EUROJUST

Eurojust meeting on the EU e-evidence package

Roles and responsibilities of Member States, service providers and Eurojust

Outcome report of the meeting of 30 September - 1 October 2025

Table of Contents

1. Introduction and background

In light of the upcoming entry into application of the EU e-evidence package, consisting of Regulation (EU) 2023/1543 (e-Evidence Regulation) and Directive (EU) 2023/1544 (e-Evidence Directive), Eurojust organised a meeting on the roles and responsibilities of EU Member States, service providers and Eurojust in relation to this new legislation. The meeting was held on 30 September and 1 October 2025 at Eurojust's premises in The Hague and online via videoconference.

The EU e-evidence package will make it faster and easier for law enforcement and judicial authorities to obtain the electronic evidence needed to investigate and prosecute criminals. The new rules introduce the European Production Order (EPOC) and European Preservation Order (EPOC-PR) and the obligation for service providers offering their services in the EU to designate a legal representative in one Member State bound by the Regulation (all except for Denmark). Under the e-Evidence Regulation, an issuing authority will be able to send an order to provide and/or preserve data (EPOC/EPOC-PR) directly to a (legal representative of a) service provider in another Member State, who will have to execute the order within certain time limits. In some situations, the issuing authority will also have to notify the enforcing authority in the country where the service provider or its legal representative is based of the issuance of the order. The e-Evidence Regulation also envisages an enforcement procedure, in case a service provider does not comply with an order, and a review procedure, in case of conflicts of law.

The channelling of the orders, the provision of the requested data and any other communication between competent authorities and service providers will take place via a decentralised IT system, the Justice Digital Exchange System (JUDEX).

These rules will apply as of 18 February 2026 for the e-Evidence Directive (which obliges Member States to introduce obligations for service providers to designate a representative in the EU) and as of 18 August 2026 for the e-Evidence Regulation.

The meeting brought together judicial practitioners and representatives of ministries of justice from the Member States; contact points of the European Judicial Cybercrime Network (EJCN); representatives of the European Commission, service providers, the Council of Europe and the European Judicial Network (EJN); members of Eurojust National Desks; and members of the Cybercrime and the Judicial Cooperation Instruments Working Groups at Eurojust.

For the full agenda, see Annex A.

2. Key takeaways

- While the legislative and technical framework for the implementation of the EU e-evidence package is advancing, a number of legal and practical matters remain under consideration at both the national and the EU level.
- There is a diversity of models being developed for the designation of competent authorities across Member States. Transparency and timely publication of these designations will be essential to enable the functioning of the new legal instruments.
- Key potential operational challenges include:
    - the impact of notification on deadlines;
    - the coexistence of parallel legal regimes and obligations; and
    - the handling of privileges, immunities and other grounds for refusal.

  These will all require timely coordination between authorities and service providers.
- Service providers also have constraints and uncertainties linked to, among other things:
    - the volume of requests;
    - technical feasibility;
    - notification mechanics; and
    - the modalities for cost reimbursement.
- Eurojust will support the practical application of the EU e-evidence package:
    - at the operational level, in cases where judicial authorities will encounter obstacles in applying the new instruments; and
    - at the strategic level, through experience-sharing, cooperation with practitioner networks and contributions to structured exchanges between authorities and service providers.

3. Summary of the main issues discussed

3.1. Update by the European Commission

The Commission (the Directorate-General for Justice and Consumers) presented the state of preparedness regarding the implementation of the EU e-evidence package.

The Commission outlined the ongoing preparatory work, including:

- the establishment and recurring meetings of the expert group on the decentralised IT system (involving representatives from the Member States and service providers);
- the expert group on implementation addressing legal interpretation questions; and
- the information sessions being carried out for service providers not represented in the expert groups.

In the Member States, draft legislation is being prepared to enable proper implementation of the EU e-evidence package.

The Commission further highlighted the need for training activities both on the legal framework and on the decentralised IT system, noting that preparatory work is being coordinated with relevant actors, including Eurojust and the SIRIUS project. It was emphasised that, despite the advanced state of preparatory work, several interpretative and operational questions remain, which will need to be addressed in parallel with national legislative processes and the technical deployment of the IT system.

