SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

E-Evidence Package
THE GENERAL APPROACH OF THE COUNCIL OF THE EU

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 General Approach of the Council of the European Union.

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 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

- **Legal regime covered**

The Council aligns its General Approach regarding the scope of the e-evidence package with the one proposed by the European Commission[2]. Accordingly, the proposed legal framework is based on a principle of mutual recognition of judgements and judicial decisions. It 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

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

[2] The factsheets on the General Approach of the Council of the EU and the Position of the European Parliament on E-Evidence Package are available in SIRIUS

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.

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 State to 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. In addition, the new rules will 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.[3]

- **Data covered**

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

Likewise, the Council took similar approach with the Commission, covering four categories of data: Subscriber data, Access data, Transactional data (together, the three categories are commonly referred to as 'non-content data') and Content data.[4] It is noted that such categorisation of data differs from the approach taken in other international instruments, such as **Budapest Convention**.

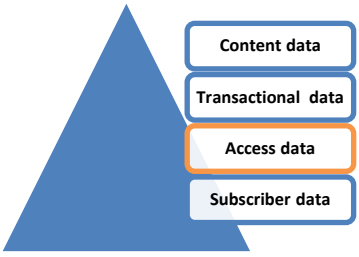

Fig.1 Data covered by the proposed legislation

- **Types of crimes covered**

The **requests to preserve data as well as to produce subscriber 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 if they were **not rendered in absentia.**[5]

Whereas, **requests to produce transactional or content data** may only be issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or the offences listed in the Art. 5 (4) points b and c of the Regulation, as well as for the execution of a custodial sentence or a detention order of at least 4 months imposed for the mentioned criminal offences.

- **Service providers covered**

The criteria for service providers covered by the draft legislation remain in line with the Commission's proposal. Therefore, 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.[6]

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. [7]

3. DEFINING THE TOOLBOX

The European Investigation Order (EIO) and the Mutual Legal Assistance (MLA) will continue to exist, but the proposed new rules provide fast track alternative tools for obtaining electronic evidence:

- **European Preservation Order**

It is 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 in view of a subsequent request for production.[8]

- **European Production Order**

It is 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.[9]

[3] Regulation, 3(1a)
[4] Regulation, Art.2(7)-2(10)
[5] Regulation, Recital 24b introduced new features indicating that the new legal framework would 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 if they were not rendered in absentia.
[6] Directive, Art.1
[7] For the definitions of electronic communications services and information society services *see* Regulation, Recital 16
[8] Regulation. Art. 2(2); For the information which shall be included into the European Production Order *see* Regulation, Art. 6(3)
[9] Regulation, Art. 2(1). For the information which shall be included into the European Production Order *see* Regulation, Art. 5(5)

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.[10]

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 a European Preservation Order for all types of data and a 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 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.[11]

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. It is noted that the Council added to the Commission's original proposal the necessity to take "due account of the impact of the measure on fundamental rights of the person whose data are sought".[12]

- **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.[13]

- **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.[14]

- **Privileges and immunities**

For requested transactional data, issuing authorities might need to check with the executing and the affected Member States, if there are any reasons to believe that the data is protected by immunities or privileges granted under the law of the enforcing State, or if in that Member State it is subject to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression. Also, they need to verify if its disclosure may impact fundamental interests of the enforcing State such as national security and defence. 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.

The issuing authority should consider the findings of the consultation 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.[15]

- **Notification**

It is noted, that the Council introduced a **notification** for requests of content data when the issuing authority has reasonable grounds to believe that the person whose data are sought is not residing in its territory. In such cases, 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 service provider/ legal representative.[16] However, such **notification** does not have any suspensive effect on the obligations of the service provider.

