E-Evidence Package
THE POSITION OF THE EUROPEAN PARLIAMENT

Last update: 9/08/2021

1. BACKGROUND OF THE E-EVIDENCE PACKAGE

More than half of all criminal investigations today rely on electronic evidence (e-evidence) that is not publicly available and is stored across borders [1]. Therefore, law enforcement and judicial authorities often experience difficulties in accessing e-evidence which is increasingly available only on private infrastructures.

With the objective of improving cross-border access to electronic evidence, the EU is currently taking important steps for a more robust common legal framework, providing clarity and legal certainty to users, service providers and competent authorities, while putting in place strong safeguards in relation to personal data protection and fundamental rights.

Accordingly, in April 2018 **the European Commission** (the Commission) proposed new rules introducing a **Regulation** on European Production and Preservation Orders for electronic evidence in criminal matters and a **Directive** laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

In December 2018, **the Council of the European Union** (the Council) agreed its **General Approach** on the above-mentioned Regulation, which in March 2019 was followed by the **General Approach** on the mentioned Directive.

Within **the European Parliament** (the EP), the proposal for the Regulation has been assigned to the Civil Liberties, Justice and Home Affairs Committee (LIBE). After receiving recommendations from the LIBE Committee in December 2020, the European Parliament agreed on its final **Position** introducing multiple changes, including the integration of the Directive's content into the proposed Regulation, mechanism of mandatory notification, modification of data categories, grounds for non-execution of orders, etc.

On 10 February 2021, the European Commission, the Council of the European Union and the European Parliament began the inter-institutional negotiations on the e-evidence legislative package.

The outcome of these negotiations could radically change the way data is requested in the context of criminal investigations in terms of speed and effectiveness, while preserving user privacy.

This factsheet analyses the Position of the European Parliament.

Other factsheets, available on the SIRIUS platform, present positions of other EU institutions involved in the inter-institutional negotiations:

- **Factsheet on the Proposal of the European Commission**
- **Factsheet on the General Approach of the Council of the European Union**

The factsheets capture initial negotiating positions of the EU institutions, which will change/develop over the course of the inter-institutional negotiations.

2. THE SCOPE

- **Legal regime covered**

The purpose of the proposed Regulation (with merged content of the Regulation and the Directive) is to establish new rules to request electronic information[2] complementing the existing EU legal framework. It is based on principle of mutual trust and aims to clarify the rules of the cooperation between law enforcement, judicial authorities and service providers establishing a binding legal process, while ensuring full compliance with fundamental rights and principles.[3]

To this purpose, service providers would be obliged to designate a **legal representative** in the EU for the receipt of, compliance with and enforcement of decisions and orders in situations where the service provider is either **not established in the EU** or

[1] According to Commission Staff Working Document, Impact assessment accompanying the e-evidence package proposals, 17.4.2018

[2] The term "electronic information" corresponds to the term "electronic evidence "used by the Commission and the Council.

[3] Regulation, Recital 9

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

established in the Member State, which is **not bound by the Regulation**.[4]

Subsequently, in cross-border cases a judicial authority in one Member State will be enabled to obtain electronic information that may serve as evidence directly from a service provider or its legal representative in another Member State. The information requested would have to be handed over within specific time limits reflecting the state of urgency.

This Regulation shall not apply to proceedings initiated for the purpose of providing mutual legal assistance to another Member State or a third country. In addition, 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.[5]

- **Data covered**

The proposed legislation will apply only to **stored data**. Thus, real-time interception of telecommunications is not covered.

Diverging from the outline of the Commission, the EP proposed to cover the three data categories established by the **Budapest Convention**: Subscriber data, Traffic and Content data. The Parliament thus did not uphold the new category of "access data", as included in the Commission's proposal.[6]

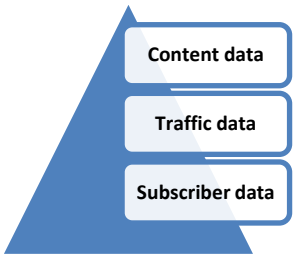

Fig.1 Data covered by the proposed legislation

- **Types of crimes covered**

The requests to **preserve data as well as to produce subscriber data or IP address** (for the sole purpose to determine the identity) may be issued for all criminal offences.