3.2. Identification of competent authorities under the e-Evidence Regulation

The session examined how different Member States are planning to designate competent authorities for the issuance, notification, enforcement and review of EPOCs and EPOC-PRs. The panellists presented their respective national approaches and the rationale behind them.

Ireland

The representative from Ireland explained the background to the approach chosen was informed by two key considerations. Firstly, Ireland has a common law system in which prosecutors and judges have no investigative function. Secondly, a large number of major service providers are established in the country, meaning that Ireland is expecting a high volume of incoming requests (at least 300 000 EPOCs annually). For these reasons, Ireland decided to centralise all key functions under the EU e-evidence package under a single entity, a newly-established Criminal Justice International Cooperation Office. The director of this entity will act as the notification and enforcing authority under the Regulation, and as the central authority under the Directive, thereby ensuring a single central point of contact for cross-border judicial cooperation in e-evidence matters. As far as the issuance of EPOCs/EPOC-PRs is concerned, orders will be generated by law enforcement officers, who are the primary investigative authority in Ireland, and validated by designated judges of the district courts. Review procedures in conflict of law situations will be referred to the High Court for adjudication.

Germany

The representative from Germany indicated that the issuance and validation of orders will rest with the same authorities that would be competent in a national case, subject to the

requirements of the e-Evidence Regulation concerning judicial validation, where applicable. Notification and enforcement will be handled by public prosecutors' offices where the service provider or its legal representative is located, while conflicts of law will be reviewed by the Higher Regional Courts. This decentralised model reflects Germany's federal structure. Lastly, the central authority under the e-Evidence Directive will be the Federal Office of Justice in Bonn.

Sweden

The representative from Sweden presented the approach adopted by the Swedish legislator, noting that the country has a centralised and not highly formalistic legal system. Public prosecutors will act as issuing authorities for EPOCs/EPOC-PRs, subject to court validation where required. Members of the police authority, the security service and customs (and other law enforcement authorities) will also be able to issue EPOCs for subscriber data and EPOC-PRs, subject to validation by a public prosecutor. Notification and enforcement will be done to and by public prosecutors while the Stockholm District Court will be competent for ruling on conflicts of law.

Issues raised during the discussion included:

- how notification under Article 8 of the e-Evidence Regulation will operate in decentralised systems;
- how duplication with the procedures to be established under the Second Additional Protocol to the Cybercrime Convention on enhanced cooperation and disclosure of electronic evidence (Second Additional Protocol) can be avoided; and
- the importance of the publication of competent authorities on the EJN website before August 2026 for the good functioning of the new legal instruments.

3.3. Practical session: EPOC/EPOC-PR in action – case scenarios

In this session, participants worked in groups on three practical case scenarios and provided feedback at a discussion in the plenary session. For the full case scenarios and the prompting questions used during the exercise, see Annex B.

The issues discussed included:

- the practical importance of having early and reliable access to information on designated establishments and legal representatives (once fully operational, the decentralised IT system is expected to provide this information and indicate the correct addressee);
- the fact that short data retention periods may significantly reduce the utility of EPOCs and EPOC-PRs, especially if not acted upon swiftly;
- that incorrect or late notification can affect the running of deadlines for the production of data;
- situations involving the coexistence of a removal order under the EU Digital Services Act (DSA) and an EPOC/EPOC-PR, which engage:
    - the need for clarity on the hierarchy between different legal instruments,
    - the importance of direct communication between authorities and service providers,
    - the possibility of technical measures to allow simultaneous compliance, thereby avoiding direct conflict between two different legal obligations, and
    - the value of early consultation through Eurojust;

- grounds for refusal under Article 12 of the e-Evidence Regulation – in relation to refusal connected to immunities and privileges, it was noted that service providers may, in some cases, be aware of circumstances relevant to privileges or immunities and it was noted that, while they may draw attention to such circumstances, they are not under an obligation to do so; and
- the interaction between the 10-day deadline for the production of data by a service provider following receipt of an EPOC and the 10-day period within which the notified enforcing authority may raise grounds for refusal, which has a suspensive effect on the service provider's production obligation – if no early indication is provided by the enforcing authority, the service provider will not know until the last moment whether the data must ultimately be produced; in this context, it was observed that service providers would need to have the data prepared in advance, and that a degree of flexibility and early communication could mitigate any operational risks.

