

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on European Production and Preservation Orders for electronic evidence in
criminal matters
2018/0108(COD)
DRAFT

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Formula				
1	COM/2018/225 final - 2018/0108 (COD)	A9-9999/2020 - 11 December 2020	10206/19 as supplemented by 9365/19	
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic <i>information</i> in criminal <i>proceedings</i>	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters	
Formula				
3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,			
Formula				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1) thereof,			
Formula				
5	Having regard to the proposal from the European Commission,			
Formula				
6	After transmission of the draft legislative act to the national parliaments,			
Formula				
7	Having regard to the opinion of the European Economic and Social Committee ¹ , _____ ¹ OJ C , , p. .			
Formula				
8	Acting in accordance with the ordinary legislative procedure,			
9	Whereas:			
Recital 1				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
10	(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.			
Recital 2				
11	(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.	(2) Measures to obtain and preserve electronic <i>information</i> are increasingly important to enable criminal investigations and prosecutions across the Union. Effective mechanisms to obtain electronic <i>information</i> are <i>essential</i> to combat crime, subject to conditions <i>and safeguards</i> to ensure full <i>compliance</i> with fundamental rights and principles recognised in <i>Article 6 of the Treaty on European Union (TEU) and</i> the Charter of Fundamental Rights of the European Union (<i>'the Charter'</i>), in particular the principles of necessity and proportionality, due process, protection of privacy <i>and personal data and confidentiality of communications</i> .	(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.	
Recital 3				
12	(3) The 22 March 2016 Joint Statement of the Ministers of Justice and Home Affairs and representatives of the Union	(3) The 22 March 2016 Joint Statement of the Ministers of Justice and Home Affairs and representatives of the Union	(3) The 22 March 2016 Joint Statement of the Ministers of Justice and Home Affairs and representatives of the Union	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 4				
13	(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.	(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.	(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.	
Recital 5				
14	(5) In the Joint Communication on Resilience, Deterrence and Defence of 13 September 2017 ² , the Commission emphasised that effective investigation and prosecution of cyber-enabled crime was a key deterrent to cyber-attacks, and that today's procedural framework needed to be better adapted to the internet age. Current procedures at times could not match the speed of cyber-attacks, which create particular need for swift cooperation across borders. ----- ² JOIN(2017) 450 final.	(5) In the Joint Communication on Resilience, Deterrence and Defence of 13 September 2017, the Commission emphasised that effective investigation and prosecution of cyber-enabled crime was a key deterrent to cyber-attacks, and that today's procedural framework needed to be better adapted to the internet age. Current procedures at times could not match the speed of cyber-attacks, which create particular need for swift cooperation across borders. ----- ²JOIN(2017) 450 final.	(5) In the Joint Communication on Resilience, Deterrence and Defence of 13 September 2017 ² , the Commission emphasised that effective investigation and prosecution of cyber-enabled crime was a key deterrent to cyber-attacks, and that today's procedural framework needed to be better adapted to the internet age. Current procedures at times could not match the speed of cyber-attacks, which create particular need for swift cooperation across borders. ----- ² JOIN(2017) 450 final.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 6				
15	<p>(6) The European Parliament echoed these concerns in its Resolution on the fight against cybercrime of 3 October 2017³, 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.</p> <p>³2017/2068(INI).</p>	<p>(6) The European Parliament echoed these concerns in its Resolution on the fight against cybercrime of 3 October 2017³, 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.</p> <p>³2017/2068(INI).</p>	<p>(6) The European Parliament echoed these concerns in its Resolution on the fight against cybercrime of 3 October 2017³, 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.</p> <p>³2017/2068(INI).</p>	
Recital 7				
16	<p>(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.</p>	<p>(7) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the relevant country <i>where the service is offered</i>. Therefore, relevant <i>electronic information</i> is often stored outside of the investigating State, <i>creating challenges regarding the gathering of electronic information in criminal proceedings</i>.</p>	<p>(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.</p>	
Recital 8				
17	<p>(8) Due to this lack of connection, judicial cooperation requests are often addressed to states which are hosts to a large number of</p>	<p>(8) Due to this, judicial cooperation requests are often addressed to states which are hosts to a large number of service</p>	<p>(8) Due to this lack of connection, judicial cooperation requests are often addressed to states which are hosts to a large number of</p>	

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p>providers. Furthermore, the number of requests has multiplied. As a result, obtaining electronic <i>information</i> using judicial cooperation channels often takes a long time — <i>which may cause problems due to the often volatile nature of electronic information</i>. Furthermore, there is no <i>harmonised</i> 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 <i>increasingly</i> rely on <i>voluntary direct</i> cooperation channels with service providers where available, <i>applying</i> different national tools, conditions and procedures.</p>	<p>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.</p>	
Recital 9				
18	<p>(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.</p>	<p>(9) The fragmented legal framework creates challenges for <i>law enforcement, judicial authorities and</i> service providers seeking to comply with <i>legal</i> requests, <i>as they are increasingly faced with legal uncertainty and, potentially, conflicts of law</i>. Therefore there is a need to put forward <i>specific rules as regards cross-border judicial cooperation for preserving and producing electronic information, in order to complement the existing EU law and to clarify the rules of the cooperation between law enforcement, judicial</i></p>	<p>(9) The fragmented legal framework creates challenges for service providers seeking to comply with law enforcement requests. Therefore there is a need to put forward a European legal framework for electronic evidence to impose an obligation on service providers covered by the scope of the instrument to respond directly to authorities without systematic the involvement of a judicial authority in the Member State of the service provider in every case.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>authorities and service providers in the field of electronic information, while ensuring full compliance with fundamental rights and principles recognised in Article 6 TEU and the Charter and with the rule of law.</i>		
Recital 9a				
19		<p><i>(9a) Directive 2014/41/EU of the European Parliament and of the Council³ provides for the acquisition, access and production of evidence in one Member State for criminal investigations and proceedings in another Member State. The procedures and timelines foreseen in the EIO may not be appropriate for electronic information, which is more volatile and could more easily and quickly be deleted. This Regulation therefore provides for specific procedures that address the nature of electronic information. However, in order to avoid a long-term fragmentation of the Union framework for judicial cooperation in criminal matters, in the mid-term, the Commission should assess the functioning of the Regulation in relation with Directive 2014/41/EU of the European Parliament and of the Council.</i></p> <p>-----</p> <p>³ <i>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).</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 10				
20	(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.	(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.	(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.	
Recital 10a				
21		<i>(10a) This Regulation respects fundamental rights and observes the principles recognised by Article 6 TEU and the Charter, by international law and international agreements to which the Union or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in Member States' constitutions, in their respective fields of application. Such rights and principles include, in particular, the respect for private and family life, the protection of personal data, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of legality and proportionality, as well as the right not to be tried or punished twice in criminal</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>proceedings for the same criminal offence.</i>		
Recital 10b				
22		<i>(10b) Nothing in this Regulation should be interpreted as prohibiting the refusal to execute a European Production Order where there are reasons to believe, on the basis of objective elements, that the European Production Order has been issued for the purpose of prosecuting or punishing a person on account of the person's gender, racial or ethnic origin, religion, sexual orientation or gender identity, nationality, language or political opinions, or that the person's position may be prejudiced for any of those reasons.</i>		
Recital 11				
23	(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.	(11) The mechanism of the European Production Order and the European Preservation Order for electronic information in criminal proceedings works on the condition of mutual trust between the Member States and a presumption of compliance by other Member States with Union law, the rule of law and, in particular, with fundamental rights , which are essential elements of the area of freedom, security and justice within the Union. However, if the executing authority has substantial grounds for believing that the execution of a European Production Order would not be compatible with its obligations concerning	(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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>the protection of fundamental rights recognised in Article 6 TEU and in the Charter, the execution of the European Production Order should be refused. Before deciding to raise one of the grounds for non-recognition or non-execution provided for in this Regulation, the executing authority should consult the issuing authority in order to obtain any necessary additional information. Information regarding a reasoned proposal by the Commission to the Council on the basis of Article 7(1) and 7(2) TEU, indicating systemic or generalised deficiencies, should be particularly relevant for the purposes of that assessment.</i></p>		
Recital 11a				
24		<p><i>(11a) If the European Council were to adopt a decision determining, as provided for in Article 7(2) TEU, that there is a serious and persistent breach in the issuing Member State of the principles set out in Article 2 TEU, such as those inherent in the rule of law, the executing judicial authority may decide automatically to raise one of the grounds for non-recognition or non-execution provided for in this Regulation, without having to carry out any specific assessment.</i></p>		
Recital 11b				
25		<p><i>(11b) The respect for private and family life and the protection of natural persons</i></p>		

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
		<p><i>regarding the processing of personal data are fundamental rights. In accordance with Articles 7 and 8(1) of the Charter and Article 16(1) of the TFEU, everyone has the right to respect for his or her private and family life, home and communications and to the protection of personal data concerning them. When implementing this Regulation, Member States should ensure that personal data are protected and processed only in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council⁴ and Directive (EU) 2016/680 of the European Parliament and of the Council⁵, as well as Directive 2002/58/EC of the European Parliament and of the Council⁶.</i></p> <hr/> <p>⁴ <i>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).</i></p> <p>⁵ <i>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</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJL 119 4.5.2016, p. 89).</i></p> <p>⁶ <i>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) (OJL 201, 31.7.2002, p.37).</i></p>		
Recital 11c				
26		<p><i>(11c) Personal data obtained under this Regulation should only be processed when necessary and in a manner that is proportionate to the purposes of prevention, investigation, detection and prosecution of crime or enforcement of criminal sanctions and the exercise of the rights of defence. In particular, Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers for the purposes of this Regulation, including measures to ensure the security of the data. Service providers should ensure that the same safeguards apply for the transmission of personal data to relevant authorities. Only authorised persons should have access to information containing personal data.</i></p>		
Recital 12				

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
27	<p>(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/JHA⁴.</p> <p>-----</p> <p>⁴ 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).</p>	<p>(12) This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. These include the right to liberty and security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of the legality and proportionality, as well as the right not to be tried or punished twice in criminal proceedings for the same criminal offence. In case the issuing Member State has indications that parallel criminal proceedings may be ongoing in another Member State, it shall consult the authorities of this Member State in accordance with Council Framework Decision 2009/948/JHA.</p>	<p>(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.</p>	
Recital 12a				
28			<p>(12a) In case, the issuing Member State has indications that parallel criminal proceedings may be ongoing in another Member State, it shall consult the authorities of this Member State in</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>accordance with Council Framework Decision 2009/948/JHA ⁴. In any case, a European Production Order should not be issued, if the issuing Member State has indications that this would be contrary to the ne bis in idem principle.</p> <p>_____</p> <p>⁴ 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).</p>	
Recital 13				
29	(13) In order to guarantee full respect of fundamental rights, this Regulation explicitly refers to the necessary standards regarding the obtaining of any personal data, the processing of such data, the judicial review of the use of the investigative measure provided by this instrument and the available remedies.	(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.	(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.	
Recital 13a				
30		<i>(13a) According to the European Court of Justice case-law, a general and indiscriminate data retention by EU national security authorities seriously interferes with the privacy rules enshrined, in particular, in the EU Charter of Fundamental Rights. Therefore, the application of this Regulation should not have the effect of resulting in any general and</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>indiscriminate retention of data, nor should it affect any rights of or obligations incumbent on service providers concerning the security of data, including the right to encryption.</i>		
Recital 14				
31	<p>(14) This Regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in Directives 2010/64/EU⁵, 2012/13/EU⁶, 2013/48/EU⁷, 2016/343⁸, 2016/800⁹ and 2016/1919¹⁰ of the European Parliament and of the Council.</p> <p>-----</p> <p>⁵ 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).</p> <p>⁶ 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).</p> <p>⁷ 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</p>	<p>(14) The procedural rights in criminal proceedings set out in Directives 2010/64/EU⁷, 2012/13/EU⁸, 2013/48/EU⁹, 2016/343¹⁰, 2016/800¹¹ and 2016/1919¹² of the European Parliament and of the Council should apply, within the scope of those Directives, to criminal proceedings covered by this Regulation as regards the Member States bound by those Directives. The procedural safeguards under the Charter apply to all proceedings covered by this Regulation.</p> <p>-----</p> <p>⁷ 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).</p> <p>⁸ 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).</p> <p>⁹ 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</p>	<p>(14) This Regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in Directives 2010/64/EU⁵, 2012/13/EU⁶, 2013/48/EU⁷, 2016/343⁸, 2016/800⁹ and 2016/1919¹⁰ of the European Parliament and of the Council.</p> <p>-----</p> <p>⁵ 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).</p> <p>⁶ 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).</p> <p>⁷ 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</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).</p> <p>⁸ 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).</p> <p>⁹ 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).</p> <p>¹⁰ 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).</p>	<p>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).</p> <p>¹⁰ 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).</p> <p>¹¹ 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).</p> <p>¹² 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).</p>	<p>consular authorities while deprived of liberty (OJ L 294, 6.11.2013, p. 1).</p> <p>⁸ 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).</p> <p>⁹ 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).</p> <p>¹⁰ 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).</p>	
Recital 14a				
32		<i>(14a) Where the issuing Member State has reason to believe that parallel criminal proceedings may be ongoing in another Member State, it should consult the authorities of the latter Member State</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>in accordance with Council Framework Decision 2009/948/JHA¹³.</i></p> <p>_____</p> <p>¹³ <i>Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJL 328, 15.12.2009, p. 42).</i></p>		
Recital 15				
33	<p>(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.</p>	<p>(15) This instrument lays down the rules under which, <i>in a criminal proceeding</i>, a competent judicial authority in the European Union may order a service provider offering services in the Union to produce or preserve electronic information that may serve as evidence through a European Production or Preservation Order. This Regulation is applicable in all cross-border cases where the service provider has its main establishment in another Member State, or, if where it is not established in the Union, is legally represented in another Member State. Authorities of the Member States should not issue domestic orders with extraterritorial effects for the production or preservation of electronic information that could be requested on the basis of this Regulation.</p>	<p>(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.</p>	
Recital 16				
34	<p>(16) The service providers most relevant for criminal proceedings are providers of</p>	<p>(16) The service providers most relevant for gathering electronic information in</p>	<p>(16) The service providers most relevant for criminal proceedings are providers of</p>	