Whereas, requests to produce **traffic or content data** may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years or for the offences listed in the Art. 5 (4a) of the Regulation.

- **Service providers covered**

The obligations established in the draft Regulation apply to service providers offering services in one or more Member States **bound by the Regulation** and established or legally represented in one of these Member States.[7]

To this end, the service providers most relevant for gathering electronic information in criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. [8]

3. DEFINING THE TOOLBOX

The proposed legal framework would introduce new legal tools:

- **European Preservation Order**

A binding decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') addressed to a service provider offering services in the EU and established or legally represented in another Member State bound by this Regulation ('the executing State'), to preserve electronic information in view of a subsequent request for production.[9]

- **European Production Order**

A binding decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') addressed to a service provider offering services in the EU and established or legally represented in another Member State bound by this Regulation ('the executing State'), to produce electronic information.[10]

Both, the European Preservation and the European Production Orders would be transmitted to the service provider and the executing State through a **European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR)**, which are provided as annexes.[11]

[4] Regulation, Art. 6a
[5] Regulation, Recital 15
[6] Regulation, Art.2(7)-2(10)
[7] Regulation, Art. 3(1)
[8] For the definitions of electronic communications services and information society services *see* Regulation, Recital 16
[9] Regulation. Art. 2(2); For the information which shall be included into the European Production Order *see* Regulation, Art. 6(3)
[10] Regulation, Art. 2(1). For the information which shall be included into the European Production Order *see* Regulation, Art. 5(5)
[11] Regulation, Recital, 38

4. ISSUING STATE

A- ISSUING AUTHORITIES

Judicial authorities (a judge, a court, an investigating judge or public prosecutor) or any **other competent authority** defined by the national law of the issuing State and **validated by a judicial authority** in the issuing State would be eligible to issue European Preservation Order for all types of data and European Production Order for subscriber data and IP address for identification purpose.

The European Production Order for traffic and content data may be issued only by **a judge, a court or an investigating judge**; or any **other competent authority** defined by the national law of the issuing State and **validated by a judge, a court or an investigating judge** in the issuing State.

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 defense rights in accordance with national criminal procedure.[12]

B- ISSUING CONDITIONS

- **Necessity and proportionality**

The 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; whether it is grave enough to justify the cross-border production of the data and whether 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 and the purpose of the specific proceeding must be demonstrable at all times. [13]

- **Specificity**

The European Preservation Order and the European Production Order 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, and in consideration of the rights of the suspected or accused person.[14]

- **Correlation of powers under the same conditions in a similar domestic case**

The EP does not establish 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 as it is maintained by the Commission and Council[15], however this principle is mentioned as part of the assessment of necessity and proportionality.

- **Privileges and immunities**

For **all data categories**, the issuing authority shall verify in advance with the executing and the affected Member if there are any reasons to believe that the data is a) protected by immunities or privileges of the person, or b) if it is bound by secrecy, or c) if it impacts the fundamental rights. Consultation process is either with the respective authorities or via EJN or Eurojust. There is no timeline provided for the executing State to reply during this consultation procedure.[16]

C- ISSUING PROCEDURE

The Parliament's position introduces changes to the issuing procedure, in comparison with the Commission's proposal. For **all types of data,** a European Production or Preservation Order would be transmitted directly and simultaneously to the **service provider/legal representative and to the executing authority** via a **common European exchange system** through an EPOC or an EPOC-PR.[17]

Upon receipt of a request, the data would be sent back by the service provider to the issuing state or, where subscriber data or IP addresses were requested for the sole purpose of identification of a person, to both, issuing authority and executing State. Such **notification** may have suspensive effect depending on the category of data and the type of order (see the section Executing State).[18]

[12] Regulation, Art. 1a
[13] Regulation, Recital 29
[14] Regulation, Recital 24
[15] Regulation, Recital 33
[16] Regulation. Art. 5 (7)
[17] Regulation, Art. 7; Art. 8a; Art. 9; Art. 10; Art.10a
[18] Regulation, Art. 8a; Art. 9; Art. 10; Art.10a

D- USE AND ADMISSIBILITY OF DATA OBTAINED

- **Limitations to the use of information obtained**

According to the introduced Article 11a, obtained electronic information shall not be used for any other purpose than the proceedings it was obtained for, except for where there is an imminent threat to the life or physical integrity of a person.