3.4. EPOC and EPOC-PR: How can Eurojust assist you?

Two leaflets, one providing a detailed ([1]) and one a more condensed ([2]) overview of the roles of Eurojust, the SIRIUS project, the EJN and the EJCN regarding the new legal tools, and the type of support they can provide to practitioners, were distributed to the participants.

In the context of the EU e-evidence package, Eurojust will support national judicial authorities both operationally and strategically, as follows.

On the operational side, Eurojust may assist at different stages of the life cycle of an EPOC/EPOC-PR, including:

- the pre-issuing phase (choice of legal basis and assistance with drafting);
- the execution phase (facilitating contacts with enforcing authorities and supporting discussions between competent authorities on the handling of grounds for refusal, conflicts of law or questions relating to privileges and immunities);
- coordination where several orders are issued simultaneously to different Member States; and
- coordination when parallel proceedings risk interfering with each other.

Eurojust will not function as a central authority for the application of the e-Evidence Regulation. Direct communication between issuing and enforcing authorities and service providers will remain the rule. However, Eurojust may be approached to support consultation in complex situations, in particular where different national approaches, conflicting legal obligations or multi-jurisdictional sensitivities make direct resolution difficult. For these purposes, judicial authorities can reach out to Eurojust through their respective National Desks or Liaison Prosecutors.

On the strategic side, Eurojust, via the Cybercrime and the Judicial Cooperation Instruments Working Groups, and in cooperation with the EJCN, the EJN and the SIRIUS project, will contribute to:

- knowledge development and the sharing of best practices;
- capturing issues arising in case work;
- cooperating with other relevant networks and stakeholders; and
- organising or contributing to structured exchanges between practitioners, service providers and policymakers.

([1]) Eurojust, *European Production and Preservation Orders: Key actors offering support*, Eurojust, 2025, https://doi.org/10.2812/9057210.
([2]) Eurojust, *European Production and Preservation Orders: Support at a glance*, Eurojust, 2025, https://doi.org/10.2812/3069390.

The SIRIUS project will continue to develop knowledge products and practical tools related to cross-border access to e-evidence, with a particular focus on cooperation with third countries, including guidelines on filling in EPOCs/EPOC-PRs and service provider specific guidelines. The project will also continue to engage in capacity-building and awareness-raising activities, again focusing on reaching out to third countries, including through the SIRIUS annual conference, in-person and online training sessions, webinars and e-learning modules. In addition, the SIRIUS project will maintain strategic dialogue with service providers on topics pertaining to cross-border access to e-evidence.

3.5. The decentralised information system for channelling EPOCs/EPOC-PRs: JUDEX

The Commission presented the state of development of JUDEX, the decentralised IT system through which EPOCs and EPOC-PRs and related communications will be channelled between competent authorities and service providers and provided a live demo of the system.

The Commission indicated that a minimum viable version is expected to be made available to Member States and service providers for testing in early 2026. Once operational, the use of JUDEX will be obligatory for the transmission of EPOCs/EPOC-PRs and related communications. With regard to Eurojust's connection to the system, the time frame remains unclear.

3.6. The point of view of service providers: workflows, challenges and needs

This session provided participants with the perspective of service providers on the upcoming application of the EU e-evidence package. Representatives from Meta, Microsoft, Google, OVH Cloud and EuroISPA (European Internet Services Providers Association) contributed to the exchange. The points raised included the following.

Existing internal workflows and expected adjustments

Service providers noted that current procedures for responding to law enforcement requests can serve as a basis for developing e-evidence package-specific workflows. However, significant adaptations will still be required, in particular due to:

- binding deadlines;
- the direct effect of orders issued by judicial authorities in other Member States; and
- the large and diverse number of competent authorities across the EU, which will require internal capacity.