Commission Proposal	EP mandate	Council Mandate	Draft agreement
<p>electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Providers of electronic communications services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. 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.</p>	<p>criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Providers of electronic communication services are defined in Directive <i>(EU) 2018/1972 of the European Parliament and of the Council</i>¹⁴. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. The categories of information society services included <i>in this Regulation</i> 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.</p> <p>-----</p> <p>¹⁴ <i>Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJL 321, 17.12.2018, p. 36).</i></p>	<p>electronic communications services and specific providers of information society services that facilitate interaction between users. Thus, both groups should be covered by this Regulation. Providers of electronic communications services are defined in the proposal for a Directive establishing the European Electronic Communications Code. They include inter-personal communications such as voice-over-IP, instant messaging and e-mail services. This Regulation should also be applicable to other The categories of information society services providers within the meaning of Directive (EU) 2015/1535 included here are those for which the storage of data is a defining component of the service provided to the user and refer in particular to social networks to the extent they that do not qualify as electronic communications services-providers, but offer their users the ability to communicate with each other or offer their users services that can be used to process or store data on their behalf. This should be in line with the terms used in the Budapest Convention on cybercrime. Processing of data should be understood in a technical sense, meaning the creation or manipulation of data, i.e. technical operations to produce or alter data by means of computer processing power. The categories of service providers included here are, for example online marketplaces facilitating transactions between their users (such as providing consumers or businesses the ability to communicate with each other and other</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms. Where an information society service provider does not provide its users the ability to communicate with each other, but only with the service provider, or does not provide the ability to process or to store data, or where the ability to store/process data is not an essential part of the service provided to users, such as legal, architectural, engineering and accounting services provided online at a distance, it would not fall within the scope of the definition, even if within the definition of information society services pursuant to Directive (EU) 2015/1535. Information society services for which the storage of data is not a defining component of the service provided to the user, and for which it is only of an ancillary nature, such as legal, architectural, engineering and accounting services provided online at a distance, should be excluded from the scope of this Regulation, even where they may fall within the definition of information society services as per Directive (EU) 2015/1535.</p>	
Recital 17				
35	(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	(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	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 18				
36	(18) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and proxy 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.	(18) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and proxy service providers, or regional internet registries for internet protocol ('IP') addresses, are of particular relevance when it comes to the identification of actors behind malicious or compromised web sites. They hold data that <i>could</i> allow for the identification of an individual or entity behind a web site used in <i>a</i> criminal activity, or the victim of <i>a</i> criminal activity	(18) Providers of internet infrastructure services related to the assignment of names and numbers, such as domain name registrars and registries and proxy 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.	
Recital 18a				
37		<i>(18a) Orders under this Regulation should be addressed to the main establishment of the service providers or to legal representatives designated for that purpose as regards service providers not established in one of the Member States bound by this Regulation. As regards a service provider with establishments in more than one Member State, the main establishment should be the place of its</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>central administration in the Union, unless the decisions on the purposes and means of the processing of data are taken in another establishment of the service provider in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions should be considered to be the main establishment.</i>		
Recital 19				
38	(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.	(19) This Regulation regulates gathering of data stored by a service provider at the time of the issuing of a European Production or Preservation Order only . It does not stipulate a general data retention obligation, nor does it authorise interception of data or obtaining data stored at a future point from the issuing of a European production or preservation order.	(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.	
Recital 20				
39	(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.	(20) The categories of data which this Regulation covers include subscriber data, traffic data and content data. Such categorisations are in line with the laws of many Member States, Union law such as Directive 2002/58/EC and the case law of the Court of Justice, as well as international law, notably the Convention on Cybercrime of the Council of Europe (CETS No.185) (‘Budapest convention’) .	(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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 21				
40	<p>(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.</p>	<p>(21) It is appropriate to single out subscriber data as a specific data category used in this Regulation. Subscriber data is pursued to identify the underlying user, and the level of interference with fundamental rights is lower than is the case with other, more sensitive data categories.</p>	<p>(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.</p>	
Recital 22				
41	<p>(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.</p>	<p>(22) Traffic data, on the other hand, is generally pursued to obtain more privacy-intrusive information, such as the contacts and whereabouts of the user and may be served to establish a comprehensive profile of an individual concerned. Therefore, as regards its sensitivity, traffic data is comparable to content data.</p>	<p>(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.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 22a				
42		<p><i>(22a) IP addresses can constitute a crucial starting point for criminal investigations in which the identity of a suspect is not known. According to the EU acquis as interpreted by the European Court of Justice, IP addresses are to be considered personal data and have to benefit from the full protection under the EU data protection acquis. In addition, under certain circumstances, they can be considered traffic data. However, for the purpose of a specific criminal investigation, law enforcement authorities might request an IP address for the sole purpose of identifying the user and, in a subsequent step, the name or address of the subscriber or the registered user. In such cases, it is appropriate to apply the same regime as for subscriber data, as defined under this Regulation.</i></p>		
Recital 22b				
43		<p><i>(22b) Metadata can be processed and analysed more easily than content data, as it is already brought into a structured and standardised format, but, where derived from electronic communications services or protocols, it may also reveal very sensitive and personal information. It is therefore essential that, where metadata of other electronic communications services or protocols are stored, transmitted, distributed or exchanged by using the respective services/by the service</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>providers, they are to be considered content data.</i>		
Recital 23				
44	(23) All data categories contain personal data, and are thus covered by the safeguards under the Union data protection <i>acquis</i> , 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.	(23) All data categories contain personal data, and are thus covered by the safeguards under the Union data protection <i>acquis</i> . However , the intensity of the impact on fundamental rights varies between the categories , in particular between subscriber data on the one hand and traffic data and content data on the other. While subscriber data and IP addresses could be useful to obtain first leads in an investigation about the identity of a suspect, traffic and content data are often more relevant as probative material, which could finally lead to a conviction of the suspect . It is therefore essential that all these data categories are covered by the instrument. Because of the different degree of interference with fundamental rights, different safeguards and conditions are imposed for obtaining such data.	(23) All data categories contain personal data, and are thus covered by the safeguards under the Union data protection <i>acquis</i> , 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.	
Recital 24				
45	(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	(24) The European Production Order and the European Preservation Order are investigative measures that should be issued only in the framework of specific criminal proceedings concerning a concrete criminal offence that has already taken place, after an individual evaluation of the proportionality and necessity in	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	of the proportionality and necessity in every single case.	every single case, <i>taking into account the rights of the suspected or accused person.</i>	of the proportionality and necessity in every single case.	
Recital 24a				
46			(24a) As proceedings for mutual legal assistance may be considered as criminal proceedings in accordance with applicable national law in the Member States, it should be clarified that a European Production Order or a European Preservation Order should not be issued to provide mutual legal assistance to another Member State or third country. In such cases, the mutual legal assistance request should be addressed to the Member State or third country which can provide mutual legal assistance under its domestic law. However, if electronic evidence had already been obtained under this Regulation by the issuing authority for its own criminal investigations or proceedings and afterwards this evidence is subject to transfer or transmission, the conditions on the speciality principle should apply.	
Recital 24b				
47			(24b) This Regulation should apply to criminal proceedings initiated by the issuing authority in order to localise a convict that absconded from justice to execute custodial sentences or detention orders. However, in case the sentence or detention order was rendered in absentia it should not be possible to issue	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			a European Production Order or a European Preservation Order as national law of the Member States on judgments in absentia vary considerably throughout the European Union.	
Recital 25				
48	(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.	(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.	(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.	
Recital 26				
49	(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.	(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.	(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.	
Recital 27				
50	(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	(27) Determining whether a service provider offers services in the Union requires an assessment whether it is apparent that the service provider envisages offering services to data subjects, either legal or natural persons, in one or more Member States in the Union . However, the mere accessibility of an online interface, as for instance the accessibility of the website or an e-mail	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.	address <i>or</i> other contact details <i>of a service provider or an intermediary, or the use of a language also used in a Member State, should be considered insufficient to ascertain such intention.</i>	or more Member States taken in isolation should not be a sufficient condition for the application of this Regulation.	
Recital 28				
51	(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	(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 <i>should</i> 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	(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 on the basis of the existence on specific factual criteria such as a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection is	

Commission Proposal	EP mandate	Council Mandate	Draft agreement
<p>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 matters¹¹. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302¹² cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.</p> <p>-----</p> <p>¹¹ 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).</p> <p>¹² 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).</p>	<p>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 matters¹⁵. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302¹⁶ cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.</p> <p>-----</p> <p>¹⁵ 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).</p> <p>¹⁶ 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).</p>	<p>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 matters¹¹. On the other hand, provision of the service in view of mere compliance with the prohibition to discriminate laid down in Regulation (EU) 2018/302¹² cannot be, on that ground alone, be considered as directing or targeting activities towards a given territory within the Union.</p> <p>-----</p> <p>¹¹ 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).</p> <p>¹² 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).</p>	
Recital 28a			

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
52		<p><i>(28a) Situations, where there is an imminent threat to life or physical integrity of a person, should be treated as emergency cases and allow for shorter time limits on the service provider and the executing authority. Where the disruption or destruction of a critical infrastructure would directly imply an imminent risk to the life or physical integrity of a person, such a situation should also be treated as an emergency case, in accordance with EU law.</i></p>		
Recital 29				
53	<p>(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.</p>	<p>(29) A European Production Order should only be issued if it is necessary and proportionate, taking into account the rights of the suspected or accused person and the seriousness of the offence. The assessment should take into account whether it could have been ordered under the same conditions in a similar domestic case, whether there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border production of the data and where the requested information is relevant for the investigation. The Order should be limited to what is strictly necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the individual case only and should be limited to data of specific persons with a direct link to the specific proceedings. The direct link between the person whose data are sought</p>	<p>(29) A European Production Order should only be issued if it is necessary and proportionate. The assessment should take into account whether the Order is limited to what is necessary to achieve the legitimate aim of obtaining the relevant and necessary data to serve as evidence in the individual case only, taking due account of the impact of the measure on fundamental rights of the person whose data are sought.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>and the purpose of the specific proceeding must be demonstrable at all times.</i>		
Recital 30				
54	(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.	(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 <i>traffic</i> and content data, the issuing or validation of European Production Orders for production of these categories requires review by a judge. As subscriber data are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent <i>public</i> prosecutors, <i>where such a public prosecutor is capable of exercising its responsibilities objectively. Where so provided by national law, the execution of the order might require the procedural involvement of a court in the executing State.</i>	(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.	
Recital 30a				
55		<i>(30a) The competent issuing authority should be considered independent where it is not exposed to the risk of being subject, directly or indirectly, to external directions or instructions, in particular from the executive, such as a Minister for Justice, in connection with the adoption of a decision. That independence should be considered to exist where, based on the appropriate statutory rules and an institutional framework, the competent</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>issuing authority is capable of exercising his or her responsibilities objectively and acts independently in the execution of his or her responsibilities which are inherent in the issuing of a European Production or Preservation Order, taking into account all incriminatory and exculpatory evidence and without being exposed to the risk that its decision-making power be subject to external directions or instructions.</i>		
Recital 31				
56	(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	(31) For the same reason, a distinction has to be made regarding the material scope of this Regulation: Orders to produce subscriber data and IP addresses for the sole purpose of identifying the person can be issued for any criminal offence, whereas access to traffic and content data should be subject to stricter requirements to reflect the more sensitive nature of such data. A threshold allows for a more proportionate approach, together with a number of other ex ante and ex post conditions and safeguards provided for in this Regulation to ensure respect for proportionality and the rights of the persons affected. At the same time, a threshold should not limit the effectiveness of the instrument and its use by practitioners. Allowing the issuing of Orders for investigations that carry at least a three-year maximum sentence limits the scope of the instrument to more serious crimes, without excessively affecting the possibilities of its use by practitioners. It excludes from the scope a significant	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 32				
57	(32) There are specific offences where evidence will typically be available exclusively in electronic form, which is particularly fleeting in nature. This is the case for cyber-related crimes, even those which might not be considered serious in and of themselves but which may cause extensive or considerable damage, in particular including cases of low individual impact but high volume and overall damage. For most cases where the offence has been committed by means of an information system, applying the same threshold as for other types of offences would predominantly lead to impunity. This justifies the application of the Regulation also for those offences where the penalty frame is less than 3 years of imprisonment. Additional terrorism-related offences as described in the Directive 2017/541/EU do not require the minimum maximum threshold of 3 years.	(32) There are specific offences where information will typically be available exclusively in electronic form, which is particularly fleeting in nature. This is the case for cyber-related crimes, even those which might not be considered serious in and of themselves but which may cause extensive or considerable damage, in particular including cases of low individual impact but high volume and overall damage. For most cases where the offence has been committed by means of an information system, applying the same threshold as for other types of offences would predominantly lead to impunity. This justifies the application of the Regulation also for those offences where the penalty frame is less than 3 years of imprisonment. Additional terrorism-related offences as described in Directive 2017/541/EU of the European Parliament and of the Council¹⁷ as well as offences concerning the sexual abuse and sexual exploitation of children as described in Directive 2011/93/EU of the European Parliament and of the Council¹⁸ do not require the minimum maximum threshold of 3 years. -----	(32) There are specific offences where evidence will typically be available exclusively in electronic form, which is particularly fleeting in nature. This is the case for cyber-related crimes, even those which might not be considered serious in and of themselves but which may cause extensive or considerable damage, in particular including cases of low individual impact but high volume and overall damage. For most cases where the offence has been committed by means of an information system, applying the same threshold as for other types of offences would predominantly lead to impunity. This justifies the application of the Regulation also for those offences where the penalty frame is less than 3 years of imprisonment. Additional terrorism-related offences as described in the Directive 2017/541/EU do not require the minimum maximum threshold of 3 years.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p>¹⁷ 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 (OJL 88, 31.3.2017, p. 6).</p> <p>¹⁸ 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 (OJL 335, 17.12.2011, p.1).</p>		
Recital 33				
58	(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.	(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.	(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.	
Recital 33a				
59			(33a) In cases where an Order is issued to obtain different data categories the issuing authority has to ensure that the conditions and procedures, such as notification of the enforcing State, are met for all of the respective data categories.	
Recital 34				

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
60	<p>(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.</p>	<p>(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.</p>	<p>(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.</p>	
	Recital 34a			
61			(34a) In case data are stored or processed as part of an infrastructure	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			provided by a service provider to a public authority only authorities of the same Member State should be able to issue a European Production or Preservation Order because such data can be considered particularly sensitive. Public authority should be understood as any authority that, by its applicable national law has a mandate to govern, administrate a part or aspect of public life, such as branches of the judiciary, the legislative or executive power of a state, province, municipality.	
Recital 35				
62	(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	(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege, <i>source confidentiality</i>) or <i>rules relating to freedom of the press and freedom of expression in other media</i> , are referred to in other mutual recognition instruments such as the European Investigation Order. <i>There is no common definition of what constitutes an immunity or privilege in Union law. The precise definition of those terms is, therefore, left to national law. This may include protections which apply to medical (such as doctors) and legal professions, clergy or otherwise protected counsellors but also, even though they are not necessarily considered to be forms of privilege or immunity, rules relating to freedom of the press and freedom of expression in other media (such as journalists). Thus, the</i>	(35) Immunities and privileges, which may refer to categories of persons (such as diplomats) or specifically protected relationships (such as lawyer-client privilege or the right of journalists not to disclose their sources of information), are referred to in other mutual recognition instruments such as the European Investigation Order. Their range and impact differ according to the applicable national law that should be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order if a similar order would be available in a comparable domestic situation. In addition to this basic principle, Whether a second legal framework needs to be taken into account should depend on the strength of the connection of the person whose data is sought to the issuing State. Where the person is residing on the territory of the issuing State, a strong	

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p>applicable national law should <i>already</i> be taken into account at the time of issuing the Order, as the issuing authority may only issue the Order <i>where it could have been ordered under the same conditions</i> in a <i>similar</i> domestic case. In addition to this basic principle, immunities and privileges which protect data in the <i>executing</i> State should be taken into account as far as possible in the issuing State in the same way as if they were provided for under the national law of the issuing State. This is relevant in particular should the law of the <i>executing</i> State provide for a higher protection than the law of the issuing State. As an additional safeguard, these aspects should be taken into account not only when the Order is issued, but also later, <i>during the notification procedure or</i> 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 <i>executing</i> authority.</p>	<p>link to the issuing State exists. The applicable legal framework to assess immunities and privileges should therefore be that of the issuing State alone. The same principle applies for rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, and fundamental interests of the enforcing State. By the time a request for content or transactional data is made, authorities will regularly have an indication of where the person resides on the basis of previous investigatory steps. Moreover, statistics show that in a large majority of cases, the person resides in the issuing State. Where that is not the case, for example because the person whose data is sought has taken steps to conceal his or her location, the same principle should be applied.</p>	
Recital 35a				
63			<p>(35a) Immunities and privileges as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, which protect access, transactional or content data in the enforcing Member State of the service provider should therefore be taken into account as far as possible in the issuing State where the issuing authority has reasonable grounds to believe the person whose data is</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>sought is not residing on its territory. in the same way as if they were provided for under the national law of the issuing State. This is relevant in particular should the law of that 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.</p>	
Recital 35b				
64			<p>(35b) Where the issuing authority seeks to obtain transactional data and has reasonable grounds to believe that the person whose data are sought is not residing on its territory and that the data requested is protected by immunities and privileges granted under the law of the enforcing State, or by rules of that Member State on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, or its disclosure may impact fundamental interests of that Member State such as national security and defence, the issuing</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			authority should seek clarification, including through appropriate consultation.	
Recital 35c				
65			<p>(35c) In cases where the European Production Order concerns content data and where the issuing authority has reasonable grounds to believe the person whose data are sought is not residing on its territory, the enforcing State is notified and can as soon as possible, preferably within 10 days, inform the issuing authority of issues that might lead to a withdrawal or adaptation of the Order, such as privileges or immunities of the person whose data are sought or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media. As opposed to non-content data, content data is of particularly sensitive nature because persons may reveal their thoughts as well as sensitive details of their private life. This justifies a different treatment and an involvement of the authorities of the enforcing State early on in the procedure. In such cases, the issuing Member State should provide a copy of the Certificate to the enforcing State at the same time as the Certificate is provided to the service provider. In the interest of allowing for a swift check, the issuing authority should choose one of the languages accepted by the enforcing State if a translation of the Certificate is needed, even where the</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>service provider indicated that it would also accept Certificates in another language than one of the official languages of the enforcing State. Where the notified authority raises issues, it should provide the issuing authority with any relevant information regarding the immunities or privileges as well as the rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media granted to the person under its law or information, or if the Order impacts fundamental interests of that Member State such as national security and defence.</p>	
Recital 35d				
66			<p>(35d) In cases where the person, at the time of issuing the European Production Order, has more than one residency, of which one is on the territory of the issuing State, or in cases where the residency of the person cannot be determined with reasonable and proportionate efforts, the above procedures do not apply. However, a short visit, a holiday or a similar stay in the issuing State without any further substantial link is not enough to establish a residence in that Member State.</p>	
Recital 35e				
67			<p>(35e) In order to provide for a swift procedure, the relevant point in time to</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>determine whether there is a need to notify the authorities of the enforcing State should be the time when the Order is issued or validated. Any subsequent change of residency should not have any impact on the procedure. Where the issuing authority did not have reasonable grounds to believe the person whose data are sought is not residing on its territory at the time of issuing or validating the Order, and it later emerges that this person was in fact not residing on the territory of the issuing Member State no later check or notification should be required. However, the person concerned can invoke his or her rights as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media during the whole criminal proceeding, and the other Member State could also raise its fundamental interests such as national security and defence at any time during the criminal proceedings. In addition, these grounds could also be invoked during the enforcement procedure.</p>	
Recital 35f				
68			<p>(35f) Where data is protected by privileges or immunities or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media granted under the law of the enforcing State, or disclosure of data might impact</p>	

Commission Proposal	EP mandate	Council Mandate	Draft agreement
		<p>fundamental interests of that Member State, the issuing State should ensure that these grounds are taken into account in the same way as if they were provided for under its own national law, in order to give effect to them. If, for example, such privileges or immunities are not granted under the law of the issuing Member State, the protection should, to the extent possible, be adapted to the closest equivalent privilege or immunity under the law of the issuing State, taking into account the aims and the interests pursued by the specific protection and the effects attached to it. The legal consequences in its own national law for such similar situations should be applied. For the purposes of determining how to take these grounds into account in the same way as if they were provided for under its national law, the issuing authority may contact the notified authority for further information on the nature and the effects of the protection, either directly or via the European Judicial Network in criminal matters or Eurojust. While the enforcing State may raise any and all objections based on these grounds, the person whose data is sought can only rely on his or her own rights, such as privileges or immunities, and cannot raise objections based on a fundamental interest of the enforcing State.</p>	
Recital 35g			