- **Admissibility of electronic information in court proceedings**

According to the introduced Article 11c, the evidence is always inadmissible if electronic information has been obtained in breach of the Regulation, including if the criteria laid down in the Regulation are not fulfilled, or if it has been obtained before a ground for non-recognition has been invoked (as listed in Article 10a).

5. SERVICE PROVIDERS

- **Timeline for execution**

Upon receipt of the EPOC-PR, the service provider shall act expeditiously to preserve the data requested for a period of **60 days**, unless the issuing authority confirms that the subsequent request for production has been launched. Diverging from the initial proposal, the EP provides that the EPOC-PR can be extended by additional 30 days, only when necessary to allow further assessment of the relevance of the data.[19] Upon receipt of the EPOC, the service provider/ legal representative will be obliged to respond within **10 days**, and within **16 hours** in cases of emergency[20], which is an extended timeline compared with 6 hours requirement proposed by the Commission and the Council.

- **Clarification of Orders**

The service provider/ legal representative would be entitled to ask clarification and, where necessary, correction from the issuing authority in case the **EPOC-PR or EPOC issued for all types of data** is incomplete, contains manifest errors, in form or content, or does not contain sufficient information to execute it. The issuing authority has to react within 5 days, otherwise the order shall be considered null and void.[21]

- **Challenge of Orders**

The service provider/ legal representative may object the EPOC or EPOC-PR if it considers that compliance would conflict with laws of a third country. As well as the Council, the EP does not differentiate review procedure based on protection of fundamental rights or fundamental interests of the third country and other grounds as it is in the Commission's proposal. It provides one common review procedure addressing conflicting obligations' cases in the introduced Article 14a of the draft Regulation.

In addition, the Order may be objected if it is considered manifestly abusive or exceeds the purpose of the order. In such cases, the executing authority may seek clarifications from the issuing authority either directly or via Eurojust or the EJN. The issuing authority shall react within 5 days, otherwise the order shall be considered null and void.[22]

- **Obligation to inform**

In cases where it is impossible to comply because of force majeure or of de facto impossibility or for other reasons, a service provider/ legal representative shall inform the issuing and the executing authorities without undue delay explaining the reasons.[23]

- **Sanctions**

The European Preservation Order and European Production Order would be legally binding and service provider as well as its legal representative could be held liable for non-compliance. The sanctions shall be effective, proportionate and dissuasive. The EP emphasized that service providers would not be held liable for the consequences resulting from compliance with an EPOC or an EPOC-PR. [24]

- **Cost reimbursement**

The service provider would be entitled to claim reimbursement of their justified costs related to the execution of the European Production Order or the European Preservation Order, from the issuing State. Moreover, the service provider could choose to claim his costs from the executing State, but the issuing State shall then reimburse these costs.[25]

[19] Regulation, Art 10 (1)
[20] According to the draft Regulation, Recital 2(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person. The EP introduces changes in relation to the Commission's proposal which in the definition of emergency also included imminent threat to "critical infrastructure".
[21] Regulation, Art. 8a(5)
[22] Regulation, Art. 8a(7); Art.9(5) para.2.; Art. 10(6) para.2.
[23] Regulation, Art. 8a (6), Art 9 (4), Art. 10 (5)
[24] Regulation, Art. 13
[25] Regulation, Art 12

- **Sharing a legal representative**

To limit the burden on small and medium-sized enterprises (SMEs), the service providers which are part of a group shall be allowed to collectively designate one legal representative.[26]

6. EXECUTING STATE

The EP has made substantial modifications to the content as well as to the concept of the proposal, introducing mandatory and non-mandatory grounds for refusal, replacing the term "enforcing state" with the term "executing state" and extending executing state's involvement in the process.