The central importance of JUDEX

Service providers underlined that the timely functioning of JUDEX will be critical for the effective operation of the EU e-evidence package. It was observed that:

- a phased roll-out or limited testing could complicate operational readiness;
- questions remain regarding liability in case of transmission failures;
- safeguards are needed against unauthorised use of the system; and
- appropriate encryption safeguards are required for all data transmitted for security purposes, including data transferred outside JUDEX where the volume exceeds 25 megabytes.

The need for clear and consistent national implementation

Several interventions stressed the importance of coherent domestic implementing legislation to avoid legal uncertainty during the initial phase of application. Reference was made to experiences with other legal instruments where divergent national interpretations led to inconsistent practices. In this regard:

- early and targeted training for competent authorities is considered essential;
- training should include information on what data individual service providers can supply and which identifiers reliably link an EPOC/EPOC-PR to a specific account; and
- the valuable role of the SIRIUS project in delivering such support was highlighted.

Technical considerations and practical challenges

Participants discussed a range of operational issues, including:

- situations in which the volume or format of data may make compliance with strict deadlines difficult, particularly in urgent cases involving large datasets;
- differences in technical understanding between authorities and service providers, which may create misalignment; and
- the suggestion that a common set of technical terms with clear definitions could help mitigate such issues.

Outstanding legal and practical questions

Service providers also pointed to several open matters, such as:

- the scope of registration obligations;
- the handling of translation and language requirements;
- cost reimbursement processes; and
- the lack of a central mechanism to map certain identifiers (e.g. telephone numbers) to the appropriate service provider.

Organisational readiness of authorities

It was noted that the functioning of the system will depend not only on its technical deployment but also on the capacity of enforcing authorities to process notifications and objections within the prescribed deadlines. Observations included:

- readiness levels may vary across Member States;
- some interpretative questions remain under consideration at the EU and the national levels; and
- continued structured dialogue, including through Eurojust, will be important to support consistent implementation.

3.7. The e-evidence legal instruments in the wider context

This session provided an overview of how the EU e-evidence package interacts with other legal instruments used to obtain electronic evidence, in particular the Second Additional Protocol. The key points discussed included the following.

Scope and features of the e-Evidence Regulation and the Second Additional Protocol

It was recalled that the e-Evidence Regulation will:

- enable the direct transmission of production and preservation orders (for subscriber, traffic and content data) to service providers offering services in the EU;
- operate together with a notification regime that may have suspensive effect; and
- apply irrespective of the physical location of the service provider, when its services are offered within the EU.

In contrast, the Second Additional Protocol will:

- permit direct cooperation only for obtaining subscriber information and domain registration information;
- apply based on the provision of services by:
    - an entity providing domain name registration services (Article 6), and/or
    - a service provider being physically present (Article 7)

  in the territory of a Party to the Second Additional Protocol;
- include a notification and consultation mechanism; and
- provide a wider framework that goes beyond public-to-private cooperation, including public-to-public channels, notably for emergency situations under Articles 9 and 10.

It was underlined that both frameworks include safeguards and that neither instrument prevents the use of the other where appropriate.

Coexistence of instruments and continued relevance of traditional cooperation tools

The EU e-evidence package will not replace existing cooperation tools. Instead, it will coexist alongside them, allowing authorities to choose the instrument best suited to the procedural needs of each case.

Existing instruments such as mutual legal assistance requests, European Investigation Orders (EIOs) and joint investigation teams will remain essential. They will continue to govern:

- categories of evidence not covered by the e-Evidence Regulation or the Second Additional Protocol; and
- investigative contexts in which their procedural scope is more suitable.

For these reasons, practitioners will require in-depth knowledge of all available instruments and their respective procedural features.

Support tools and ongoing capacity-building efforts

Reference was made to the CyberSPEX project, a joint EU–Council of Europe initiative implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC). The project aims to strengthen cooperation on cybercrime and electronic evidence and provides templates, manuals and guidance, including support for the implementation of the Second Additional Protocol into Member States' domestic law.