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
69			(35g) Where a privilege or immunity prohibits the use of the data but these rights could be lifted and where the issuing authority intends to use the data obtained as evidence or does not withdraw the Order in case the data was not obtained, yet, the issuing Member State should have the possibility to request the competent authority to apply for lifting the privilege or immunity.	
Recital 36				
70	(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.	(36) The European Preservation Order may be issued for any <i>criminal</i> offence, <i>where it could have been ordered under the same conditions in a similar domestic case in the issuing State, where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border preservation of the data and where the requested information is relevant for that investigation. It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in this Regulation and the direct link between the person whose data are sought and the purpose of the specific processing must be demonstrable at all times. The aim of European Preservation Orders</i> 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.	(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.	
Recital 36a				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
71			(36a) In order to ensure full protection of fundamental rights, any validation of European Production or Preservation Orders by judicial authorities should in principle be obtained before the order is issued. Exceptions to this principle can only be made in exceptional cases when seeking subscriber and access data where the issuing authority validly establishes an emergency case and where it is not possible to obtain the prior validation by the judicial authority in time, in particular because the validating authority cannot be reached to obtain validation and the threat is so imminent that immediate action has to be taken. However, this only applies where this procedure is provided for in a similar domestic case under national law.	
Recital 37				
72	(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	(37) European Production and Preservation Orders should be addressed to the <i>main establishment of the service provider where the data controller is, or, where not established in the Union or one of the Member States bound by this Regulation, to its</i> legal representative designated by the service provider. <i>Simultaneously, it should be addressed directly to the executing authority.</i>	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>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.</p>		<p>non-compliance by the legal representative in non-emergency situations, but where there are clear risks of loss of data, a European Production or Preservation Order may also be addressed to any establishment of the service provider in the Union. Because of these various possible scenarios, the general term ‘addressee’ is used in the provisions. Where an obligation, such as on confidentiality, applies not only to the addressee, but also to the service provider if it is not the addressee, this is specified in the respective provision. In cases where the European Production or Preservation Order is addressed to the service provider following non-compliance by the legal representative, it can also be enforced against the service provider.</p>	
Recital 38				
73	<p>(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</p>	<p>(38) The European Production and European Preservation Orders should be transmitted through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). The Certificates should contain the same mandatory information as the Orders. Where necessary, a Certificate <i>should</i> be translated into (one of) the official language(s) of the <i>executing State and the service provider</i>, or into another official language that the <i>Member State or the service provider have declared they will accept. In this regard, Member States should be allowed, at any time, to state in a declaration submitted to the</i></p>	<p>(38) The European Production and European Preservation Orders should be transmitted to the service provider addressee through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR), which should be translated. The Certificates should contain the same mandatory information as the Orders, except for the grounds for the necessity and proportionality of the measure or further details about the case to avoid jeopardising the investigations. But as they are part of the Order itself, they allow the suspect to challenge it later during the criminal proceedings. Where necessary, a</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	<i>Commission that they would accept translations of EPOCs and EPOC-PRs in one or more official languages of the Union other than the official language or languages of that Member State. The Commission should make the declarations available to all Member States and to the European Judicial Network in criminal matters.</i>	Certificate needs to be translated into (one of) the official language(s) of the Member State of the addressee enforcing State , or into another official language that the service provider has declared it will accept.	
Recital 39				
74	(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.	<i>(39) The competent issuing authority should transmit the EPOC or the EPOC-PR directly to the addressees, via a common European digital exchange system established by the Commission by [date of application of this Regulation]. This system should allow for secure channels for the handling of authorised cross-border communication, authentication and transmission of the Orders and of the requested data between the competent authorities and service providers, by guaranteeing an effective, reliable and smooth exchange of the relevant information and a high level of security, confidentiality and integrity as well as the necessary protection of privacy and personal data in line with Regulation (EU) 2018/1725 of the European Parliament and of the Council¹⁹, Regulation (EU) 2016/679, Directive (EU) 2016/680, and Directive 2002/58/EC. To this end, open and commonly used state-of-the-art electronic signature and encryption technology should be applied. The system should also allow the</i>	(39) The competent issuing authority or the authority competent for transmission should transmit the EPOC or the EPOC-PR directly to the addressee in a secure and reliable way by any means capable of producing a written record under conditions that allow the service provider to establish authenticity, such as by registered mail, secured email and platforms or other secured channels, including those made available by the service provider, in line with the rules protecting personal data.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>addressees to produce a written record under conditions that allow the addressees to establish authenticity of the Order and of the issuing authority, in line with the rules protecting personal data.</i></p> <p>-----</p> <p><i>¹⁹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).</i></p>		
Recital 39a				
75		<p><i>(39a) Where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, it should be possible to interconnect such systems or channels with this common European digital exchange system.</i></p>		
Recital 40				
76	<p>(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</p>	<p><i>(40) Upon receipt of an EPOC for subscriber data or IP addresses for the sole purpose of identifying a person, the service provider should ensure that the requested data is transmitted to the issuing authority at the latest within 10 days upon</i></p>	<p>(40) The requested data should be transmitted to the authorities in a secure and reliable way that allows to establish the authenticity of the sender and integrity of the data at the latest within 10 days upon receipt of the EPOC. Shorter</p>	

		Commission Proposal	EP mandate	Council Mandate	Draft agreement
		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.	receipt of the EPOC <i>and within 16 hours in emergency cases. Where the executing authority decides to invoke any of the grounds listed for non-recognition or non-execution provided for in this Regulation within the time periods, it should immediately inform the issuing authority and the service provider of its decision. The issuing authority should erase the data. Where the requested data has not yet been transmitted to the issuing authority, the addressed service provider may not transmit the data.</i>	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.	
Recital 40a					
77			<i>(40a) Upon receipt of an EPOC for traffic or content data, the service provider should act expeditiously to preserve the requested data. Where the executing authority has invoked any of the grounds listed for non-recognition or non-execution provided for in this Regulation within the time periods, it should immediately inform the issuing authority and the service provider of its decision. Where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) TEU, the service provider should transmit the requested data only after receiving the explicit written approval of the executing authority. Without prejudice to this special provision, where the executing authority has not invoked any of the grounds listed in this Regulation within the time periods, the service provider should ensure that the requested data is immediately transmitted directly to</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>the issuing authority or the law enforcement authorities as indicated in the EPOC.</i>		
Recital 41				
78	(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.	(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.	(41) In order to allow service providers to address formal problems, it is necessary to set out a procedure for the communication between the service provider and the issuing judicial authority in cases where the EPOC might be incomplete or contains manifest errors or not enough information to execute the Order. Moreover, should the service provider not provide the information in an exhaustive or timely manner for any other reason, for example because it thinks there is a conflict with an obligation under the law of a third country, or because it thinks the European Production Order has not been issued in accordance with the conditions set out by this Regulation, it should go back to the issuing authorities and provide the opportune justifications. The communication procedure thus should broadly allow for the correction or reconsideration of the EPOC European Production Order by the issuing authority at an early stage. To guarantee the availability of the data, the service provider should preserve the data if they can identify the data sought.	
Recital 41a				
79			(41a) The addressee should not be obliged to comply with the Order in case	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>of de facto impossibility which was not created by the addressee or, if different, the service provider at the time when the Order was received. De facto impossibility should be assumed if the person whose data were sought is not a customer of the service provider or cannot be identified as such even after a request for further information to the issuing authority, or if the data have been deleted lawfully before receiving the order.</p>	
Recital 42				
80	<p>(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.</p>	<p>(42) Upon receipt of a European Preservation Order Certificate ('EPOC-PR'), the service provider should <i>act expeditiously to preserve the</i> requested data for a maximum of 60 days. <i>The 60 day period is calculated to allow for the launch of an official request for production. It may only be extended by additional 30 days, where necessary to allow further assessment of the relevance of the data in the ongoing investigations in order to prevent that potentially relevant data is lost before the European Preservation Order ends. Where the issuing authority submits the subsequent European Production Order to the addressees within these time periods European Production Order has been the service provider should continue to preserve the data as long as necessary for the execution of the European Production Order.</i></p>	<p>(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.</p>	

Commission Proposal

EP mandate

Council Mandate

Draft agreement

Recital 42a

81

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

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>issuing authority should react expeditiously and within 5 days at the latest. In the absence of a reaction from the issuing authority, the order should be considered null and void. Where the relevant conditions are fulfilled, the issuing authority should set a new deadline or withdraw the order. To guarantee the availability of the data, the service provider should preserve the requested data during this procedure, where possible.</i></p>		
Recital 42b				
82		<p><i>(42b) Notwithstanding the principle of mutual trust, the executing authority should be able to refuse the recognition of execution of a European Production Order, where such refusal is based on the fact that the conditions for issuing a European Production Order as laid down in this Regulation are not fulfilled or based on further specific grounds as listed in this Regulation.</i></p>		
Recital 42c				
83		<p><i>(42c) The principle of ne bis in idem is a fundamental principle of law in the Union, as recognised by the Charter and developed by the case law of the Court of Justice of the European Union. Therefore, where the executing authority assesses the Order, it should refuse the execution of a European Production Order if its execution would be contrary to that principle.</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 42d				
84		<i>(42d) Furthermore, where the executing authority assesses the Order and there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter, the executing authority should refuse the execution of a European Production Order.</i>		
Recital 42e				
85		<i>(42e) In addition, where the recognition or execution of a European Production Order would involve the breach of an immunity or privilege in the executing State, the executing authority should refuse that order in cases where it is assessed by the executing authority.</i>		
Recital 42f				
86		<i>(42f) Due to the more intrusive character of European Production Orders for traffic and content data, the executing authority should have additional optional grounds for non-recognition and non-execution at their disposal for these data categories.</i>		
Recital 43				
87	(43) Service providers and their legal representatives should ensure confidentiality and when requested by the	<i>(43) Since informing the person whose data is sought is an essential element as regards data protection rights and defence</i>	(43) Service providers and their legal representatives should ensure confidentiality. Furthermore they should	

Commission Proposal	EP mandate	Council Mandate	Draft agreement
<p>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) 2016/679¹³. 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) 2016/680¹⁴.</p> <p>-----</p> <p>¹³ 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).</p> <p>¹⁴ 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).</p>	<p><i>rights, in enabling effective review and judicial redress, in accordance with Article 6 TEU and the Charter, the service provider should inform the person whose data is being sought without undue delay. When informing the person, the service provider should take the necessary state-of-the-art operational and technical measures to ensure the security, confidentiality and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.</i></p>	<p>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) 2016/679¹³. However except where requested by the issuing authority to inform the person. In these cases, the issuing authority should also provide the necessary information about the applicable legal remedies to the service provider, so that it can be included in the information to the person. In any case, user information is an essential element in enabling review and judicial redress and should be provided by the authority if the service provider was not asked not to inform the user, where as soon as there is no risk of jeopardising ongoing investigations, in accordance with the national measure implementing Article 13 of Directive (EU) 2016/680¹⁴. The issuing authority may abstain from informing the person whose subscriber or access data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought. This could be the case where an Order concerns subscriber or access data of a third person, in light of the presumption of innocence of the suspect. Where the identity of the person concerned is unknown to the issuing authority, investigations to determine the identity of this person should only be</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>carried out insofar as it seems necessary and proportionate in relation to the invasiveness of the measure and the respective effort associated with establishing their identity.</p> <hr/> <p>¹³ 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).</p> <p>¹⁴ 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).</p>	
Recital 43a				
88		<i>(43a) As long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings or in order to protect the fundamental rights of another person, the issuing authority, taking due account of the impact of the</i>		

Commission Proposal	EP mandate	Council Mandate	Draft agreement
		<p><i>measure on the fundamental rights of the person whose data is sought, may request the service provider to refrain from informing the person whose data is being sought, based on a judicial order, which should be duly justified, specify the duration of the obligation of confidentiality and be subject to periodic review. Where the issuing authority requests the service provider to refrain from informing the person, the issuing authority should inform the person whose data is being sought without undue delay about the data production or preservation. That information could be delayed as long as necessary and proportionate, taking into account the rights of the suspected and accused person and without prejudice to defence rights and effective legal remedies. User information should include information about any available remedies as referred to in this Regulation.</i></p>	
Recital 43b			
89		<p><i>(43b) Electronic information obtained in accordance with this Regulation should not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except for where there is an imminent threat to the life or physical integrity of a person. Where the disruption or destruction of a critical infrastructure would directly imply an imminent risk to the life or physical integrity of a person, such a situation should also be treated as an imminent</i></p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>threat to the life or physical integrity of a person, in accordance with EU law.</i>		
Recital 43c				
90		<i>(43c) Electronic information that has been gathered in breach of any of the conditions listed in this Regulation should be erased without undue delay. Electronic information that is no longer necessary for the investigation or prosecution for which it was produced or preserved, including possible appeals, should also immediately be erased, unless this would affect the defence rights of the suspected or accused person. For this purpose, periodic reviews for the need of the storage of the electronic information should be established. The person whose data was sought should be informed about the erasure.</i>		
Recital 43d				
91		<i>(43d) Electronic information that has been gathered in breach of this Regulation should not be admissible before a court. This should also include all cases where the criteria laid down in this Regulation are not fulfilled. Where electronic information has been obtained before a ground for non-recognition listed in this Regulation has been invoked, it neither should be admissible before a court. When assessing the admissibility of electronic information, obtained in accordance with this Regulation, the competent judicial authorities should at</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>any stage of the proceedings ensure that the rights of the defence and the fairness of the proceedings are respected. For such an assessment, the competent judicial authorities should also take into due account whether the criteria laid down in this Regulation were fulfilled, in particular where the data sought might be protected by immunities or privileges.</i></p>		
Recital 43e				
92		<p><i>(43e) Where claimed by the service provider, the issuing State should reimburse the justified costs borne by the service provider and related to the execution of the European Production Order or the European Preservation Order. To this end, Member States should inform the Commission on the rules for reimbursement, which the Commission should make public. Where for practical reasons, such as the economic size of the service provider, different language regimes between the issuing State and the executing State or different national rules for the reimbursement of costs between these States, the service provider is substantially hampered from claiming the reimbursement of costs related to the execution of a European Production Order or European Investigation order from the issuing State, the service provider should be entitled to claim reimbursement of the costs from the executing State. Where the service provider chooses the executing State, the</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>issuing State should reimburse the executing State for these costs.</i>		
Recital 43f				
93		<i>(43f) Member States should lay down the rules on sanctions applicable to infringements of the obligations pursuant to this Regulation. These sanctions should be effective, proportionate and dissuasive. When determining the appropriate sanction applicable to infringements of service providers, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence and whether the service provider was held responsible for similar previous breaches. Particular attention should, in this respect, be given to micro enterprises.</i>		
Recital 43g				
94		<i>(43g) Where a service provider acts with due diligence, in particular with regards to data protection obligations, and requested clarification or justification from the issuing authority, in accordance with this Regulation, it should not be held liable for the consequences of any delays caused. In addition, sanctions applied to infringements of the obligations of service provider pursuant to this Regulation should be annulled, where an order has been successfully challenged in accordance with this Regulation.</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 44				
95	(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.	(44) <i>Where the service provider does not comply with an EPOC within the deadlines or with an EPOC-PR, without providing sufficient reasons, and where, as regards the EPOC, the executing authority has not invoked any of the grounds as provided for in this Regulation, the issuing authority may request the competent authority in the executing State to enforce the Order. In such a case, the executing State should formally require the service provider to comply with the Order, informing the service provider of the possibility to oppose the execution by invoking one of the grounds which the service provider has at its disposal for correction or reconsideration of the order, in accordance with this Regulation. Where a service provider still does not comply with its obligations, Member States should impose a sanction in accordance with this Regulation.</i>	(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.	
Recital 45				
96	(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	(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	(45) The enforcement procedure is a procedure where the addressee can oppose invoke formal grounds against the enforcement based on certain restricted grounds. The enforcing authority can refuse to recognize and enforce the Order based on the same grounds, or and additionally, in case they have to be taken into account under this Regulation, if immunities and privileges	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p>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.</p>	<p>as well as rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media under its national law apply or the disclosure may impact its fundamental interests such as national security and defense. 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.</p>	
Recital 45a				
97			<p>(45a) When determining in the individual case the appropriate pecuniary sanction, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence, whether the service provider was held responsible for similar previous breaches and the financial strength of the service provider held liable. In exceptional circumstances, that assessment may lead the enforcing authority to decide to abstain from imposing any pecuniary sanctions. Particular attention should, in this respect, be given to micro enterprises that fail to comply with an Order in an emergency case due to lack of personal</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			resources outside normal business hours, if the data is transmitted without undue delay.	
Recital 46				
98	(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.	(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.	(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. The responsibility to ensure the legality of the Order, in particular its necessity and proportionality, should lie with the issuing authority.	
Recital 47				
99	(47) In addition to the individuals whose data is requested, the service providers and third countries may be affected by the investigative measure. To ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned and to address conflicting obligations on service providers, this instrument provides a specific mechanism for judicial review where compliance with a European Production Order would prevent service providers from complying with legal obligation deriving from a third State's law.	(47) In addition to the individuals whose data is <i>sought</i> , the <i>laws of a third country</i> may be affected by the investigative measure. <i>In such situations, judicial cooperation based on international agreements would generally be the most appropriate way to request electronic information when conflicts of law with a third country arise. Without prejudice to such international agreements and in order</i> 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 review where <i>the service provider or the executing authority consider that</i> compliance with a European Production Order <i>or a European</i>	(47) In addition to the individuals whose data is requested, the service providers and third countries may be affected by the investigative measure. To ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned and to address conflicting obligations on service providers, this instrument provides a specific mechanism for judicial review where compliance with a European Production Order would prevent service providers from complying with legal obligation deriving from a third State's law.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>Preservation Order would conflict with applicable laws of third country prohibiting disclosure of the data concerned.</i>		
Recital 48				
100	(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.	(48) To this end, whenever the <i>service provider or the executing authority</i> consider that the European Production Order <i>or the European Preservation Order</i> 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 <i>and the relevant addressees, without undue delay at the latest within 10 days from the receipt of the order, thereby suspending the execution of the Order. Such notice should include all relevant details on the law of the third country, its applicability in the case at hand and the nature of the conflicting obligation.</i> The issuing authority should then review the European Production Order <i>or European Preservation Order, within 10 days of receiving the notice</i> , taking into account criteria <i>including the interests protected by the relevant law, the connection of the criminal case and the third country, the connection between the service provider and the third country, the interests of the issuing State in obtaining the electronic information and the possible consequences for the addressees of complying with the European Production Order or the European Preservation Order. During this procedure, the</i>	(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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>requested data should be preserved where possible.</i>		
Recital 48a				
101		<i>(48a) The issuing authority should be able to withdraw, uphold or adapt the Order where necessary, to give effect to the relevant criteria. In the event of withdrawal, the issuing authority should immediately inform the addressees of the withdrawal. Where the issuing authority decides to uphold the Order, it should inform the addressees of its decision. The executing authority, while duly taking into account the decision of the issuing authority should take a final decision based on the criteria listed in this Regulation, within 10 days of receiving the decision of the issuing authority, and inform the issuing authority and the service provider of its final decision.</i>		
Recital 49				
102	(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.	(49) In determining the existence of a conflicting obligation in the specific circumstances of the case under examination, the issuing authority and the executing authority should seek information from the competent authority of the third country , for example if the review raises questions on the interpretation of the law of the third country concerned, in compliance with Directive (EU) 2016/680 and to the extent that this does not obstruct the deadlines provided for in this Regulation.	(49) In determining the existence of a conflicting obligation in the specific circumstances of the case under examination, the competent court should may rely on appropriate external expertise where needed, for example if the review raises questions on the interpretation of the law of the third country concerned. This could include consulting the central authorities of that country.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Recital 50				
103	(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 platforms 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.	(50) Expertise on interpretation could also be provided through expert opinions where available. Information and case law on the interpretation of <i>the laws of a third country</i> and on conflict procedures in Member States should be made available on a central platforms such as the SIRIUS project and/or the European Judicial Network, <i>with a view to benefitting</i> from experience and expertise gathered on the same or similar questions. It should not prevent a renewed consultation of the third state where appropriate.	(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 platforms 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.	
Recital 51				
104	(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	(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	(51) Where conflicting obligations exist, the court should determine whether the conflicting provisions of the third country law applies and if so, whether they prohibit disclosure of the data concerned. on the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country related to national security or defence. In carrying out this assessment, the court should take into account whether the third country law, rather than being intended to protect fundamental rights or fundamental interests of the third country related to national security or defence, manifestly seeks to protect other interests or is being aimed to shield illegal activities from law enforcement requests in the context of criminal investigations. Where the court	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p>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.</p>	<p>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.</p>	
Recital 52				
105	<p>(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</p>	<p>(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</p>	<p>(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</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	Order. Importantly for cyber-related offences, the place where the crime was committed covers both the place(s) where the action was taken and the place(s) where the effects of the offence materialised. Particular importance and weight should be given to the protection of fundamental rights by the third country's provisions and other fundamental interests, such as national security interests of the third country as well as the degree of connection of the criminal case to either of the two jurisdictions when conducting the assessment.	
Recital 53				
106	(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.	(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.	(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.	
Recital 54				
107	(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	(54) In line with Article 47 of the Charter of Fundamental Rights of the European Union, it is essential that all persons whose data was sought via a European Production Order or a European Preservation Order have the right to effective remedies against such Orders in the issuing and executing State in	(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 cs should be exercised	

