SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

E-Evidence Package

THE PROPOSAL OF THE EUROPEAN COMMISSION

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 initial proposal of the European Commission.

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

- **Factsheet on the General Approach of the Council of the European Union**
- **Factsheet on the Position of the European Parliament**

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 OF THE PROPOSAL

- **Legal regime covered**

The proposed legal framework departs from location of data storage as the determining factor for jurisdiction. It is based on the principle of mutual recognition of judgements and judicial decisions and aims to establish direct interaction with the service providers to access e-evidence as a binding legal process. The same rules and obligations would be applicable to all service providers, regardless of where the data is stored and where they are based, as long as they offer services on the EU market.

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 this way, the suggested legislation establishes asymmetrical cooperation, which will allow a judicial authority in one Member

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

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.

State to request and obtain e-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.

However, the proposed legislation would not be applicable to purely domestic requests when national authorities would be obliging service providers established or represented on their territory to comply with similar national measures.

- **Data covered**

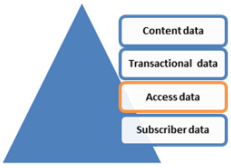

Fig.1 Data covered by the proposed legislation

The proposed legislation aims to preserve and obtain electronic evidence, which refers only to stored data. Real-time interception of telecommunications is not covered. The proposal defines four categories: Subscriber data, Access data, Transactional data (together, the three categories are commonly referred to as 'non-content data') and Content data.[2] It is noted, that such categorisation of data differs from the approach taken in other international instruments, such as the **Budapest Convention**.

- **Types of crimes covered**

According to the proposal, requests to preserve data as well as to produce subscriber or access data may be issued for all criminal offences.

Whereas, access to transactional and content data should be subject to stricter requirements to reflect the more sensitive nature of such data. Accordingly, requests to produce transactional or content data may only be issued for criminal offences punishable in the issuing State by a custodial sentence of at least 3 years, or the offences listed in the Art. 5 (4) points b and c of the Regulation.

- **Service providers covered**

The obligations established in the legislative proposal apply to the service providers offering their services in the EU with the exceptions when those service providers are established on the territory of a single Member State and offer services exclusively on the territory of that Member State.[3]

To this end, the service providers most relevant for criminal proceedings are providers of electronic communications services and specific providers of information society services that facilitate interaction between users. [4]

3. DEFINING THE TOOLBOX

The proposed legal framework would introduce new legal tools:

- **European Preservation Order**

A binding decision by an issuing authority of a Member State compelling a service provider offering services in the EU and established or represented in another Member State, to preserve electronic evidence. It can be issued in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order.[5]

- **European Production Order**

A binding decision by an issuing authority of a Member State compelling a service provider offering services in the EU and established or represented in another Member State, to produce electronic evidence.[6]

Both, the European Preservation and the European Production Orders would be transmitted to the service provider through a **European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR**), which are provided as annexes to the Regulation.[7]

4. ISSUING STATE

A- ISSUING AUTHORITIES

Judicial authorities (a judge, a court, an investigating judge or 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 and access data.

The European Production Order for transactional and content data can be issued only by **a judge, a**

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

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.[8]

B- ISSUING CONDITIONS

- **Necessity and proportionality**

Both, the European Preservation and the 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.[9]

- **Specificity**

The European Production Order and the European Preservation Order should be issued only in the framework of specific criminal proceedings against the specific known or still unknown perpetrators of a concrete criminal offence that has already taken place, after an individual evaluation of proportionality and necessity [10].

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

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.[11]

- **Privileges and immunities**

For transactional and content data, issuing authorities might need to check with the enforcing and the affected Member States, if there are any reasons to believe that the data is protected by immunities or privileges, or if it is bound by secrecy, or impact the fundamental rights. The consultation process takes place between the respective authorities or via the European Judicial Network (EJN) or Eurojust. There is no timeline provided for the consultation.[12]

C- ISSUING PROCEDURE

Aiming to preserve and subsequently obtain the specific data via European Preservation and Production Order, the issuing authority (as defined in sub-chapter A) would directly transmit[13] their certificates to the service provider or its legal representative. The service provider would send the data back either directly to the issuing authority or via its legal representative.

5. SERVICE PROVIDERS

- **Timeline for execution**

Upon receipt of the EPOC-PR, the service provider/ legal representative would be obliged to preserve the requested data without undue delay for a period of 60 days, unless the issuing authority confirms that the subsequent request for production has been launched.[14] Upon receipt of the EPOC, the service provider/ legal representative will be obliged to respond within **10 days** and within **6 hours** in cases of emergency[15].