ANNEX A

30 September–1 October 2025

The e-evidence package:

Exchange between Member States, service providers and Eurojust on their roles and responsibilities

DAY ONE	
13:30 – 13:40	**Welcome by Eurojust**
13:40 – 14:00	**The e-evidence package: Implementation and future application– are we ready?** This presentation will set the scene on the topic, providing a short overview of the procedure, workflow and stages of the EPOC/EPOC-PR, the authorities involved and the use of JUDEX as the decentralised IT-system to channel EPOCs/EPOC-PRs. European Commission, Directorate-General for Justice and Consumers
14:00 – 14:30	**Identification of competent authorities under the e-Evidence Regulation: Key considerations** This session will provide an opportunity to exchange information on which authorities have been/should be appointed as competent authorities under the e-Evidence Regulation, including authorities to be notified, enforcing authorities and courts that will rule on conflicts of law and remedies. Ireland Germany Sweden Open discussion with participants
14:30 – 14:45	**Coffee break**
14:45 – 15:30	**Practical session: EPOC/EPOC-PR in action – case scenarios** In this session, participants will work in groups on practical case scenarios, considering how to issue and handle EPOCs/EPOC-PRs.
15:30 – 16:15	**Feedback from the practical session** In this plenary session, a representative from each group will present an overview of the main findings from the practical session. Moderation: Eurojust
16:15 – 16:30	**Coffee break**
16:30 – 17:00	**EPOC and EPOC-PR: How can Eurojust assist you?** This presentation will raise awareness among participants of the future role of Eurojust, including the SIRIUS Project, and the interplay with other stakeholders (EJN, EJCN) in the context of the new legal instruments. It will also provide an opportunity for participants to flag potential challenges for which they might reach out to these actors. Eurojust Open discussion with participants

17:00 – 17:30	**The decentralised information system for channelling EPOCs/EPOC-PRs: JUDEX** In this session, the use of JUDEX for channelling EPOCs and EPOC-PRs will be elaborated. Participants from both practitioners' and service providers' side will be able to discuss considerations in relation to the use of JUDEX. European Commission, Directorate-General for Justice and Consumers Open discussion with participants

DAY TWO	
9:30 – 10:15	**The point of view of service providers: Workflows, challenges and needs** This session will provide participants with the perspective of service providers on the upcoming application of the e-evidence package, including their designated establishments or legal representatives, internal workflows, and potential legal and practical challenges that can be foreseen. Meta Microsoft Google OVHcloud EuroISPA
10:15 – 11:00	**Plenary discussion: Addressing challenges raised by service providers** In this session, specific legal and practical challenges related to the implementation of the e-evidence package raised by service providers will be discussed. Moderation: Eurojust
11:00 – 11:30	**Coffee break**
11:30 – 12:15	**The e-evidence legal instruments in the wider context** During this session, participants will take a closer look at the interplay between the e-evidence package and other legal instruments for the acquisition of e-evidence, particularly the Second Additional Protocol to the Budapest Convention. Eurojust Council of Europe, Cybercrime Convention Committee (T-CY) Open discussion with participants
12:15 – 12:30	**Concluding session and final remarks** During this session, an overview of the main topics discussed throughout the two days, including particular challenges that were highlighted, will be presented. Eurojust

ANNEX B

The e-evidence package:
Exchange between Member States, service providers and Eurojust on their roles and responsibilities

Practical session: EPOC/EPOC-PR in action
CASE SCENARIOS

CASE SCENARIO 1

Italian authorities are conducting a large investigation into mafia-related organised crime. The main target is believed to be a mafia organisation leader who resides in Belgium but coordinates the group's activities in Italy. Italian authorities have evidence that he issues orders to members of the organisation in Italy through various messaging platforms and cloud services, including service providers established in Germany, France and the Netherlands.

To gather the necessary evidence, the Italian authorities issue three European Production Orders simultaneously:

- One to a service provider with headquarters in Dresden, Germany;
- One to a service provider with its designated establishment in France; and
- One to a service provider with its designated establishment in the Netherlands.