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p><i>accordance with national law, including the possibility to challenge the legality of the Order, including its necessity and proportionality, without prejudice to remedies available under Regulation (EU) 2016/679 and Directive (EU) 2016/680. The substantive reasons for issuing the European Production Order or the European Preservation Order should be challenged in the issuing State, without prejudice to the guarantees of fundamental rights in the executing State. The issuing authority and the executing authority should take the appropriate measures to ensure that information about the options for seeking legal remedies under national law is provided in due time, including about when such remedies become applicable, and ensure that they can be exercised effectively.</i></p>	<p>during the whenever data obtained is used in criminal proceedings against them. This may affect the admissibility, or as the case may be, the weight in the proceedings, of the evidence obtained by such means. In addition, they benefit from all procedural guarantees applicable to them, such as the right to information. Other persons, whose data were sought but who are not suspects or accused persons, should also have a right to an effective remedy. Therefore, as a minimum, the possibility to challenge the legality of a European Production Order, including the necessity and the proportionality of the Order, should be provided. This Regulation should not limit the possible grounds to challenge the legality of the Order. These remedies should be exercised in the issuing State in accordance with national law. Rules on interim relief should be governed by national law.</p>	
Recital 55				
108	<p>(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</p>	<p>(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</p>	<p>(55) In addition, During the enforcement procedure the enforcing authority may refuse the recognition and enforcement of a European Production or Preservation Order on a number of limited grounds, and subsequent legal remedy the addressee may oppose the enforcement of a European Production or Preservation Order on a number of limited grounds, including it not being issued or validated by a competent authority or it being apparent that it manifestly violates</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 56				
109	(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.	(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.	(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.	
Recital 56a				
110			(56a) Transmission and transfer as well as making use of electronic evidence obtained through a European Production Order in other proceedings and for another purpose as for the one for which the Order was issued should be restricted, in particular to criminal offences for which the issuing authority could have also issued a European Production Order. The use, transmission	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>or transfer of electronic evidence should, in addition only be possible where the data are needed to prevent an immediate and serious threat to public security of the respective Member State or third country as well as their essential interests. International transfer of electronic evidence is furthermore subject to conditions as set out in Chapter V of Directive (EU) 2016/680. In cases, where the obtained personal data is used for the prevention of an immediate and serious threat to public security of the respective Member State or third country as well as their essential interests, and such threat may not lead to criminal investigations Regulation (EU) 2016/679 should apply.</p>	
Recital 56b				
111			<p>(56b) When making a declaration concerning the language regime, Member States are encouraged to include at least one additional language to their official language(s).</p>	
Recital 57				
112	<p>(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</p>	<p>(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</p>	<p>(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</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 57a				
113		<i>(57a) In order to monitor the outputs, results and impacts of this Regulation, the Commission should publish an annual report on the preceding calendar year, based on data obtained from the Member States. For this purpose, Member States should collect and maintain comprehensive statistics from the relevant authorities on different aspects of this Regulation, by type of data requested, the addressees (executive authority addressed), the type of service provider addressed [electronic communications service, information society service or</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>internet domain name and IP number service (such as IP address providers, domain name registries, domain name registrars or related proxy services)] and whether it was an emergency case or not. Where applicable, the data collected should also include the grounds for non-recognition or non-execution raised, the legal remedies used, the sanctions imposed, the costs claimed by the service provider and the enforcement proceeding launched.</i>		
Recital 58				
114	(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.	(58) The Commission should carry out an evaluation of this Regulation that should be based on the five criteria of efficiency, effectiveness, relevance, coherence and EU added value, should provide the basis for impact assessments of possible further measures and include an evaluation of the use of derogations (emergency derogation, derogation from the principle of user information) as well as an assessment of the functioning of the common European exchange system and of the functioning of the Regulation in relation with Directive 2014/41/EU. Information should be collected regularly and in order to inform the evaluation of this Regulation.	(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.	
Recital 59				
115	(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information between	(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information between	(59) The use of pretranslated and stardardised forms facilitates cooperation and the exchange of information between	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	<i>different</i> judicial authorities <i>as well as with</i> service providers, allowing <i>for a quicker and more effective transmission of electronic information</i> in a user-friendly manner. They <i>could also</i> reduce translation costs and contribute to a high quality standard. Response forms similarly should allow for a standardised exchange of information. The forms should also facilitate the gathering of statistics.	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.	
Recital 60				
116	(60) In order to effectively address a possible need for improvement regarding the content of the EPOCs and EPOC-PRs and of the Form to be used to provide information on the impossibility to execute the EPOC or EPOC-PR, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ¹⁵ . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council	(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-Making²⁴. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council	(60) In order to effectively address a possible need for improvement regarding the content of the EPOCs and EPOC-PRs and of the Form to be used to provide information on the impossibility to execute the EPOC or EPOC-PR, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III to this Regulation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ¹⁵ . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>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.</p> <p>_____</p> <p>¹⁵ OJ L 123, 12.5.2016, p. 1.</p>	<p>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.</p> <p>_____</p> <p>²⁰ OJ L 123, 12.5.2016, p. 1.</p>	<p>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.</p> <p>_____</p> <p>¹⁵ OJ L 123, 12.5.2016, p. 1.</p>	
Recital 61				
117	<p>(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 Council¹⁶ 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.</p> <p>_____</p> <p>¹⁶ Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p.1).</p>	<p>(61) The measures based on this Regulation should not supersede European Investigation Orders in accordance with Directive 2014/41/EU or Mutual Legal Assistance Procedures to obtain electronic information. Member States' authorities should choose the tool most adapted to their situation; they may prefer to use the European Investigation Order when requesting a set of different types of investigative measures including but not limited to the production of electronic information from another Member State.</p>	<p>(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 Council¹⁶ to obtain electronic evidence. Member States' authorities should choose the tool most adapted to their situation the case at hand; they may prefer to use the European Investigation Order when requesting a set of different types of investigative measures including but not limited to the production of electronic evidence from another Member State.</p> <p>_____</p> <p>¹⁶ Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p.1).</p>	
Recital 62				
118	<p>(62) Because of technological developments, new forms of</p>	<p>(62) Because of technological developments, new forms of</p>	<p>(62) Because of technological developments, new forms of</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Recital 63				
119	(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic evidence across borders, cannot be sufficiently achieved by the Member States given its cross-border nature, but can rather be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.	(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic information across borders, cannot be sufficiently achieved by the Member States given its cross-border nature, but can rather be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective .	(63) Since the objective of this Regulation, namely to improve securing and obtaining electronic evidence across borders, cannot be sufficiently achieved by the Member States given its cross-border nature, but can rather be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.	
Recital 64				
120	(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, <i>[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</i>	(64) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation and without prejudice to Article 4 of that Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.	(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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<i>adoption of this Regulation and is not bound by it or subject to its application.].</i>		Regulation and is not bound by it or subject to its application.	
Recital 65				
121	(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.			
Recital 66				
122	<p>(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 Council¹⁷ and delivered an opinion on (...) ¹⁸,</p> <p>-----</p> <p>¹⁷ 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).</p> <p>¹⁸ OJ C , , p. .</p>	<p>(66) The European Data Protection Supervisor was consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council²¹ and delivered an opinion on 6 November 2019²²,</p> <p>-----</p> <p>²¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).</p> <p>²² EDPS Opinion 7/2019 on Proposals regarding European Production and</p>	<p>(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 Council¹⁷ and delivered an opinion on (...) ¹⁸,</p> <p>-----</p> <p>¹⁷ 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).</p> <p>¹⁸ OJ C , , p. .</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>Preservation Orders for electronic evidence in criminal matters (6 November 2019).</i>		
Formula				
123	HAVE ADOPTED THIS REGULATION:			
Chapter I				
124	Chapter 1: Subject matter, definitions and scope			
Article 1				
125	<i>Article 1</i> <i>Subject matter</i>			
Article 1(1)				
126	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.	1. This Regulation lays down the rules under which an authority of a Member State, <i>in a criminal proceeding</i> , may order a service provider offering services in the Union <i>and established or, if not established, legally represented in another Member State</i> to produce or preserve electronic <i>information that may serve as evidence</i> , regardless of the location of data. <i>Authorities of the Member States shall not issue domestic orders with extraterritorial effects for the production or preservation of electronic information that could be requested on the basis of this Regulation.</i>	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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 1a				
127		<i>1a. The issuing of a European Production or Preservation Order may also be requested on behalf of a suspected or accused person, within the framework of applicable defence rights in accordance with national criminal procedures.</i>		
Article 1(2)				
128	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.	2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined <i>in the Charter and</i> in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement, judicial authorities <i>or service providers</i> in this respect shall remain unaffected.	2. This Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities in this respect shall remain unaffected.	
Article 2				
129	<i>Article 2</i> <i>Definitions</i>			
Article 2, introductory paragraph				
130	For the purpose of this Regulation, the following definitions shall apply:			
Article 2(1)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
131	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;	1. 'European Production Order' means a decision <i>which has been issued or validated</i> by a <i>judicial</i> authority of a Member State (<i>'the issuing State'</i>) <i>addressed to</i> a service provider offering services in the Union and established or <i>legally</i> represented in another Member State <i>bound by this Regulation ('the executing State')</i> , to produce electronic <i>information</i> ;	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;	
Article 2(2)				
132	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;	2. 'European Preservation Order' means a decision <i>which has been issued or validated</i> by a <i>judicial</i> authority of a Member State (<i>'the issuing State'</i>) <i>addressed to</i> a service provider offering services in the Union and established or <i>legally</i> represented in another Member State <i>bound by this Regulation ('the executing State')</i> , to preserve electronic <i>information</i> in view of a subsequent request for production;	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;	
Article 2(3)				
133	3. 'service provider' means any natural or legal person that provides one or more of the following categories of services:	3. 'service provider' means any natural or legal person that provides one or more of the following categories of services <i>and, where it concerns personal data, acts as a data controller within the meaning of Regulation (EU) 2016/679:</i>	3. 'service provider' means any natural or legal person that provides one or more of the following categories of services, with the exception of financial services referred to in Article 2(2)(b) of Directive 2006/123/EC:	
Article 2(3), point a				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
134	a) electronic communications service as defined in Article 2(4) of [Directive establishing the European Electronic Communications Code];			
Article 2(3), point b				
135	<p>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 Council¹⁹ 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;</p> <p>¹⁹ 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).</p>	<p>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;</p> <p>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).</p>	<p>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;</p>	
Article 2(3), point c				
136	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;	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;	<p>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 Council¹⁹ that provide:</p> <p>- the ability to its users to communicate with each other; or</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>- 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;</p> <p>-----</p> <p>¹⁹ 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).</p>	
Article 2(4)				
137	4. 'offering services in the Union' means:			
Article 2(4), point a				
138	a) enabling legal or natural persons in one or more Member State(s) to use the services listed under (3) above; and	a) enabling legal or natural persons in one or more Member State(s) to use the services listed under <i>point (3)</i> above; and	a) enabling legal or natural persons in one or more Member State(s) to use the services listed under (3) above; and	
Article 2(4), point b				
139	b) having a substantial connection to the Member State(s) referred to in point (a);	b) having a substantial connection to the Member State(s) referred to in point (a); <i>such a substantial connection to the Union shall be considered to exist where the service provider has an establishment in the Union, or, in the absence of such</i>	b) having a substantial connection based on specific factual criteria to the Member State(s) referred to in point (a);	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>an establishment, based on the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States;</i>		
Article 2(5)				
140	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;	5. ‘ <i>main establishment</i> ’ means, <i>as regards a service provider with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of data are taken in another establishment of the service provider in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;</i>	5. ‘establishment’ or ‘ being established ’ means either the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or a stable infrastructure from where the business is managed;	
Article 2(6)				
141	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;	6. ‘electronic <i>information</i> ’ means <i>subscriber data, traffic data, or content data lawfully</i> stored by a service provider at the time of the <i>issuing</i> of a <i>European Production or Preservation order, that is requested for the purpose of serving as evidence during the investigation, prosecution and court proceedings relating to a criminal offence in a Member State, in accordance with national law</i> ;	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;	
Article 2(7)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
142	7. 'subscriber data' means any data pertaining to:	7. 'subscriber data' means any data, <i>collected in the normal course of business</i> , pertaining to <i>the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address identifying the subscriber or customer as well as the type of service provided and the duration of the contract with the service provider, which is strictly necessary for the sole purpose of identifying the user of the service;</i>	7. 'subscriber data' means any data pertaining to:	
Article 2(7), point a				
143	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;	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;	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;	
Article 2(7), point b				
144	b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;	b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;	b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user;	
Article 2(8)				
145	8. 'access data' means data related to the commencement and termination of a user	8. ' <i>traffic data</i> ' means data <i>collected in the normal course of business</i> related to: the	8. 'access data' means data related to the commencement and termination of a user	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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];	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];	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 (gc) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];	
Article 2(8), point a				
146		<i>(a) the type of service provided and its duration where it concerns technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of the service, excluding passwords or other authentication means used instead of a password that are provided by a user, or created at the request of a user;</i>		
Article 2(8), point b				
147		<i>(b) the commencement and termination of a user access session to a service, such as the date and time of use, or the log-in to, and log-off from the service;</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 2(8), point c				
148		<i>(c) electronic communications metadata as processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content, including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication;</i>		
Article 2(9)				
149	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];	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];	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 (gc) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 2(10)				
150	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;	10. 'content data' means <i>the</i> stored data in a digital format <i>by the service provider</i> such as text, voice, videos, images, and sound other than subscriber or <i>traffic</i> data;	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;	
Article 2(11)				
151	11. 'information system' means information systems as defined in point (a) of Article 2 of Directive 2013/40/EU of the European Parliament and of the Council ²⁰ ; ----- ²⁰ 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).			
Article 2(12)				
152	12. 'issuing State' means the Member State in which the European Production Order or the European Preservation Order is issued;			
Article 2(12a)				
153		<i>(12a) 'issuing authority' means the authority in the issuing State, competent in the case concerned, to issue the</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>European Production Order or European Preservation Order;</i>		
Article 2(13)				
154	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;	13. ‘ <i>executing</i> State’ means the Member State in which the <i>service provider</i> is established <i>or legally represented</i> 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 <i>notification and enforcement of the order in accordance with this Regulation;</i>	13. ‘enforcing State’ means the Member State in which the addressee of the European Production Order or the European Preservation Order resides or is established and to which, if necessary , the European Production Order and the European Production Order Certificate or the European Preservation Order and the European Preservation Order Certificate are transmitted for enforcement;	
Article 2(14)				
155	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;	14. ‘ <i>executing</i> authority’ means the competent authority in the <i>executing</i> 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 <i>for notification and enforcement of the order in accordance with this Regulation; where provided by national law, the executing authority may be a court authority in the executing State;</i>	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;	
Article 2(15)				
156	15. ‘emergency cases’ means situations where there is an imminent threat to life or physical integrity of a person or to a	15. ‘emergency cases’ means situations where there is an imminent threat to life or physical integrity of a person or to a critical	15. ‘emergency cases’ means situations where there is an imminent threat to life or physical integrity of a person or to a critical	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC ²¹ . ----- ²¹ 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).	infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC²⁵. ----- ²⁵ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 34523.12.2008. p 75).	infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC ²¹ . ----- ²¹ 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				
157	<i>Article 3</i> <i>Scope</i>			
Article 3(1)				
158	1. This Regulation applies to service providers which offer services in the Union.	1. This Regulation applies to Member States and service providers, offering services in one or more Member States bound by this Regulation and established or legally represented in one of these Member States.	1. This Regulation applies to service providers which offer services in the Union.	
Article 3(1a)				
159		1a. This Regulation shall not apply to proceedings initiated by the issuing authority for the purpose of providing mutual legal assistance to another Member State or a third country.	1a. The Regulation shall not apply to proceedings initiated by the issuing authority for the purpose of providing mutual legal assistance to another Member State or a third country.	
Article 3(2)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
160	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.	2. The European Production Orders and European <i>Preservation</i> Orders may only be issued in the framework and for the purposes of criminal proceedings, both during the pre-trial and trial phase. The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.	2. The European Production Orders and European Production Preservation Orders may only be issued for criminal proceedings, both during the pre-trial and trial phase and for the execution of custodial sentences or detention orders that were not rendered in absentia in case the convict absconded from justice. The Orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing State.	
Article 3(3)				
161	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 II				
162	Chapter 2: European Production Order, European Preservation Order and Certificates			
Article 4				
163	<i>Article 4</i> <i>Issuing authority</i>			
Article 4(1)				
164	1. A European Production Order for subscriber data and access data may be issued by:	1. A European Production Order for obtaining subscriber data and IP addresses for the sole purpose of determining the	1. A European Production Order for subscriber data and access data may be issued by:	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>identity of specific persons with a direct link to the specific proceedings referred to in Article 3(2)</i> may be issued by:		
Article 4(1), point a				
165	a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or	a) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or	a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or	
Article 4(1), point b				
166	b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.	b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.	b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.	
Article 4(2)				
167	2. A European Production Order for transactional and content data may be issued only by:	2. A European Production Order for traffic and content data may be issued only by:	2. A European Production Order for transactional and content data may be issued only by:	
Article 4(2), point a				
168	a) a judge, a court or an investigating judge competent in the case concerned; or			

