Member States ~~where shall ensure that~~ the legal representatives ~~are~~ residing or ~~are~~ established ~~on their territory~~ **shall verify that the said legal representatives have received from the service providers the necessary powers and resources to comply with decisions and orders received from any Member State and that they** cooperates with the competent authorities when receiving those decisions and orders, in accordance with the applicable legal framework.
8. Member States shall ensure that **both the** designated legal representative **and the service provider** can be held **jointly and severally** liable for non-compliance with obligations deriving from the applicable legal framework when receiving decisions and orders, ~~without prejudice to the liability and legal actions that could be initiated against the service provider~~ **with the effect that each of the legal representative and service provider may be sanctioned for non-compliance of either of them**. In particular, the lack of appropriate internal procedures between the service provider and the legal representatives cannot be used **by either side** as a justification for non-compliance with those obligations. **Joint and several liability shall not apply for actions or omissions of either the service provider or the legal representative which constitute a criminal offence in the Member State applying the sanction**.
9. Member States shall ensure that the obligation to designate a legal representative ~~applies~~ **is fulfilled by [6 months from the date of transposition set out in Article 7]** for service providers that offer services in the Union at that date, or from the moment service providers start offering services in the Union for those service providers that will start offering services after ~~the date of transposition of the Directive~~ **that date**.

¹⁶ Paragraphs 6 and 7 of this Article from the Commission Proposal have been switched.

Article 4
Notifications and languages

1. Member States shall ensure that, upon designation of its legal representative in accordance with Article 3(1), (2), ~~and (3)~~ **and (4)**, each service provider established or offering services in their territory notifies in writing the central authority of the Member State where its legal representative resides or is established of the designation and contact details of its legal representative as well as any changes thereof.
2. The notification shall specify the official language(s) of the Union, as referred to in Regulation 1/58, in which the legal representative can be addressed. This shall include, ~~at least,~~ **one or more of the official languages in accordance with the national law** of the Member State where the legal representative resides or is established.
3. When a service provider designates several representatives, the notification shall specify the official language(s) of the Union or Member States covered by each of them ~~or~~ **and** any other considerations to determine the appropriate legal representative to be addressed. ~~In duly justified cases, Member States'~~ **Competent** authorities may depart from those considerations **on a case-by-case basis; where necessary Member States shall ensure that in such cases, the addressed legal representative has to comply with these orders and decisions.**
4. [~~Member States shall ensure that the service provider makes the information notified to them in accordance with this Article is publicly available~~] ~~Member States shall publish that information on a dedicated internet page of the e-Justice Portal of the European Judicial Network in criminal matters.~~ **Member States shall ensure that this information is regularly updated. This information may be further disseminated to facilitate access by competent authorities.**

Article 5

Sanctions

1. Member States shall lay down rules on sanctions applicable to infringements of national provisions adopted pursuant to **Article 3 and 4** ~~this Directive~~ and shall take all measures necessary to ensure that they are implemented. The sanctions provided for shall be effective, proportionate and dissuasive.
2. Member States shall, by the date set out in Article 7, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. Member States shall also inform the Commission on an annual basis about non-compliant service providers and relevant enforcement action taken against them.

Article 6

~~Coordination mechanism~~ **Central authorities**

1. **In accordance with their legal systems**, Member States shall designate **one or more** a central **authorities** ~~authority or, where its legal system so provides, more than one central authority~~, to ensure the application of this Directive in a consistent and proportionate manner.
2. Member States shall inform the Commission of their designated central authority, or central authorities, referred to in paragraph 1. The Commission shall forward a list of designated central authorities to the Member States. The Commission will also make publicly available a list of designated central authorities to facilitate the notifications by a service provider to the Member States where its legal representative resides or is established.
3. Member States shall ensure that **their** central authorities ~~shall provide each other with relevant~~ **coordinate and cooperate with each other and, where relevant, with the Commission, and provide any appropriate** information and ~~mutual~~ assistance **to each other in order to relevant to application of apply this** Directive in a consistent and proportionate manner. The **coordination, cooperation and** provisioning of information and ~~mutual~~ assistance shall cover, in particular, enforcement actions.

~~4. Member States shall ensure that the central authorities shall cooperate with each other and, where relevant, with the Commission to ensure the application of this Directive in a consistent and proportionate manner. Cooperation shall cover, in particular, enforcement actions.~~

Article 7

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by ~~6~~ **18** months after entry into force. They shall immediately inform the Commission thereof.
2. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.
3. Member States shall communicate to the Commission the text of the measures of national law which they adopt in the field covered by this Directive.

Article 8

Evaluation

By [~~5 years from the date of application of this Directive~~] at the latest, the Commission shall carry out an evaluation of the Directive and present a report to the European Parliament and to the Council on the application of this Directive, which shall include an assessment of the need to enlarge its scope. Where appropriate, the report shall be accompanied by a proposal for the amendment of this Directive. The evaluation shall be conducted according to the Commission's Better Regulation Guidelines. Member States shall provide the Commission with the information necessary for the preparation of that Report.

Article 9

Entry into force

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

Article 10

Addressees

This Directive is addressed to the Member States ~~in accordance with the Treaties~~.

Done at Brussels,

For the European Parliament

The President

For the Council

The President