European Production Order issued to service provider in Germany

The Italian authorities issue a European Production Order to obtain subscriber data from a service provider in relation to which they are not sure where the designated establishment / legal representative under the E-Evidence Directive is located but which has its headquarters in Dresden, Germany.

Issues for consideration:

- How can the Italian authorities find out where the service provider's designated establishment / legal representative is located in order to correctly address the European Production Order?
- Would it be possible for them to send the European Production Order to the service provider's headquarters?
- Which steps need to be followed by the Italian authorities to validly issue the European Production Order?

Assume that the European Production Order was correctly addressed to the designated legal entity in Germany. However, the service provider informs the Italian authorities that it is unable to produce the requested data, as it has already been deleted in accordance with its short data retention period.

Issue for consideration:

- How should authorities and service providers address the challenges posed by short data retention periods in such cases?

European Production Order issued to service provider in France

Italian authorities also issue a European Production Order to obtain IP addresses and connection time stamps showing when the main target's device accessed the platform's servers from a service provider with its designated establishment in France.

Issue for consideration:

- Which steps need to be followed by the Italian authorities to validly issue the European Production Order?

As far as notification under Article 8 of the E-Evidence Regulation is concerned, Italian authorities mistakenly notify the wrong authority. They only realise this error on day 8 following the issuance of the European Production Order, and the correct French enforcing authority finally receives notification on day 9 following the European Production Order's issuance.

Issue for consideration:

- How should the authorities and the service provider deal with the late notification error? Does the error affect the deadlines for the production of the data by the service provider?

European Production Order issued to service provider in the Netherlands

Italian authorities issue a European Production Order to obtain content data from a service provider with its designated establishment in the Netherlands.

Issue for consideration:

- Which steps need to be followed by the Italian authorities to validly issue the European Production Order?

Notification to the enforcing authority is done correctly in accordance with Article 8 of the E-Evidence Regulation. The Dutch enforcing authority identifies that the Italian target is already under a covert federal investigation in the Netherlands involving a high-value target. Dutch law provides for embargo procedures in such covert investigations, preventing disclosure of details to foreign authorities.

Furthermore, Italian authorities did not request that the person whose data are being requested about the production of data not be informed about the production of their data on the basis of the European Production Order. Dutch authorities consider that user notification could seriously harm the ongoing investigation in the Netherlands.

Issues for consideration:

- What could the Dutch enforcing authority do to prevent the execution of the European Production Order in the circumstances of the case?
- Can user notification be prevented? What if the user would (also) be notified as a consequence of the European Production Orders issued to service providers in Germany and France?

CASE SCENARIO 2

Order under Article 9 of the DSA vs. European Production and Preservation Orders

Telegram has designated the same legal representative in Belgium under Article 13 of the DSA and under the E-Evidence Directive. This representative receives an order under Article 9 of the DSA from the Polish authorities to remove 101 channels allegedly involved in international arms trafficking.

At the same time, Spanish authorities are conducting a criminal investigation into an organised criminal group (OCG) that allegedly uses Telegram to coordinate arms trafficking activities in Spain. To advance their investigation, the Spanish authorities decide to use the new e-evidence instruments.

The next day, Telegram's legal representative also receives:

- A European Production Order from Spain, requesting subscriber data, traffic data and content data for 49 of the same channels; and
- A European Preservation Order for the same data.

Issue for consideration:

- Which steps need to be followed by the Spanish authorities to validly issue the European Production and Preservation Orders?

Upon receipt of the European Production and Preservation Orders from the Spanish authorities, Telegram has already partially implemented the order under Article 9 of the DSA, but fortunately not yet for the 49 channels that Spain is targeting. However, it still faces a catch-22 situation. On one hand, the order under Article 9 of the DSA from the Polish authorities obliges it to remove illegal content. On the other hand, the Spanish European Preservation and Production Orders require it to preserve and produce exactly that data.

Issues for consideration:

- What should Telegram do in the circumstances of the case? Does any of the two legal instruments prevail when there is a direct conflict between an order under Article 9 of the DSA and a European Preservation / Production Order under the E-Evidence Regulation? Who could Telegram contact to seek guidance?
- Would there be a role to be played by Eurojust in this scenario?