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 4(2), point b				
169	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.			
Article 4(3)				
170	3. A European Preservation Order may be issued by:	3. A European Preservation Order <i>for all data categories</i> may be issued by:	3. A European Preservation Order may be issued by:	
Article 4(3), point a				
171	a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or	a) a judge, a court, an investigating judge or <i>a public</i> prosecutor competent in the case concerned; or	a) a judge, a court, an investigating judge or prosecutor competent in the case concerned; or	
Article 4(3), point b				
172	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a prosecutor in the issuing State.	issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a <i>public</i> prosecutor in the issuing State.	issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a prosecutor in the issuing State.	
Article 4(4)				
173	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 4(5)				
174			5. In validly established emergency cases, the authorities mentioned under paragraphs 1(b) and 3(b) may issue the respective Order for subscriber and access data, without prior validation if the validation cannot be obtained in time and if these authorities could issue the Order in a similar domestic case without validation. The issuing authority shall seek validation ex-post without undue delay, at the latest within 48 hours. Where such ex-post validation is not granted the issuing authority shall withdraw the Order immediately and shall, in accordance with its national law, either delete any data that was obtained or ensure that the data are not used as evidence.	
Article 4(6)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
175			6. Each Member State may designate one or more central authority responsible for the administrative transmission of Certificates, Orders and notifications, the receipt of data and notifications as well as transmission of other official correspondence relating to the Certificates or Orders.	
Article 5				
176	Article 5 Conditions for issuing a European Production Order			
Article 5(1)				
177	1. An issuing authority may only issue a European Production Order where the conditions set out in this Article are fulfilled.			
Article 5(2)				
178	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.	2. The European Production Order shall be necessary and proportionate for the purpose of the proceedings referred to in Article 3 (2), taking into account the rights of the person concerned. It may only be issued if it could have been ordered under the same conditions in a similar domestic case , where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border production of the data and where the	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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>requested information is relevant for the investigation. It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in Article 3(2).</i>		
Article 5(3)				
179	3. European Production Orders to produce subscriber data or access data may be issued for all criminal offences.	3. A European Production Order for obtaining subscriber data or IP addresses for the sole purpose of determining the identity of specific persons with a direct link to the specific proceedings referred to in Article 3(2) may be issued for all criminal offences.	3. European Production Orders to produce subscriber data or access data may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months.	
Article 5(4)				
180	4. European Production Orders to produce transactional data or content data may only be issued	4. A European Production Order to produce traffic data or content data may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years.	4. European Production Orders to produce transactional data or content data may only be issued	
Article 5(4), point a				
181	a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or	a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or	a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or	
Article 5(4), point b				
182	b) for the following offences, if they are wholly or partly committed by means of an information system:	b) for the following offences, if they are wholly or partly committed by means of an information system:	b) for the following offences, if they are wholly or partly committed by means of an information system:	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 5(4), point b, paragraph 1				
183	<p>- offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA ²²;</p> <p>-----</p> <p>²² 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).</p>	<p>- offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA ²⁶;</p> <p>-----</p> <p>²⁶ 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).</p>	<p>- offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA ²²;</p> <p>-----</p> <p>²² 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).</p>	
Article 5(4), point b, paragraph 2				
184	<p>- offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council ²³;</p> <p>-----</p> <p>²³ 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).</p>	<p>- offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council;</p> <p>- offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council ²⁷;</p> <p>-----</p> <p>²⁷ 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).</p>	<p>- offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council ²³;</p> <p>-----</p> <p>²³ 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).</p>	
Article 5(4), point b, paragraph 3				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
185	- offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;	- offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;	- offences as defined in Articles 3 to 8 of Directive 2013/40/EU, of the European Parliament and of the Council;	
Article 5(4), point c				
186	c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council ²⁴ . ----- ²⁴ 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).	e) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council²⁸. ----- ²⁸ 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) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council ²⁴ . ----- ²⁴ 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).	
Article 5(4), point d				
187			d) for the execution of a custodial sentence or a detention order of at least four months imposed for criminal offences pursuant to point (a), (b) and (c) of this paragraph;	
Article 5(4a)				
188		4a. European Production Orders to produce traffic data or content data may also be issued for the following offences:		
Article 5(4a), point a				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
189		<i>(a) for the following offences if they are wholly or partly committed by means of an information system,</i>		
Article 5(4a), point a, line 1				
190		<i>–offences as defined in Articles 3, 4 and 5 of the Council Framework Decision 2001/413/JHA;</i>		
Article 5(4a), point a, line 2				
191		<i>– offences as defined in Articles 3 to 8 of Directive 2013/40/EU;</i>		
Article 5(4a), point b				
192		<i>(b) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541;</i>		
Article 5(4a), point ba				
193		<i>(ba) for criminal offences as defined in Articles 3 to 7 of Directive 2011/93/EU;</i>		
Article 5(5)				
194	5. The European Production Order shall include the following information:	5. The European Production Order shall include the following information:	5. The European Production Order shall include the following information:	
Article 5(5), point a				
195	a) the issuing and, where applicable, the validating authority;	a) the issuing and, where applicable, the validating authority; for traffic and content data and where the issuing State is subject to a procedure referred to in	a) the issuing and, where applicable, the validating authority;	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>Article 7(1) or 7(2) of the Treaty on European Union, information on the special procedure as referred to in Article 9 (2a) of this Regulation;</i>		
Article 5(5), point b				
196	b) the addressee of the European Production Order as referred to in Article 7;			
Article 5(5), point c				
197	c) the persons whose data is being requested, except where the sole purpose of the order is to identify a person;	c) <i>the individually identifiable persons, or</i> where the sole purpose of the order is to identify a person, <i>any other unique identifier such as user name or Login ID;</i>	c) the user, except where the sole purpose of the order is to identify the user, or any other unique identifier such as user name, ID or account name to determine the data that are being sought, persons whose data is being requested except where the sole purpose of the order is to identify a person;	
Article 5(5), point d				
198	d) the requested data category (subscriber data, access data, transactional data or content data);	d) the requested data category (subscriber data, <i>traffic</i> data or content data);	d) the requested data category (subscriber data, access data, transactional data or content data);	
Article 5(5), point e				
199	e) if applicable, the time range requested to be produced;	e) the time range requested to be produced, <i>tailored as narrowly as possible;</i>	e) if applicable, the time range requested to be produced;	
Article 5(5), point f				
200	f) the applicable provisions of the criminal law of the issuing State;			

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 5(5), point g				
201	g) in case of emergency or request for earlier disclosure, the reasons for it;	g) in case of emergency, the <i>duly justified</i> reasons for it;	g) in case of emergency or request for earlier disclosure, the reasons for it;	
Article 5(5), point h				
202	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;	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;	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;	
Article 5(5), point i				
203	i) the grounds for the necessity and proportionality of the measure.	i) the grounds for the necessity and proportionality of the measure, <i>taking due account of the impact of the measure on the fundamental rights of the specific persons whose data is sought and the seriousness of the offence.</i>	i) the grounds for the necessity and proportionality of the measure.	
Article 5(6)				
204	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.	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.	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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 5(6a)				
205			6a. A European Production Order to produce data stored or processed as part of an infrastructure provided by a service provider to a public authority may only be issued if the public authority for which the data is stored or processed is in the issuing State.	
Article 5(7), paragraph 1				
206	<p>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.</p>	<p>7. If the issuing authority has reasons to believe that data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed <i>or under the law of the Member State where the person whose data is sought resides or is bound by an obligation of professional secrecy or lawyer-client privilege</i>, or its disclosure may impact fundamental interests of that Member State such as national security and defence, the issuing authority <i>shall</i> 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 <i>in criminal matters</i>. <i>Where</i> the issuing authority finds that the requested data is protected by such immunities and privileges or its disclosure would impact fundamental interests of the other Member State, <i>the issuing authority</i> shall not issue the European Production Order.</p>	<p>7. If In cases where the Order concerns transactional data and where the issuing authority has reasons reasonable grounds to believe that transactional or content</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 5(7), paragraph 1, point a				
207			a) the person whose data are sought is not residing on the territory of the issuing State, and	
Article 5(7), paragraph 1, point b				
208			b) the data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed enforcing State or it is subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media its disclosure may impact fundamental interests of the at Member-enforcing State such as national security and defence,	
Article 5(7), paragraph 2				
209			the issuing authority has to shall seek clarification on the circumstances referred to in point b) before issuing the European Production Order, including by consulting the competent authorities of the Member enforcing State concerned, either directly or via Eurojust or the European Judicial Network. If the issuing authority finds that the requested access, transactional or content data <i>is are</i> protected by such immunities and privileges or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media or its	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			disclosure would impact fundamental interests of the other Member State such as national security and defence, it shall take these circumstances into account in the same way as if they were provided for under its national law and it shall not issue or shall adapt the European Production Order where necessary to give effect to these grounds.	
Article 5(8)				
210			8. Where the power to waive the privilege or immunity lies with an authority of the enforcing State, the issuing authority may request the enforcing authority to contact the competent authority to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.	
Article 6				
211	<i>Article 6</i> <i>Conditions for issuing a European Preservation Order</i>			
Article 6(1)				
212	1. An issuing authority may only issue a European Preservation Order where the	1. An issuing authority may only issue a European Preservation Order where the	1. An issuing authority may only issue a European Preservation Order where the	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	conditions set out in this Article are fulfilled.	conditions set out in this Article are fulfilled.	conditions set out in this Article are fulfilled. Article 5 (6a) shall apply mutatis mutandis.	
Article 6(2)				
213	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.	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, <i>taking into account the rights of the person concerned.</i> European Preservation Orders to preserve data may be issued for all criminal offences, <i>if it could have been ordered under the same conditions in a similar domestic case in the issuing State, where there are sufficient reasons to believe that a crime has been committed, where it is grave enough to justify the cross-border preservation of the data and where the requested information is relevant for that investigation. It shall be limited to data of specific persons with a direct link to the specific proceedings referred to in Article 3(2).</i>	2. It may be issued where necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order. European Preservation Orders to preserve data may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months.	
Article 6(3)				
214	3. The European Preservation Order shall include the following information:			
Article 6(3), point a				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
215	a) the issuing and, where applicable, the validating authority;			
Article 6(3), point b				
216	b) the addressee of the European Preservation Order as referred to in Article 7;			
Article 6(3), point c				
217	c) the persons whose data shall be preserved, except where the sole purpose of the order is to identify a person;	c) the <i>individually identifiable persons</i> whose data shall be preserved, <i>or</i> , where the sole purpose of the order is to identify a person, <i>any other unique identifier such as user name or Login ID</i> ;	c) the persons whose data is being requested <i>user</i> , except where the sole purpose of the order is to identify a person <i>the user, or any other unique identifier such as user name, ID or account name to determine the data that are being sought</i> ;	
Article 6(3), point d				
218	d) the data category to be preserved (subscriber data, access data, transactional data or content data);	d) the data category to be preserved (subscriber data, <i>traffic</i> data or content data);	d) the data category to be preserved (subscriber data, access data, transactional data or content data);	
Article 6(3), point e				
219	e) if applicable, the time range requested to be preserved;	e) the time range requested to be preserved, <i>tailored as narrowly as possible</i> ;	e) if applicable, the time range requested to be preserved;	
Article 6(3), point f				
220	f) the applicable provisions of the criminal law of the issuing State;			
Article 6(3), point g				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
221	g) the grounds for the necessity and proportionality of the measure.	g) the grounds for the necessity and proportionality of the measure, <i>taking due account of the impact of the measure on the fundamental rights of the specific persons whose data is sought and the seriousness of the offence.</i>	g) the grounds for the necessity and proportionality of the measure.	
Article 6(3a)				
222		<i>3a. If the issuing authority has reasons to believe that data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, or its preservation may impact fundamental interests of that Member State such as national security and defence, the issuing authority shall seek clarification before issuing the European Preservation Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network in criminal matters. Where the issuing authority finds that the requested data is protected by such immunities and privileges or its preservation would impact fundamental interests of the other Member State, the issuing authority shall not issue the European Preservation Order.</i>		
Article 6a				
223		<i>Article 6a</i> <i>Legal representative</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 6a(1)				
224		<p><i>1. Service providers, offering services in the Member States bound by this Regulation, but not established in the Union, shall designate one legal representative for receipt of, compliance with and enforcement of European Production Orders and European Preservation Orders issued by the competent authorities of the Member States, for the purpose of gathering electronic information in criminal proceedings. The legal representative shall be established in one of the Member States (bound by this Regulation) where the service provider offers its services.</i></p>		
Article 6a(2)				
225		<p><i>2. Service providers, offering services in the Member States bound by this Regulation, but established in a Member State not bound by this Regulation, shall designate one legal representative for receipt of, compliance with and enforcement of European Production Orders and European Preservation Orders issued by the competent authorities of the Member States, for the purpose of gathering electronic information in criminal proceedings. The legal representative shall be established in one of the Member States (bound by this Regulation) where the service provider offers its services.</i></p>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 6a(3)				
226		<i>3. Service providers which are part of a group shall be allowed to collectively designate one legal representative.</i>		
Article 6a(4)				
227		<i>4. The legal representative shall be entrusted with the receipt, compliance and enforcement of those decisions and orders on behalf of the service provider concerned.</i>		
Article 6a(5)				
228		<i>5. Upon designation of the legal representative, service providers shall notify in writing that Member State where their legal representative is established. The notification shall contain the designation and contact details of its legal representative as well as any changes thereof.</i>		
Article 6a(6)				
229		<i>6. The notification shall specify the official language(s) of the Union, as referred to in Regulation 1/58, in which the legal representative can be addressed. This shall include, at least, one of the languages accepted by the Member State where the legal representative is established.</i>		
Article 6a(7)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
230		<i>7. Information, notified to Member States in accordance with this Article, shall be made available on a dedicated internet page of the European Judicial Network in criminal matters. Such information shall be regularly updated.</i>		
Article 6a(8)				
231		<i>8. Member States shall ensure that the designated legal representative can be held liable for non-compliance with obligations under this Regulation when receiving decisions and orders, without prejudice to the liability and legal actions that could be initiated against the service provider.</i>		
Article 6a(9)				
232		<i>9. Member States shall lay down rules on sanctions applicable to infringements pursuant to this Article and shall take all measures necessary to ensure that they are implemented. The sanctions provided for shall be effective, proportionate and dissuasive.</i>		
Article 7				
233	<i>Article 7</i> <i>Addressee of a European Production Order and a European Preservation Order</i>			
Article 7(1)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
234	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.	<i>1. For the purpose of gathering electronic information in criminal proceedings, the European Production Order and the European Preservation Order shall be addressed directly and simultaneously:</i>	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.	
Article 7(1), point a				
235		<i>a) to the main establishment of the service provider, or, where applicable, its legal representative in the executing State designated by the service provider for the purpose of gathering evidence in criminal proceedings; and</i>		
Article 7(1), point b				
236		<i>b) to the executing authority.</i>		
Article 7(1a)				
237		<i>1a. Member States shall ensure that any service provider established on their territory notifies that Member State in writing of where its main establishment is. The notification shall contain the contact details, as well as any changes thereof.</i>		
Article 7(1b)				
238		<i>1b. Information, notified to Member States in accordance with paragraph 1a, shall be made available on a dedicated internet page of the European Judicial Network in criminal matters. Such information shall be regularly updated.</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 7(2)				
239	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.	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.	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.	
Article 7(3)				
240	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.	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.	3. Where the legal representative does not comply with an EPOC in an emergency case pursuant to Article 9(2), the European Production Order EPOC may be addressed to any establishment of the service provider in the Union.	
Article 7(4)				
241	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.	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.	4. Where the legal representative does not comply with its obligations under Articles 9 or 10 and the issuing authority considers that there is a serious risk of loss of data, the European Production Order or the European Preservation Order may be addressed to any establishment of the service provider in the Union.	
Article 7a (Council Mandate)				
242			<i>Article 7a</i> <i>Notification</i>	
Article 7a(1)				