- **Clarification of Orders**

The service provider/ legal representative would be entitled to ask clarification from the issuing state. The issuing authority would be obliged to react within 5 days.

- **Challenge of Orders**

The service provider/ legal representatives would be entitled to oppose the enforcement of the EPOC or the EPOC-PR only on the basis of certain grounds.[16]

In addition, they would be entitled to object[17] the execution of the Order if they consider that compliance would conflict with laws of a third country prohibiting disclosure of the data (e.g. based on protection of fundamental rights of the individuals concerned, the fundamental interests of the third country related to national security or defence or other grounds). The proposed Regulation provides an explicit review procedure addressing such cases. [18]

- **Obligation to inform:**

- **Impossibility to comply**

In cases where it is impossible to comply with the obligation because of force majeure or de facto impossibility (e.g. because the person whose data is sought is not the customer, or the data has been deleted before receiving the EPOC), the service

[8] Regulation, Art.4
[9] Regulation, Recital 29
[10] Regulation, Recital 24
[11] Regulation, Recital 33
[12] Regulation, Art. 5 (7) para 1)
[13] By any means capable of producing a written record under conditions that allow the service provider to establish authenticity and in line with the rules protecting personal data.
[14] Regulation, Art 10(1)
[15] According to the Regulation, Recital 2(15) 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure.
[16] Regulation, Art. 14, para. 4-5
[17] Such an objection would have a suspensive effect of the execution of the European Production Order pending a review by the competent court in the Member State of the issuing authority, according to Article 16(3) of the Regulation.
[18] Regulation, Art.15-16.

provider/ legal representative would have to inform the issuing authority without undue delay explaining the reasons.[19]

- **Requested information is not provided, partially provided or provided with delay**

In all cases where requested information is not provided in full, at all or not within the deadline, upon receipt of the EPOC, the service provider/ legal representative would have to inform the issuing authority without undue delay and latest within 10 days or 6 hours in case of emergency, explaining the reasons.[20]

- **Sanctions**

The European Preservation Order and European Production Order would be legally binding, i.e. the service provider would be obliged to cooperate and would face pecuniary sanctions in case of non-compliance.[21]

- **Cost Reimbursement**

The service provider would be entitled to claim reimbursement of their costs from the issuing State, if in similar situations reimbursement was provided in national law of the issuing State for domestic orders.[22]

6. ENFORCING STATE

In case of non-compliance with the EPOC or an EPOC-PR, the issuing authority could transfer the Orders, their certificates and the form filled by the service provider/ legal representative to the enforcing state, which is the Member State in which the service provider or its legal representative resides or is established. Upon receipt, the enforcing authority should recognise the Order within 5 working days, if there are no grounds for non- enforcement, and should formally require the service provider/ legal representative to comply within a set deadline.[23]

There are 3 main outcome scenarios:

- The **data is obtained** from the service provider/ legal representative and the enforcing authority transmits it to the issuing authority within 2 working days.
- The **objection from the service provider/legal representative is received** and the enforcing authority either enforces the Order or requests supplementary information from the issuing authority.
- If the enforcing authority **considers not to recognise** or enforce the Order, before issuing its decision it would consult with the issuing authority, which should reply within 5 working days.

7. USERS

- **Confidentiality and User Notification**

The Commission proposes an approach of non-notification to the concerned user when requested by the issuing authority, obliging the service provider/legal representative to ensure confidentiality of the EPOC-PR, the EPOC and of the data preserved or produced, in order not to obstruct the relevant criminal proceedings.[24]

- **Access to legal remedies**

The person, whose information was sought, would be entitled to challenge the legality of the measures taken to disclose and/or use of this data, including the grounds of necessity and proportionality. Such remedies would be exercised before a court in the issuing State in accordance with its national law.[25]

8. SIRIUS PROJECT

The acknowledgement of the **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.[26] The Recital 50 of the draft Regulation indicates that: "Information and case law on the interpretation of third countries' laws and on conflicts procedures in Member States should be made available on a central platform such as the SIRIUS project and/or the European Judicial Network. […]"

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.

[19] Regulation, Art 9(4)
[20] Regulation, Art 9(5)
[21] Regulation, Art. 13.
[22] Regulation, Art. 12.
[23] Regulation, Art.14
[24] Regulation, Art.11
[25] Regulation, Art.17.
[26] Regulation, Recital 50.