Non-compliance with European Production and Preservation Orders

Assume that Telegram does not comply with the European Production and Preservation Orders from the Spanish authorities within the deadlines foreseen in the E-Evidence Regulation.

Issue for consideration:

- Which enforcement mechanism is available to the Spanish authorities in this case? How should they proceed?

Issuance of the same European Production Order to several service providers

Spanish authorities have reasons to believe that the same OCG also uses other platforms (Signal and Threema) to communicate in parallel with Telegram. In order to obtain the data quickly, they decide to

issue the same European Production Order simultaneously to those service providers for overlapping sets of channels.

Issue for consideration:

- Can a single European Production Order be validly issued to multiple service providers at the same time?

CASE SCENARIO 3

Finland is conducting an investigation into alleged acts of corruption involving a Finnish member of the European Parliament. According to a source, the parliamentarian carried out an online bank transfer from Strasbourg to a bank in Luxembourg, allegedly to make payments to his Hungarian lawyer involved in the cover-up of the alleged acts of corruption. The transaction was reportedly initiated from the parliamentarian's professional account within the European Parliament's premises in Strasbourg. The source provided an email confirming the transaction, with the email header indicating that it originated from the European Parliament network.

<u>European Production Order issued to service provider in France</u>

To substantiate the allegation, Finnish authorities issue a European Production Order to obtain IP traffic data from the French cell phone subscription used by the parliamentarian to a service provider with its designated establishment in France.

Issue for consideration:

- Which steps need to be followed by the Finnish authorities to validly issue the European Production Order?

The French enforcing authority notified pursuant to Article 8 of the E-Evidence Regulation raises the ground for refusal under Article 12(1)(a), invoking the parliamentarian's immunity. Finnish authorities, however, are of the view that the execution of the European Production Order is not hindered by the immunity of the parliamentarian in the investigative phase.

Issues for consideration:

- Can the French enforcing authority invoke a ground for refusal in the circumstances of the case?
- How should the service provider and the Finnish authorities proceed?

<u>European Production Order issued to service provider in Hungary</u>

On 25 April 2028, the Finnish authorities receive information that the parliamentarian's Hungarian lawyer has been disbarred with effect from 1 April 2028.

On 16 May 2028, Finnish authorities issue a European Production Order to a service provider with its designated legal establishment in Hungary, requesting traffic data concerning the parliamentarian's Hungarian lawyer's cell phone communications for the period 1 January to 31 March 2028.

In line with Article 8 of the E-Evidence Regulation, the Hungarian enforcing authority is notified but does not raise any ground for refusal within the applicable deadline. However, the service provider is of the

view that the decisive factor is the lawyer's professional status at the time the data was generated. Since the lawyer was still practicing during the requested period, the service provider concludes that the data is protected by professional secrecy and should not be transferred.

The Finnish issuing authority requests the Hungarian enforcing authority to enforce the European Production Order pursuant to Article 16 of the E-Evidence Regulation.

Issues for consideration:

- Which steps need to be followed by the Finnish authorities to request the Hungarian enforcing authority to enforce the Order?
- Is the European Production Order enforceable, given that the lawyer was still practicing at the time the data was generated? Does the lawyer's subsequent disbarment eliminate the protection of legal professional privilege or does the privilege continue to apply to the data created during the period of legal practice?
- Can or should the service provider take any initiative towards the enforcing authority concerning the potential existence of a ground for refusal?
- Would there be a role to be played by Eurojust in this scenario?

Scan the QR code for the digital version

EUROJUST

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, The Netherlands
www.eurojust.europa.eu • info@eurojust.europa.eu • +31 70 412 5000
Follow Eurojust on X, LinkedIn and YouTube @Eurojust

PDF: Catalogue number: QP-01-26-001-EN-N • ISBN: 978-92-9404-528-7 • DOI: 10.2812/1024623

Eurojust is an agency of the European Union

© Eurojust, 2026. Reproduction is authorised provided the source is acknowledged.