Commission Proposal	EP mandate	Council Mandate	Draft agreement
243		<p>1. In cases where the European Production Order concerns content data, and the issuing authority has reasonable grounds to believe that the person whose data are sought is not residing on its own territory, the issuing authority shall submit a copy of the EPOC to the competent authority of the enforcing State at the same time the EPOC is submitted to the addressee in accordance with Article 7.</p>	
Article 7a(2)			
244		<p>2. The notified authority may as soon as possible inform the issuing authority of any circumstances pursuant to Article 5 (7) (b) and shall endeavour to do so within 10 days. The issuing authority shall take these circumstances into account in the same way as if they were provided for under its national law and shall withdraw or adapt the Order where necessary to give effect to these grounds if the data were not provided yet. In case of withdrawal the issuing authority shall immediately inform the addressee.</p>	
Article 7a(3)			
245		<p>3. Where power to waive the privilege or immunity lies with an authority of the enforcing State, the issuing authority may request the notified authority to contact the competent authority to request it to exercise its power forthwith. Where power to waive the privilege or</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			immunity lies with an authority of another Member State or a third country or with an international organisation, the issuing authority may request the authority concerned to exercise that power.	
Article 7a(4)				
246			4. The notification shall not have suspensive effect on the obligations of the addressee under this Regulation.	
Article 7a (EP mandate)				
247		<i>Article 7a Common European exchange system</i>		
Article 7a(1)				
248		<i>1. By ... [date of application of this Regulation] the Commission shall establish a common European exchange system with secure channels for the handling of authorised cross-border communication, authentication and transmission of the Orders and of the requested data between the competent authorities and service providers. The competent authorities and service providers shall use this system for the purpose of this Regulation.</i>		
Article 7a(2)				
249		<i>2. The Commission shall ensure that the system guarantees an effective, reliable and smooth exchange of the relevant</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>information and a high level of security, confidentiality and integrity as well as the necessary protection of privacy and personal data in line with Regulation (EU) 2018/1725, Regulation (EU) 2016/679, Directive (EU) 2016/680, and Directive (EC) 2002/58. To this end, open and commonly used state-of-the-art electronic signature and encryption technology shall be applied.</i>		
Article 7a(3)				
250		<i>3. Where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, it shall be possible to interconnect such systems or channels with this common European exchange system.</i>		
Article 8				
251	<i>Article 8 European Production and Preservation Order Certificate</i>			
Article 8(1)				
252	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).	1. A European Production or Preservation Order shall be transmitted to the addressee as defined in Article 7 via the system as defined in Article 7a through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).	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).	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Article 8(2)				
253	<p>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.</p> <p>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.</p>	<p>2. The EPOC or the EPOC-PR shall be directly transmitted <i>via the system as defined in Article 7a, allowing the addressees to produce</i> a written record allowing the addressees to establish <i>the authenticity of the Order and of the issuing authority</i>.</p>	<p>2. The EPOC or the EPOC-PR shall be directly transmitted by or on behalf of the issuing authority any means capable in a secure and reliable way allowing of producing a written record under conditions allowing the addressee to produce a written record and to establish its the authenticity of the Certificate.</p> <p>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.</p>	
Article 8(3)				
254	<p>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.</p>	<p>3. The EPOC shall contain <i>all</i> the information listed in Article 5(5) (a) to (i), including sufficient information to allow the addressees to identify and contact the issuing authority, <i>and information regarding the means and technical interfaces it has at its disposal to receive the produced data, or where to find this information</i>.</p>	<p>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.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 8(4)				
255	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.	4. The EPOC-PR shall contain <i>all</i> the information listed in Article 6(3) (a) to (g), including sufficient information to allow the addressee to identify and contact the issuing authority.	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.	
Article 8(5)				
256	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.	5. Where needed, the EPOC or the EPOC-PR shall be translated into an official language of the <i>executing State or in any other language explicitly accepted by the executing State in accordance with paragraph 5a.</i>	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 8a				
257		<i>Article 8a</i> <i>Execution of an EPOC for subscriber data and IP addresses for the sole purpose of identifying a person</i>		
Article 8a (1), paragraph 1				
258		<i>1. An EPOC for subscriber data and IP addresses, for the sole purpose of</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>identifying a person, shall be addressed directly and simultaneously:</i>		
Article 8a (1), paragraph 1, point a				
259		<i>(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and</i>		
Article 8a (1), paragraph 1, point b				
260		<i>(b) to the executing authority.</i>		
Article 8a (1), paragraph 2				
261		<i>The simultaneous information of the executing authority shall not have a suspensive effect on the obligations of the service provider as referred to in paragraph 1.</i>		
Article 8a(2)				
262		<i>2. Upon receipt of the EPOC for subscriber data and IP addresses, for the sole purpose of identifying a person, the service provider shall ensure that the requested data is transmitted directly to the issuing authority, or the law enforcement authorities as indicated in the EPOC, as soon as possible and at the latest within 10 days upon receipt of the EPOC. When transmitting the requested data, the service provider shall simultaneously send a copy of the data</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>transferred for information to the executing authority.</i>		
Article 8a(3)				
263		<i>3. In emergency cases, the service provider shall transmit the requested data without undue delay, at the latest within 16 hours upon receipt of the EPOC. When transmitting the requested data, the service provider shall simultaneously make the data available to the executing authority for information.</i>		
Article 8a(4)				
264		<i>4. Where the executing authority decides to invoke any of the grounds listed in Article 10a (1), it shall act as soon as possible and at the latest within the time periods as referred to in paragraphs 1 or 2, and immediately inform the issuing authority and the service provider of its decision. The issuing authority shall erase the data. Where the requested data has not yet been transmitted to the issuing authority, the addressed service provider shall not transmit the data.</i>		
Article 8a(5)				
265		<i>5. Where the EPOC is incomplete, contains manifest errors, in form or content, or does not contain sufficient information to execute the EPOC, the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC without</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>undue delay and ask for clarification or, where necessary, correction from the issuing authority, using the Formset out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.</i>		
Article 8a(6)				
266		<i>6. Where the service provider cannot comply with its obligations because of force majeure or of de facto impossibility due to circumstances not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. Where the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC and inform the addressees of its decision.</i>		
Article 8a(7)				
267		<i>7. In all cases where the service provider does not provide the requested information, does not provide it exhaustively or does not provide it within</i>		

Commission Proposal	EP mandate	Council Mandate	Draft agreement	
		<p><i>the deadline, for other reasons, including for technical or operational ones, it shall inform the issuing authority as well as the executing authority referred to in the EPOC without undue delay and at the latest within the deadlines set out in paragraphs 1 and 2 of the reasons for this using the Form in Annex III. The issuing authority shall review the order in light of the information provided by the service provider and if necessary, set a new deadline for the addressees. In case the service provider considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it is manifestly abusive or that it exceeds the purpose of the order, the service provider shall also send the Form in Annex III to the issuing authority as well as to the executing authority referred to in the EPOC with a suspensive effect as regards the transmission of the requested data. In such cases the executing authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network in criminal matters. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1 and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.</i></p>		
Article 8a(8)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
268		<i>8. Where the service provider does not produce the data requested immediately, in accordance with paragraphs 3, 4, and 5, it shall preserve the data requested, where possible. The preservation shall be upheld until the data is produced or until the EPOC is withdrawn or null and void.</i>		
Article 9				
269	<i>Article 9 Execution of an EPOC</i>	<i>Article 9 Execution of an EPOC for traffic or content data</i>	<i>Article 9 Execution of an EPOC</i>	
Article 9(-1a)				
270		<i>- 1a. An EPOC for traffic or content data shall be addressed directly and simultaneously:</i>		
Article 9(-1a), point a				
271		<i>(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and</i>		
Article 9(-1a), point b				
272		<i>(b) to the executing authority.</i>		
Article 9(1)				
273	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	1. Upon receipt of the EPOC <i>for traffic and content data, the service provider</i>	1. Upon receipt of the EPOC, the addressee shall ensure that the requested data is are transmitted in a secure and reliable way allowing the establishment of	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	indicated in the EPOC at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure.	<i>shall act expeditiously to preserve the data.</i>	authenticity and integrity directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days upon receipt of the EPOC, unless the issuing authority indicates reasons for earlier disclosure.	
Article 9(1a)				
274		<i>1a. Where the executing authority decides to refuse the EPOC, based on one of the grounds provided for in Article 10a (new), it shall act as soon as possible and at the latest within 10 days upon receipt of the EPOC and inform the issuing authority and the service provider of such decision immediately.</i>		
Article 9(2)				
275	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.	2. In emergency cases, <i>where the executing authority decides to refuse the EPOC based on one of the grounds provided for in Article 10a, it shall act as soon as possible and at the latest within 16 hours upon receipt of the EPOC and inform the issuing authority and the service provider of such decision immediately.</i>	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.	
Article 9(2a)				
276		<i>2a. Where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) of the Treaty on European Union, the service provider shall transmit the requested data only after receiving the explicit written approval of the executing</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>authority. For this, the executing authority shall assess the order of the issuing authority with due diligence and check in particular for grounds for non-recognition or non-execution pursuant to Article 10a, before giving its written approval within the deadlines set out in paragraph 1a and 2.</i>		
Article 9(2b)				
277		<i>2b. Without prejudice to paragraph 2a, where the executing authority has not invoked any of the grounds listed in Article 10a within the time periods referred to in paragraphs 1a and 2, the service provider to which the order is addressed shall ensure that the requested data is immediately transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC.</i>		
Article 9(2c)				
278		<i>2c. Where it is not possible in a specific case for the executing authority to meet the time limit set out in paragraph 1 or 2, it shall, without undue delay, inform the issuing authority and the service provider by any means, giving the reasons for the delay and the estimated time necessary for the decision to be taken.</i>		
Article 9(3)				
279	3. If the addressee cannot comply with its obligation because the EPOC is	3. Where the EPOC is incomplete, contains manifest errors, in form or content , or does	3. If the addressee cannot comply with its obligation because the EPOC is	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	not contain sufficient information to execute the EPOC, the <i>service provider</i> shall inform the issuing authority <i>as well as the executing authority</i> referred to in the EPOC without undue delay and ask for clarification <i>or, where necessary, correction from the issuing authority</i> , using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1a and 2 shall not apply until the clarification is provided. <i>In the absence of a reaction from the issuing authority, the order shall be considered null and void.</i>	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.	
Article 9(4)				
280	4. If the addressee cannot comply with its obligation because of <i>force majeure</i> 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.	4. <i>Where</i> the <i>service provider</i> cannot comply with its obligations because of <i>force majeure</i> or of de facto impossibility <i>due to circumstances</i> not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC, the <i>service provider</i> shall inform the issuing authority <i>as well as the executing authority</i> referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. <i>Where</i> the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC <i>and inform the addressees of its decision.</i>	4. If the addressee cannot comply with its obligation because of <i>force majeure</i> or of de facto impossibility due to circumstances not created by the addressee or the service provider at the time the order was received not attributable to the addressee or, if different, the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC , the addressee shall inform the issuing authority referred to in the EPOC without undue delay explaining the reasons, using the Form set out in Annex III. If the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC.	
Article 9(5), paragraph 1				