- **EPOCs for subscriber data and IP addresses for the sole purpose of identifying a person**

Upon the notification (as described in chapter 4, sub-chapter C), the executing State is required to scrutinize the four **mandatory grounds of non-execution** listed in Article 10a (1). However, there will be **no suspensive effect** on the obligations of the service provider. Therefore, if the executing authority decides to invoke any of the grounds listed in Article 10a (1), it will have to immediately inform the issuing authority and the service provider. Then, the service provider shall not transmit the data and if the requested data has been already transmitted, the issuing authority shall erase this data.

- **EPOCs for traffic and content data**

Upon the notification, the executing State is required to check **mandatory and non-mandatory grounds** provided in Article 10a (1) and (2). The notification would **have a suspensive effect** on the obligations of the service provider. Whether the executing authority decides to refuse the EPOC, based on one of the grounds provided for in Article 10a, it shall inform the issuing authority and the service provider within 10 days, or 16 hours in emergency cases.

- **Non-compliance with an EPOC-PR or an EPOC**

If the service provider does not comply with an EPOC-PR or with an EPOC, and if the executing authority has not invoked any of the grounds for non-recognition or non-execution as provided for in Article 10a, the issuing authority may request the competent authority in the executing State to enforce the European Production Order or the European Preservation Order.[27] Following the request, the executing authority shall formally require the service provider to comply with the relevant obligation within a set deadline for compliance or opposition.

There are 2 main outcome scenarios:

- The **data is obtained** from the service provider/ legal representative and the executing authority transmits it to the issuing authority without undue delay.

- The **objection from the service provider/legal representative is received** and the executing authority decides to enforce it, not to recognize the Order, or to request supplementary information from the issuing authority. The decision shall be notified to the service provider and the issuing authority without undue delay.

7. USERS

- **User Information and Confidentiality**

The EP took a different position from the non-notification approach proposed by the Commission and maintained by the Council, underlying that the service provider must, in principle, **inform the person whose data are requested without undue delay**. The delay, if it is deemed proportionate and necessary in order not to obstruct the relevant criminal proceedings or to protect the fundamental rights of another person, shall be based on a judicial order. Such an order shall be duly justified, specifying the duration of the obligation of confidentiality and shall be subject to a periodic review.[28]

- **Access to legal remedies**

The persons who were affected by **a preservation order and/ or a production order** would be entitled to challenge the legality of the measure, including its necessity and proportionality. Also, an effective remedy may be exercised not only before the courts of the issuing State but also before the courts of the executing State in accordance with national laws, with the limitation that substantive reasons for issuing an order shall be assessed by the courts of the issuing State without prejudice to the

[26] Regulation, Art. 6a(3)
[27] Regulation, Art.14
[28] Regulation, Art. 11 (1a)

guarantees of fundamental rights in the executing State.[29]

8. SIRIUS PROJECT

The acknowledgement of **SIRIUS project** and its role as a knowledge repository of cross-border access to e-evidence and of legal information based on domestic legislation and case law, is emphasised.[30] The Recital 50 of the draft Regulation indicates that: "Information and case law on the interpretation of the laws of a third country and on conflict procedures in Member States should be made available on a central platform such as the SIRIUS project and/or the European Judicial Network, with a view to benefitting from experience and expertise gathered on the same or similar questions. […]"

Adhering to this, the SIRIUS project will continue to expand its repository of data, by creating **country specific fiches** related to the interpretation of third countries' law and conflicting procedures among Member States. Moreover, the SIRIUS project will develop a **repository of information on legislation and case-law** related to the privileges and immunities available under national legislation of the enforcing EU Member States.

[29] Regulation, Art.17.

[30] Regulation, Recital 50.