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[17] their certificates to the service provider or its legal representative. The service provider would send the data back either directly to the issuing authority

[10] Regulation, Recital, 38
[11] Regulation, Art.4
[12] Regulation, Recital 29
[13] Regulation, Recital 24
[14] Regulation, Recital 33
[15] Regulation. Art. 5 (7). The possibilities to waive a privilege or immunity are provided in Art. 5 (8) of the Regulation
[16] Regulation, Articles 8a (1), 9 (1a) and 10 (1a))
[17] 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.

or via its legal representative. This procedure would also apply if the electronic evidence were stored in a third country.

D- USE OF DATA OBTAINED

The Council introduced the principle of specialty, emphasizing that electronic evidence shall not be used for the purpose of proceedings other than those for which it was obtained, except a) for proceedings for which a European Production Order could have been issued (Article 5(3) and (4)); b) for preventing an immediate and serious threat to public security of the issuing State or its essential interests. In addition, the Council sets similar conditions for a possibility to transfer electronic evidence obtained in accordance with the Regulation to a third country or to an international organisation.

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.[18] 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[19].

- **Clarification of Orders**

The service provider/ legal representative would be entitled to ask clarification from the issuing state in case the EPOC does not allow it to identify the data requested and when the EPOC-PR is incomplete, contains manifest errors or does not contain sufficient information to execute it.

- **Challenge of Orders**

The service provider/ legal representatives would be entitled to object the enforcement of the EPOC or the EPOC-PR based on Article 14 paragraph 4 points (a) to (e) and paragraph 5 of the proposed Regulation.

In addition, diverging from the proposal of the Commission, the service providers/legal representatives would be entitled to object[20] the execution of the Order based only on one ground, i.e. if they consider that compliance would conflict with laws of a third country.[21]

- **Obligation to inform about the impossibility to comply**

In cases where it is impossible to comply because of de facto impossibility or for other reasons, a service provider/ legal representative would have to inform the issuing authority without undue delay explaining the reasons. It is noted that the Council modified the Commission's proposal in this regard by not restricting the "impossibility to comply" to specific reasons.[22]

- **Sanctions**

The European Preservation Order and the European Production Order would be legally binding and thus service providers and legal representatives could be held jointly liable for non-compliance. The pecuniary sanctions imposed can reach up to 2% of the total worldwide annual turnover of the service provider's preceding financial year. However, the Council also emphasized that legal representatives should have sufficient resources and powers to perform their tasks. Therefore, when determining a sanction, all relevant circumstances, such as the nature, gravity, duration of the breach, intention, financial strength of the service provider, shall be taken into consideration. [23]

- **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.

- **Sharing a legal representative**

To limit the burden on small and medium-sized

enterprises, there is a possibility to share the same legal representative.

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. Upon receipt, the enforcing

[18] Regulation, Art 10(1)
[19] 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.
[20] 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.
[21] In its General Approach, the Council has deleted Art. 15 related to the review procedure based on protection of fundamental rights or fundamental interests of the third country, as well as deleted other grounds" in the Article 16 (1), leaving in the draft only considerations for review procedure based on conflicts with applicable laws of a third country.
[22] Regulation, Art. 9 (4)
[23] Regulation, Art. 13., Recital 45a

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.[24]

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 the decision it should consult with the issuing authority, which should reply within 5 working days.

7. USERS

- **Confidentiality and User Notification**

The Council maintains an approach of **non-notification**, obliging the service provider/ legal representative to ensure confidentiality of the EPOC-PR, the EPOC and of the data preserved or produced in order to avoid obstructing the relevant criminal proceedings. They shall only inform the person whose data are being sought if explicitly requested by the issuing authority.

Where the issuing authority did not request the service provider to inform the person whose data were sought, this authority shall inform this person. However, the delay of a notification can take as long as it constitutes a necessary and proportionate measure. [25]

- **Access to legal remedies**

The person whose data 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.[26]

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.[27] 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.

[24] Regulation, Art.14
[25] Regulation, Art.11
[26] Regulation, Art.17.
[27] Regulation, Recital 50.