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
281	<p>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.</p>	<p>5. In all cases where the <i>service provider</i> does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons, <i>including for technical or operational ones</i>, it shall inform the issuing authority <i>as well as the executing authority referred to in the EPOC</i> without undue delay and at the latest within the deadlines set out in paragraphs 1a 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 <i>addressees</i>.</p>	<p>5. In all cases where the addressee does not provide the requested information, does not provide it exhaustively or does not provide it within the deadline, for other reasons listed in the Form of Annex III, it shall inform the issuing authority without undue delay and at the latest within the deadlines set out in paragraphs 1 and 2 of the reasons for this using the Form in Annex III. The issuing authority shall review the order in light of the information provided by the service provider and if necessary, set a new deadline for the service provider to produce the data.</p>	
Article 9(5), paragraph 2				
282	<p>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.</p>	<p>In case the <i>service provider</i> considers that the EPOC cannot be executed because based on the sole information contained in the EPOC it is apparent that it is manifestly abusive <i>or that it exceeds the purpose of the order</i>, the <i>service provider</i> shall also send the Form in Annex III <i>to the issuing authority as well as to the executing authority referred to in the EPOC with a suspensive affect as regards the transmission of the requested data</i>. In such cases the competent <i>executing</i> authority may seek clarifications from the issuing authority on the European Production Order, either directly or via Eurojust or the European Judicial Network <i>in criminal matters. The issuing authority</i></p>	<p>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.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>shall react expeditiously and within 5 days at the latest. The deadlines set out in paragraphs 1a and 2 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.</i>		
Article 9(6)				
283	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.	6. During the procedure referred to in paragraphs 1, 1a, 2, 2b, 2c, 3, 4, and 5, the service provider shall preserve the data requested, where possible. The preservation shall be upheld until the data is produced or until the EPOC is withdrawn or null and void.	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				
284	<i>Article 10 Execution of an EPOC-PR</i>			
Article 10(-1a), paragraph 1				
285		- 1a. An EPOC-PR shall be addressed directly and simultaneously		
Article 10(-1a), paragraph 1, point a				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
286		<i>(a) to the main establishment of the service provider or, where applicable, where its legal representative is established; and</i>		
Article 10(-1a), paragraph 1, point b				
287		<i>(b) to the executing authority.</i>		
Article 10(-1a), paragraph 2				
288		<i>The simultaneous information of the executing authority shall not have a suspensive effect on the obligations of the service provider as referred to in paragraph 1.</i>		
Article 10(1)				
289	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.	1. Upon receipt of the EPOC-PR, the service provider shall act expeditiously to preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been launched. The EPOC-PR can be extended by additional 30 days, only when necessary to allow further assessment of the relevance of the data.	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.	
Article 10(2)				
290	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	2. Where the issuing authority submits the subsequent European Production Order within the deadline referred to in paragraph 1, the service provider shall preserve the data as long as necessary for the execution of that European	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	data once the subsequent request for production is served.	<i>Production Order pursuant to Articles 8a or 9.</i>	data once the subsequent request for production is served.	
Article 10(3)				
291	3. If the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay.	3. Where the preservation is no longer necessary, the issuing authority shall inform the addressees without undue delay and the preservation shall cease immediately.	3. If the preservation is no longer necessary, the issuing authority shall inform the addressee without undue delay.	
Article 10(4)				
292	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.	4. Where the EPOC-PR is incomplete, contains manifest errors, in form or content , or does not contain sufficient information to execute the EPOC-PR, the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC-PR without undue delay and ask for clarification or, where necessary, correction from the issuing authority , using the Form set out in Annex III. The issuing authority shall react expeditiously and within 5 days at the latest. The addressees shall ensure that the needed clarification can be received in order, for the service provider , to fulfil its obligations set out in paragraphs 1, 2 and 3. In the absence of a reaction from the issuing authority, the order shall be considered null and void.	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.	
Article 10(5)				
293	5. If the addressee cannot comply with its obligation because of <i>force majeure</i> , or of	5. Where the service provider cannot comply with its obligations because of	5. If the addressee cannot comply with its obligation because of <i>force majeure</i> or of	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	<i>force majeure</i> , or of de facto impossibility due to circumstances not attributable to the service provider, notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the EPOC-PR, the service provider shall contact the issuing authority as well as the executing authority referred to in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. Where the relevant conditions are fulfilled, the issuing authority shall withdraw the EPOC-PR and inform the addressees of its decision.	de facto impossibility due to circumstances not created by the addressee or the service provider at the time the order was received not attributable to the addressee or, if different, the service provider , notably because the person whose data is sought is not their customer, or the data has been deleted before receiving the Order, it the addressee shall contact inform the issuing authority set out in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. If these conditions are fulfilled, the issuing authority shall withdraw the EPOC-PR.	
Article 10(6), paragraph 1				
294	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.	6. In all cases where the service provider does not preserve the requested information, for other reasons listed in the Form of Annex III, including for technical or operational ones , the service provider shall inform the issuing authority as well as the executing authority referred to in the EPOC-PR without undue delay of the reasons for this in the Form set out in Annex III. The issuing authority shall review the Order in light of the justification provided by the service provider.	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 10(6), paragraph 2				
295		<i>In case the service provider considers that the EPOC-PR cannot be executed because based on the sole information contained in the EPOC-PR it is apparent that it is manifestly abusive or that it exceeds the</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>purpose of the order, the service provider shall also send the Form in Annex III to the issuing authority as well as to the executing authority referred to in the EPOC-PR. In such cases the competent executing authority may seek clarifications from the issuing authority on the European Preservation Order, either directly or via Eurojust or the European Judicial Network in criminal matters. The issuing authority shall react expeditiously and within 5 days at the latest. The deadline set out in paragraph 1 shall not apply until the clarification is provided. In the absence of a reaction from the issuing authority, the order shall be considered null and void.</i>		
Article 10a (new)				
296		<i>Article 10a Grounds for non-recognition or non-execution</i>		
Article 10a(1)				
297		<i>1. Without prejudice to Article 1(2), where the EPOC is assessed by the executing authority, the EPOC shall be refused, where:</i>		
Article 10a(1), point a				
298		<i>(a) the conditions for issuing a European Production Order as laid down in Article 5 of this Regulation are not fulfilled;</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 10a(1), point b				
299		<i>(b) the execution of the European Production Order would be contrary to the principle of ne bis in idem;</i>		
Article 10a(1), point c				
300		<i>(c) there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter; or</i>		
Article 10a(1), point d				
301		<i>(d) there is an immunity, a privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the executing State, which makes it impossible to execute the European Production Order;</i>		
Article 10a(2)				
302		<i>2. In addition to paragraph 1, an EPOC for traffic and content data may be refused by the executing authority, where:</i>		
Article 10a(2), point a				
303		<i>(a) the execution of the European Production Order would harm essential national security interests, jeopardise the</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>source of the information or involve the use of classified information relating to specific intelligence activities;</i>		
Article 10a(2), point b				
304		<i>(b) the European Production Order relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct for which the EPOC was issued does not constitute a criminal offence under the law of the executing State;</i>		
Article 10a(2), point c				
305		<i>(c) the conduct for which the EPOC has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex IIIa, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years;</i>		
Article 10a(2), point d				
306		<i>(d) the execution of the European Production Order is restricted under the law of the executing State to a list or category of offences or to offences punishable by a higher threshold; or</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 10a(2), point e				
307		<i>(e) compliance with the European Production Order would conflict with applicable laws of a third country that prohibits disclosure of the data concerned.</i>		
Article 10a(3)				
308		<i>3. Point (e) of paragraph 2 shall be applied according to the procedure set out in Article 14a.</i>		
Article 10a(4)				
309		<i>4. Where the European Production Order concerns an offence in connection with taxes or duties, customs and exchange, the executing authority shall not refuse recognition or execution on the ground that the law of the executing State does not impose the same kind of tax or duty or does not contain a tax, duty, customs and exchange regulation of the same kind as the law of the issuing State.</i>		
Article 10a(5)				
310		<i>5. In the cases referred to in paragraphs 1 and 2 of this Article, before deciding not to recognise or not to execute a European Production Order, either in whole or in part, the executing authority shall consult the issuing authority, by any appropriate means, and shall, where appropriate, request the issuing authority to supply any necessary information without delay.</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 10a(6)				
311		<i>6. In the case referred to in point (d) of paragraph 1 and where power to waive the privilege or immunity lies with an authority of the executing State, the executing authority shall request it to exercise that power forthwith. Where power to waive the privilege or immunity lies with an authority of another State or international organisation, it shall be for the issuing authority to request the authority concerned to exercise that power.</i>		
Article 10a(7)				
312		<i>7. The executing authority shall inform the issuing authority about the use of any of the grounds for non-recognition or non-execution as listed in paragraphs 1 and 2 of this Article, by using the form set out in Annex III.</i>		
Article 11				
313	<i>Article 11 Confidentiality and user information</i>	<i>Article 11 User information and confidentiality</i>	<i>Article 11 Confidentiality and user information</i>	
Article 11(1)				
314	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	1. The service provider shall inform the person whose data is being sought without undue delay. The service provider shall take the necessary <i>state-of-the-art operational and technical</i> measures to ensure the confidentiality, <i>secrecy and</i>	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings.	<i>integrity</i> of the EPOC or the EPOC-PR and of the data produced or preserved.	informing the person whose data is being sought in order to avoid not to obstructing the relevant criminal proceedings. They shall only inform the person whose data is are being sought if explicitly requested by the issuing authority. In this case the issuing authority shall also provide information pursuant to paragraph 4 of this Article to the addressee or, if different, to the service provider.	
Article 11(1a)				
315		<i>1a. As long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings or in order to protect the fundamental rights of another person, the issuing authority, taking into due account the impact of the measure on the fundamental rights of the person whose data is sought, may request the service provider to refrain from informing the person whose data is being sought, based on a judicial order. Such an order shall be duly justified, specify the duration of the obligation of confidentiality and shall be subject to periodic review.</i>		
Article 11(2)				
316	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	2. Where the issuing authority requested the addressee to refrain from informing the person whose data is being sought, based on a judicial order , the issuing authority shall inform the person whose data is being sought by the EPOC or the EPOC-PR without undue delay about the	2. Where the issuing authority did not request the addressee to refrain from the service provider to informing the person whose data were being sought in accordance with paragraph 1 , the issuing authority shall inform this person whose data is being sought by the EPOC without	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings.	data production <i>or preservation</i> . This information may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings, <i>taking into account the rights of the suspected and accused person and without prejudice to defense rights and effective legal remedies.</i>	undue delay about the data production. This issuing authority may delay informing the person whose data were sought as long as it constitutes a necessary and proportionate measure information shall be submitted as soon as this is possible without may be delayed as long as necessary and proportionate to avoid obstructing the relevant criminal proceedings. Information about available remedies pursuant to Article 17 shall be included. The issuing authority may abstain from informing the person whose subscriber or access data was sought about the production of data where fundamental rights and legitimate interests of another person outweigh the interest of the person whose data was sought.	
Article 11(3)				
317	3. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.	3. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.	3. The issuing authority may abstain from informing the person whose subscriber or access data was sought where necessary and proportionate to protect the fundamental rights and legitimate interests of another person, and in particular where these rights and interests outweigh the interest to be informed of the person whose data were sought. When informing the person, the issuing authority shall include information about any available remedies as referred to in Article 17.	
Article 11(4)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
318			4. Information about available remedies pursuant to Article 17 shall be included.	
Article 11a				
319		<i>Article 11a Limitations to the use of information obtained</i>		
Article 11a, paragraph 1				
320		<i>Electronic information obtained in accordance with this Regulation shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except for where there is an imminent threat to the life or physical integrity of a person.</i>		
Article 11b				
321		<i>Article 11b Erasure of electronic information</i>		
Article 11b(1)				
322		<i>1. Electronic information that has been gathered in breach of this Regulation shall be erased without undue delay.</i>		
Article 11b(2)				
323		<i>2. Electronic information that is no longer necessary for all phases of the proceeding for which it was produced or preserved, including possible appeals, shall be erased</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>without undue delay, unless this would affect the defence rights of the suspected or accused person. Periodic reviews for the need of the storage of the electronic information shall be established.</i>		
Article 11b(3)				
324		<i>3. The person whose data was sought shall be informed about the erasure without undue delay.</i>		
Article 11c				
325		<i>Article 11c Admissibility of electronic information in court proceedings</i>		
Article 11c, paragraph 1				
326		<i>Electronic information that has been obtained in breach of this Regulation, including where the criteria laid down in this Regulation are not fulfilled, shall not be admissible before a court. Where electronic information has been obtained before a ground for non-recognition listed in Article 10a (new) has been invoked, it neither shall be admissible before a court.</i>		
Article 12				
327	<i>Article 12 Reimbursement of costs</i>			

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 12, paragraph 1				
328	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.	Where so claimed by the service provider, the issuing State shall reimburse the justified costs borne by the service provider and related to the execution of the European Production Order or the European Preservation Order. For practical reasons, the service provider may claim reimbursement of the costs by the executing State. Where the service provider chooses the executing State, the issuing State shall reimburse the executing State for these costs. Member States shall inform the Commission on the rules for reimbursement, which the Commission shall make public.	The service provider may claim reimbursement of their costs by the issuing State, if this is provided by the national law of the issuing State for domestic orders in similar situations, in accordance with these national provisions. Member States shall inform the Commission about rules for reimbursement who shall make them public.	
Article 12a				
329			Article 12a <i>18 Ensuring privileges and immunities under the law of the enforcing State</i> Limitations to the use of data obtained	
Article 12a(1)				
330			1. In case the person whose data are sought is not residing on the territory of the issuing State, and transactional or content data has been obtained by the European Production Order and the issuing authority receives information that these data it is are protected by privileges or immunities granted under the law of the Member enforcing State of the addressee, or is subject, in the enforcing State, to rules on determination and	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			<p>limitation of criminal liability relating to freedom of press and freedom of expression in other media, or it impacts fundamental interests of that Member State if invoked by that Member State, disclosure of these data would impact its fundamental interests such as national security and defense, the court the competent authorities in the issuing State shall ensure during the criminal proceedings for which the Order was issued that these grounds are taken into account in the same way as if they were provided for under their national law when assessing the relevance and admissibility of the evidence concerned. The court The competent authorities may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust.</p>	
Article 12a(2)				
331			<p>2. Where power to waive the privilege or immunity lies with an authority of the enforcing State, the competent authority in the issuing State may request the enforcing or notified authority to contact the competent authority of the enforcing State to request it to exercise its power forthwith. Where power to waive the privilege or immunity lies with an authority of another Member State or a third country or with an international organisation, the competent authority in the issuing State may request the authority concerned to exercise that power.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 12b				
332			<p style="text-align: center;">Article 12b</p> <p style="text-align: center;"><i>Speciality principle</i></p>	
Article 12b(1)				
333			<p>1. Electronic evidence shall not be used for the purpose of proceedings other than those for which it was obtained in accordance with this Regulation, except:</p>	
Article 12b(1), point a				
334			<p>a) for the purpose of proceedings for which a European Production Order could have been issued in accordance with Article 5(3) and (4); or</p>	
Article 12b(1), point b				
335			<p>b) for preventing an immediate and serious threat to public security of the issuing State or its essential interests;</p>	
Article 12b(2)				
336			<p>2. Electronic evidence obtained in accordance with this Regulation may only be transmitted to another Member State:</p>	
Article 12b(2), point a				
337			<p>a) for the purpose of proceedings for which a European Production Order</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			could have been issued in accordance with Article 5(3) and (4); or	
Article 12b(2), point b				
338			b) for preventing an immediate and serious threat to public security of that Member State or its essential interests.	
Article 12b(3)				
339			3. Electronic evidence obtained in accordance with this Regulation may only be transferred to a third country or to an international organisation pursuant to conditions of paragraph 2, points a) and b) of this Article and Chapter V of the Directive (EU) 2016/680.	
Chapter III				
340	Chapter III: Sanctions and enforcement	Chapter III: Sanctions, review procedure and remedies	Chapter III: Sanctions and enforcement	
Article 13				
341	<i>Article 13 Sanctions</i>			
Article 13, paragraph 1				
342	Without prejudice to national laws which provide for the imposition of criminal sanctions, Member States shall lay down the rules on pecuniary sanctions applicable	1. Member States shall lay down the rules on sanctions applicable to infringements of the obligations pursuant to Articles 8a, 9, 10 and 11 of this Regulation <i>as regards to</i>	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	<i>the service providers on their territory</i> and shall take all necessary measures to ensure that they are implemented. The sanctions provided for <i>by national laws of the Member States</i> 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.	pursuant to Articles 9, 10 and 11 (1) of this Regulation and shall take all necessary measures to ensure that they are implemented. Member States shall, without delay, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. The Member States shall ensure that pecuniary sanctions provided for shall be are effective, proportionate and dissuasive. Member States shall ensure that pecuniary sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed.	
Article 13(1a)				
343		<i>1a. Without prejudice to data protection obligations, service providers shall not be held liable in Member States for the consequences resulting from compliance with an EPOC or an EPOC-PR.</i>		
Article 14				
344	<i>Article 14 Procedure for enforcement</i>			
Article 14(1)				
345	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	1. <i>Where</i> the <i>service provider</i> does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons <i>and where the executing authority has not invoked any of the grounds for non-recognition or non-execution as</i>	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	

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
	<p>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.</p>	<p><i>provided for in Article 10a</i>, the issuing authority may <i>request</i> the competent authority in the <i>executing State to enforce</i> the European Production Order or the European Preservation Order.</p>	<p>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 of accepted by this Member State and shall inform the addressee of the transfer.</p>	
Article 14(2)				
346	<p>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.</p>	<p>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.</p>	<p>2. Upon receipt, the enforcing authority shall without further formalities recognise and take the necessary measures for enforcement of (a) a European Production Order unless the enforcing authority considers that one of the grounds provided for in paragraph 4 apply, or (b) a European Preservation Order transmitted in accordance with paragraph 1 and shall take the necessary measures for its enforcement, unless the enforcing authority considers that one of the grounds provided for in paragraph 4 or 5 apply or that the data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence.</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			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.	
Article 14(2a)				
347			2a. Article 5(8) shall apply mutatis mutandis.	
Article 14(3)				
348	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.	3. The <i>executing</i> authority it shall formally require the <i>service provider</i> to comply with the relevant obligation, informing the <i>service provider</i> of the possibility to oppose the <i>execution</i> by invoking the grounds listed in <i>Articles 8a, 9 and 10</i> , as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.	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 point (a) to (e) or paragraph 5 , as well as the applicable sanctions in case of non-compliance, and set a deadline for compliance or opposition.	
Article 14(4)				
349	4. The addressee may only oppose the enforcement of the European Production Order on the basis of the following grounds:	4. The addressee may only oppose the enforcement of the European Production Order on the basis of the following grounds:	4. The addressee may only oppose the Recognition or enforcement of the European Production Order may only be denied on the basis of the following grounds:	
Article 14(4), point a				
350	a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;	a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;	a) the European Production Order has not been issued or validated by an issuing authority as provided for in Article 4;	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 14(4), point b				
351	b) the European Production Order has not been issued for an offence provided for by Article 5(4);	b) the European Production Order has not been issued for an offence provided for by Article 5(4);	b) the European Production Order has not been issued for an offence provided for by Article 5(4);	
Article 14(4), point c				
352	c) the addressee could not comply with the EPOC because of de facto impossibility or force majeure, or because the EPOC contains manifest errors;	c) the addressee could not comply with the EPOC because of de facto impossibility or force majeure, or because the EPOC contains manifest errors;	c) the addressee could not comply with the EPOC because of de facto impossibility or force majeure, or because the EPOC contains manifest errors;	
Article 14(4), point d				
353	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;	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;	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;	
Article 14(4), point e				
354	e) the service is not covered by this Regulation;	e) the service is not covered by this Regulation;	e) the service is not covered by this Regulation;	
Article 14(4), point f				
355	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.	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.	f) based on the sole information contained in the EPOC, it is apparent that it manifestly violates the Charter or that it is manifestly abusive one of the grounds referred to in Article 12a (1) apply.	
Article 14(5)				
356	5. The addressee may only oppose the enforcement of the European Preservation	5. The addressee may only oppose the enforcement of the European Preservation	5. The addressee may only oppose the Recognition or enforcement of the	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	Order on the basis of the following grounds:	Order on the basis of the following grounds:	European Preservation Order may only be denied on the basis of the following grounds:	
Article 14(5), point a				
357	a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4;	a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4;	a) the European Preservation Order has not been issued or validated by an issuing authority as specified in Article 4;	
Article 14(5), point b				
358	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;	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;	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;	
Article 14(5), point c				
359	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;	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;	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;	
Article 14(5), point d				
360	d) the service is not covered by the scope of the present Regulation;	d) the service is not covered by the scope of the present Regulation;	d) the service is not covered by the scope of the present Regulation;	
Article 14(5), point e				
361	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.	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.	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.	
Article 14(6)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
362	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.	6. In case of an objection by the <i>service provider</i> , the <i>executing</i> authority shall decide whether to enforce <i>or not to recognise</i> the Order on the basis of the information provided by the <i>service provider</i> and, if necessary, supplementary information obtained from the issuing authority. <i>The executing authority shall notify its decision without undue delay to the service provider and the issuing authority.</i>	6. In case of an objection by the addressee pursuant to paragraphs 4 point (a) to (e) and 5 , the enforcing authority shall decide whether to enforce the Order on the basis of the information provided by the addressee and, if necessary, supplementary information obtained from the issuing authority in accordance with paragraph 7.	
Article 14(7)				
363	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.	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.	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.	
Article 14(8)				
364	8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.	8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.	8. All decisions shall be notified immediately to the issuing authority and to the addressee by any means capable of producing a written record.	
Article 14(9)				
365	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	9. If the <i>executing</i> authority obtains the data from the <i>service provider</i> , it shall transmit it to the issuing authority <i>without undue delay</i> .	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.		by an immunity or privilege or by rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media under its own domestic law or it impacts its fundamental interests such as national security and defence. In such case, it shall inform the issuing authority of the reasons for not transmitting the data.	
Article 14(10)				
366	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.	10. In case the <i>service provider</i> does not comply with its obligations, <i>the executing authority</i> shall impose a sanction in accordance with <i>Article 13</i> . An effective judicial remedy shall be available against the decision to impose a fine	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 IV				
367	Chapter 4: Remedies	Chapter 4: Remedies	Chapter 4: Remedies	
Article 14a				
368		<i>Article 14a</i> <i>Review procedure in case of conflicting obligations with third country law</i>		
Article 14a(1)				
369		<i>1. Where the service provider or the executing authority considers that compliance with the European Production</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>Order or the European Preservation Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned, it shall inform the issuing authority and the relevant addressees without undue delay and at the latest within 10 days from the receipt of the order. In this case, execution of an order shall be suspended.</i>		
Article 14a(2)				
370		<i>2. Such notice shall include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation.</i>		
Article 14a(3)				
371		<i>3. The competent authority of the issuing State shall review the European Production Order or the European Preservation Order and inform the addressees, within 10 days after receiving the notice, on the basis of the following criteria:</i>		
Article 14a(3), point a				
372		<i>a) the interests protected by the relevant law of the third country, including fundamental rights as well as other interests preventing disclosure of the data, in particular national security interests of the third country;</i>		
Article 14a(3), point b				
373		<i>b) the degree of connection of the criminal case for which the Order was issued to the jurisdiction of the issuing</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>State and the third country, as indicated inter alia by:</i>		
Article 14a(3), point b, item i				
374		<i>i) the location, nationality and residence of the person whose data is being sought and/or of the victim(s);</i>		
Article 14a(3), point b, item ii				
375		<i>ii) the place where the criminal offence in question was committed;</i>		
Article 14a(3), point c				
376		<i>c) the degree of connection between the service provider and the third country in question;</i>		
Article 14a(3), point d				
377		<i>d) the interests of the issuing State in obtaining the electronic information concerned, based on the seriousness of the offence and the importance of obtaining the electronic information in an expeditious manner;</i>		
Article 14a(3), point e				
378		<i>e) the possible consequences for the addressees of complying with the European Production Order or the European Preservation Order, including the sanctions that may be imposed against the service providers under the law of the third country.</i>		
Article 14a(4)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
379		<p><i>4. Within 10 days after receiving the notice, the issuing authority shall withdraw, uphold or adapt the Order where necessary, to give effect to these criteria. To this end, the issuing authority shall request clarifications on the applicable law from the competent authority of the third country, in compliance with Directive (EU) 2016/680, to the extent that this does not obstruct the deadlines provided for in this Regulation. In the event of withdrawal, the issuing authority shall immediately inform the addressees of the withdrawal.</i></p>		
Article 14a(5)				
380		<p><i>5. Where the issuing authority decides to uphold the Order, it shall inform the addressees of its decision. While duly taking into account the decision of the issuing authority and after also consulting the competent authority of the third country, in compliance with Directive (EU) 2016/680, to the extent that this does not obstruct the deadlines provided for in this Regulation, the executing authority shall take a final decision based on the criteria listed in paragraph 3, within 10 days after receiving the decision of the issuing authority, and inform the issuing authority, the service provider and the competent authority of the third country its final decision.</i></p>		
Article 14a(6)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
381		<i>6. For the duration of the procedure referred to in Article 14a, the service provider shall preserve the data requested.</i>		
Article 15				
382	<i>Article 15 Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country</i>	<i>Article 15 Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country</i>	<i>Article 15 Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country</i>	
Article 15(1)				
383	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).	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).	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).	
Article 15(2)				
384	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Article 15(3)				
385	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	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	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	
Article 15(3), point a				
386	(a) the third country law applies based on the specific circumstances of the case in question and if so,	(a) the third country law applies based on the specific circumstances of the case in question and if so,	(a) the third country law applies based on the specific circumstances of the case in question and if so,	
Article 15(3), point b				
387	(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.	(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.	(b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.	
Article 15(4)				
388	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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.	
Article 15(5)				
389	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.	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.	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.	
Article 15(6)				
390	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	response. If no objection is received within this additional deadline, the competent court shall uphold the Order.	response. If no objection is received within this additional deadline, the competent court shall uphold the Order.	response. If no objection is received within this additional deadline, the competent court shall uphold the Order.	
Article 15(7)				
391	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.	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.	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				
392	<i>Article 16 Review procedure in case of conflicting obligations based on other grounds</i>	<i>Article 16 Review procedure in case of conflicting obligations based on other grounds</i>	<i>Article 16 Review procedure in case of conflicting obligations based on other grounds</i>	
Article 16(1)				
393	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).	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).	1. If the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country prohibiting disclosure of the data concerned on other grounds than those referred to in Article 15, it shall inform the issuing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5) and (6).	
Article 16(2)				
394	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country. It shall be filed no later than 10 days after the date on which the addressee was served with the EPOC. Time limits shall be calculated in accordance with the national law of the issuing authority.	
Article 16(3)				
395	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.	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.	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.	
Article 16(4)				
396	4. The competent court shall first assess whether a conflict exists, based on an examination of whether	4. The competent court shall first assess whether a conflict exists, based on an examination of whether	4. The competent court shall first assess whether a conflict exists, based on an examination of whether	
Article 16(4), point a				
397	a) the third country law applies based on the specific circumstances of the case in question and if so,	a) the third country law applies based on the specific circumstances of the case in question and if so,	a) the third country law applies based on the specific circumstances of the case in question and if so,	
Article 16(4), point b				
398	b) the third country law, when applied to the specific circumstances of the case in	b) the third country law, when applied to the specific circumstances of the case in	b) the third country law, when applied to the specific circumstances of the case in	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	question, prohibits disclosure of the data concerned.	question, prohibits disclosure of the data concerned.	question, prohibits disclosure of the data concerned.	
Article 16(5)				
399	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:	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:	5. If the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. If the competent court establishes that the third country law, when applied to the specific circumstances of the case under examination, prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or lift withdraw the Order. That assessment shall in particular be based on the basis of the following factors while giving particular weight to the factors referred to in points (a) and (b):	
Article 16(5), point a				
400	a) the interest protected by the relevant law of the third country, including the third country's interest in preventing disclosure of the data;	a) the interest protected by the relevant law of the third country, including the third country's interest in preventing disclosure of the data;	a) the interest protected by the relevant law of the third country, including fundamental rights as well as other interests preventing disclosure of the data in particular national security interests of the third country;	
Article 16(5), point b				
401	b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated <i>inter alia</i> by:	b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated <i>inter alia</i> by:	b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated <i>inter alia</i> by:	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	<p>- the location, nationality and residence of the person whose data is being sought and/or of the victim(s),</p> <p>- the place where the criminal offence in question was committed</p>	<p>the location, nationality and residence of the person whose data is being sought and/or of the victim(s),</p> <p>the place where the criminal offence in question was committed</p>	<p>- the location, nationality and residence of the person whose data is being sought and/or of the victim(s),</p> <p>- the place where the criminal offence in question was committed</p>	
Article 16(5), point c				
402	<p>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;</p>	<p>e) 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;</p>	<p>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;</p>	
Article 16(5), point d				
403	<p>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;</p>	<p>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;</p>	<p>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;</p>	
Article 16(5), point e				
404	<p>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.</p>	<p>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.</p>	<p>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.</p>	
Article 16(5b)				
405			<p>5b. The court may seek information from the competent authority of the third country taking into account Directive 2016/680, in particular its</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			Chapter V and to the extent that such the transmission does not obstruct the relevant criminal proceedings.	
Article 16(6)				
406	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	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	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				
407	<i>Article 17 Effective remedies</i>	<i>Article 17 Effective remedies</i>	<i>Article 17 Effective remedies</i>	
Article 17(1)				
408	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.	1. Persons whose data was <i>sought</i> via a European Production Order or a European Preservation Order shall have the right to effective remedies against such Orders , without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.	1. Without prejudice to further legal remedies available in accordance with national law, any Suspects and accused persons whose data was sought obtained via a European Production Order shall have the right to effective remedies against the European Production Order. Where that person is a suspect or accused person, the person shall have the right to effective remedies during the criminal proceedings for in which the Order was issued data were being used. Such remedies shall be without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.	
Article 17(2)				

	Commission Proposal	EP mandate	Council Mandate	Draft agreement
409	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.	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.	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.	
Article 17(3)				
410	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.	3. Such right to an effective remedy shall <i>be exercised before a court in the issuing State or the executing State in accordance with national law and shall</i> include the possibility to challenge the legality of the measure, including its necessity and proportionality.	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.	
Article 17(3a)				
411		<i>3a. The substantive reasons for issuing the European Production Order or the European Preservation Order shall be challenged in the issuing State, without prejudice to the guarantees of fundamental rights in the executing State.</i>		
Article 17(4)				
412	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	4. Without prejudice to Article 11, the issuing authority <i>and the executing authority</i> shall take the appropriate measures to ensure that information is provided <i>in due time</i> about the possibilities under national law for seeking <i>legal</i>	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	ensure that they can be exercised effectively.	remedies, <i>including about when such remedies apply</i> , and ensure that they can be exercised effectively.	ensure that they can be exercised effectively.	
Article 17(5)				
413	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.			
Article 17(6)				
414	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.	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.	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				
415	<i>Article 18 Ensuring privileges and immunities under the law of the enforcing State</i>	<i>Article 18 Ensuring privileges and immunities under the law of the enforcing State</i>	<i>Article 18 Ensuring privileges and immunities under the law of the enforcing State</i>	
Article 18, paragraph 1				
416	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	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	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	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	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.	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.	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 V				
417	Chapter 5: Final provisions			
Article 18a				
418			Article 18a Language	
Article 18, paragraph 1				
419			Each Member State shall indicate, if and which language(s) in addition to their official language(s) they will accept for the transmission of the EPOC or EPOC-PR, and/or of a European Production Order and a European Preservation Order in case of enforcement.	
Article 19				
420	<i>Article 19 Monitoring and reporting</i>			
Article 19(1)				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
421	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.	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 <i>information</i> 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 <i>information</i> .	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.	
Article 19(2)				
422	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:	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:	2. In any event, Member States shall collect and maintain comprehensive statistics from the relevant authorities. The data collected shall be sent to the Commission each year by 31 March for the preceding calendar year and shall, as far as possible , include:	
Article 19(2), point a				
423	a) the number of EPOCs and EPOC-PRs issued by type of data requested, service providers addressed and situation (emergency case or not);	a) the number of EPOCs and EPOC-PRs issued by <i>the</i> type of data requested, <i>the addressees</i> and <i>the</i> situation (emergency case or not);	a) the number of EPOCs and EPOC-PRs issued by type of data requested, service providers addressed and situation (emergency case or not, ex-post validation);	
Article 19(2), point aa				
424		<i>aa) the number of EPOCs issued under emergency case derogations, including</i>		

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<i>details on circumstances and possible outcomes;</i>		
Article 19(2), point ab				
425		<i>ab) the number of EPOCs and EPOC-PRs issued making use of the possibility of the issuing authority to request the service provider to refrain from informing the person whose data is being sought pursuant to Article 11(1a), including information of the circumstances and possible later information pursuant to Article 11(2);</i>		
Article 19(2), point b				
426	b) the number of fulfilled and non-fulfilled EPOCs by type of data requested, service providers addressed and situation (emergency case or not);	b) the number of fulfilled and non-fulfilled EPOCs <i>and EPOC-PRs</i> by <i>the</i> type of data requested, <i>the addressees</i> and <i>the</i> 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);	
Article 19(2), point ba				
427		<i>(ba) the number of EPOCs that were refused, by the type of data requested, the addressees, the situation (emergency case or not) and the ground for non-recognition or non-execution raised;</i>		
Article 19(2), point c				
428	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);	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 <i>the</i> type of data	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);	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		requested, <i>the addressees</i> and <i>the</i> situation (emergency case or not);		
Article 19(2), point ca				
429		<i>ca) for fulfilled EPOC-PRs, the average duration for the respective EPOC procedure following the EPOC-PR, from the moment the EPOC-PR is issued to the moment the EPOC is issued, by the type of data requested and the addressees;</i>		
Article 19(2), point d				
430	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;	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;	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;	
Article 19(2), point e				
431	e) the number of legal remedies against European Production Orders in the issuing State and in the enforcing State by type of data requested;	e) the number of legal remedies <i>used</i> against European Production Orders <i>and European Preservation Orders</i> in the issuing State and in the <i>executing</i> State by <i>the</i> type of data requested;	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 19(2), point f				
432		<i>f) the sanctions imposed, in accordance with Article 13, by the type of data requested, the addressees, the situation (emergency case or not) and the amount of sanctions.</i>	f) the number of cases where no ex-post validation was granted.	
Article 19(2), point g				

Commission Proposal		EP mandate	Council Mandate	Draft agreement
433		<i>g) an overview of the costs claimed by service providers related to the execution of the EPOC or the EPOC-PR and the costs reimbursed by the issuing authorities.</i>		
Article 19(2), point h				
434		<i>h) the number of enforcement procedures launched by the type of data requested, the addressees, the situation (emergency case or not) and the final outcome.</i>		
Article 19(2a)				
435		<i>2a. The Commission shall, by 30 June of each year, publish a report containing the data referred to in paragraph 2 in a compiled form subdivided per into Member States.</i>		
Article 19(3)				
436			3. Service providers may collect, maintain and publish statistics if any such data were collected they may be sent to the Commission by 31 March for the preceding calendar year and may, as far as possible, include:	
Article 19(3), point a				
437			a) the number of EPOCs and EPOC-PRs received by type of data requested, Member States and situation (emergency case or not);	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 19(3), point b				
438			b) the number of fulfilled and non-fulfilled EPOCs by type of data requested, Member States and situation (emergency case or not);	
Article 19(3), point c				
439			c) for fulfilled EPOCs, the average duration for providing of the requested data from the moment the EPOC is received to the moment it is provided, by type of data requested, Member State and situation (emergency case or not).	
Article 20				
440	<i>Article 20 Amendments to the Certificates and the Forms</i>	<i>Article 20 Amendments to the Certificates and the Forms</i>	<i>Article 20 Amendments to the Certificates and the Forms</i>	
Article 20, paragraph 1				
441	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.	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.	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				
442	<i>Article 21 Exercise of delegation</i>	<i>Article 21 Exercise of delegation</i>	<i>Article 21 Exercise of delegation</i>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 21(1)				
443	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	
Article 21(2)				
444	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].	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].	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].	
Article 21(3)				
445	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 <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	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 <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	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 <i>Official Journal of the European Union</i> or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	
Article 21(4)				
446	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ²⁵ . _____	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 2016²⁵. _____	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016 ²⁵ . _____	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	²⁵ OJ L 123, 12.5.2016, p. 13.	²⁰ OJ L 123, 12.5.2016, p. 13.	²⁵ OJ L 123, 12.5.2016, p. 13.	
Article 21(5)				
447	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	
Article 21(6)				
448	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.	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.	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				
449	<i>Article 22 Notifications</i>			
Article 22(1)				
450	1. By [date of application of this Regulation] each Member State shall notify the Commission of the following:	1. By ... [12 months before the date of application of this Regulation] each Member State shall notify the Commission of the following	1. By [date of application of this Regulation] each Member State shall notify the Commission of the following:	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Article 22(1), point a				
451	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;	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;	a) the authorities which, in accordance with its national law, are competent in accordance with to Article 4 to issue and/or , validate, transmit and/or receive European Production Orders and European Preservation Orders or the notifications thereof ;	
Article 22(1), point b				
452	b) the enforcing authority or authorities which are competent to enforce European Production Orders and European Preservation Orders on behalf of another Member State;	b) the <i>executing</i> authority <i>to which the EPOC or EPOC-PR is transmitted for the execution or enforcement of</i> 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;	
Article 22(1), point ba				
453		<i>(ba) where service providers or Member States have already established dedicated systems or other secure channels for the handling of requests for data for law enforcement purposes, the means and technical interfaces the competent authorities have at their disposal to receive or access data produced to be interconnected with the system referred to in Article 7a;</i>		
Article 22(1), point c				
454	c) the courts competent to deal with reasoned objections by addressees in accordance with Articles 15 and 16.	c) the courts competent to deal with reasoned objections by addressees in accordance with Articles 15 and 16.	c) the courts competent to deal with reasoned objections by addressees in accordance with Articles 15 and 16.	
Article 22(1), point d				
455			d) languages accepted for the transmission of the EPOC or EPOC-PR	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
			and/or a European Production Order and a European Preservation Order, in case of enforcement in accordance with Article 18a.	
Article 22(1a)				
456		<i>1a. By the same date, service providers with establishments in more than one Member State shall notify the Commission of the place of their main establishment in the Union.</i>		
Article 22(2)				
457	<p>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/JHA²⁶.</p> <p>-----</p> <p>²⁶ Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).</p>	<p>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 <i>in criminal matters</i> referred to in Article 9 of the Council Decision 2008/976/JHA³⁰.</p> <p>-----</p> <p>³⁰ Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).</p>	<p>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/JHA²⁶.</p> <p>-----</p> <p>²⁶ Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).</p>	
Article 23				
458	<p><i>Article 23 Relationship to European Investigation Orders</i></p> <p>Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for</p>	<p><i>Article 23 Relationship to European Investigation Orders and Mutual Legal Assistance Procedures</i></p>	<p><i>Article 23 Relationship to European Investigation Orders other instruments, agreements and arrangements</i></p> <p>This Regulation does not affect EU and other international instruments,</p>	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
	the gathering of evidence that would also fall within the scope of this Regulation.	<i>The authorities of the Member States</i> may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU, or to use the existing mutual legal assistance procedures for the gathering of electronic information , that would also fall within the scope of this Regulation.	agreements and arrangements on Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for the gathering of evidence that would also fall within the scope of this Regulation.	
Article 24				
459	<i>Article 24 Evaluation</i>			
Article 24, paragraph 1				
460	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.	By [2 years from the date of application of this Regulation] at the latest, the Commission shall carry out an evaluation of the Regulation and present a report to the European Parliament and to the Council on the functioning of this Regulation, which shall, include an assessment of the need to enlarge its scope. in particular, evaluate the number of cases in which the emergency derogation, pursuant to Article 9 (2), and the derogation from the principle of user information, pursuant to Article 11, were applied. If necessary, The report shall be accompanied by an assessment of the functioning of the common European exchange Ssystem as well as an assessment of the functioning of the Regulation in relation with	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.	

Commission Proposal		EP mandate	Council Mandate	Draft agreement
		<p><i>Directive 2014/41/EU of the European Parliament and of the Council.</i></p> <p>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.</p>		
Article 25				
461	<p><i>Article 25</i> <i>Entry into force</i></p>			
Article 25, paragraph 1				
462	<p>This Regulation shall enter into force on the twentieth day following its publication in the <i>Official Journal of the European Union</i>.</p> <p>It shall apply from <i>[6 months after its entry into force]</i>.</p> <p>This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.</p>	<p>This Regulation shall enter into force on the twentieth day following its publication in the <i>Official Journal of the European Union</i>.</p> <p>It shall apply from <i>[18 months after its entry into force]</i>.</p> <p>This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.</p>	<p>This Regulation shall enter into force on the twentieth day following its publication in the <i>Official Journal of the European Union</i>.</p> <p>It shall apply from <i>[6-24 months after its entry into force]</i>.</p> <p>This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.</p>	
Formula				
463	Done at Strasbourg,			

Commission Proposal		EP mandate	Council Mandate	Draft agreement
Formula				
464	<i>For the European Parliament</i> <i>The President</i>			
Formula				
465	<i>For the Council</i> <i>The President</i>			
