EUROJUST

EUROPOL

Funded by the European Union

SIRIUS guidelines for completing the European Production Order Certificate (EPOC)

Practical guidance for judicial and law enforcement authorities

June 2026

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement NDICI/2024/700002618.

Contents

Introduction 3

SIRIUS guidelines for completing the European Production Order Certificate 4

Section A: Issuing/validating authority 5

Section B: Addressee 6

Section C: Deadlines (tick the appropriate box and complete additional sections, if necessary) 9

Section D: Relation to a previous production/preservation request (tick and complete if applicable and information is available) 12

Section E: Information to support the identification of requested data (complete based on the information that is known and to the extent necessary to identify the data) 15

Section F: Electronic evidence to be produced 18

Section G: Information on the underlying conditions 23

Section H: Information for the user 28

Section I: Details of the issuing authority 30

Section J: Details of the validating authority (complete if applicable) 34

Section K: Notification and details of the enforcing authority (if applicable) 36

Section L: Transfer of data 38

Section M: Further information to be included (not to be sent to the addressee – to be provided to the enforcing authority in the event that it needs to be notified) 41

Funded by the European Union

Introduction

The *SIRIUS guidelines for completing the European Production Order Certificate* provide practical, step-by-step guidance for completing the certificate, as set out in Annex I to Regulation (EU) 2023/1543 (the e-Evidence Regulation).

The guidelines are designed to be used as a practical tool in daily work. They focus on:

- clarity and completeness of information;
- consistency across sections;
- avoiding common errors that may lead to delays or refusals.

The guidelines are structured to follow the layout of the official forms. Each section of the certificate is explained in a consistent manner, including:

- a purpose statement describing the role of the section;
- general guidance applicable to the section as a whole;
- specific instructions for individual fields, where relevant.

Instructions specific to the use of the justice digital exchange system (JUDEX), a decentralised IT system, are highlighted.

The guidelines do not modify the content of the certificate, which is an integral part of the legislation and cannot be changed. The use and acceptance of the guidelines is voluntary and does not affect the obligations arising under EU law. They are without prejudice to the interpretation of EU law by the Court of Justice of the European Union. However, it is strongly recommended that issuing authorities use them to support the efficient, secure and timely preparation and transmission of the European Production Order Certificate (EPOC) in practice.

These guidelines form part of a broader set of SIRIUS guidance materials assisting competent authorities in completing the EPOC and the European Preservation Order Certificate (EPOC-PR). The following documents should be considered alongside the EPOC guidance:

- the Background note to the SIRIUS guidelines for completing the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR), providing background information, context and explanations necessary to understand the scope and rationale of the guidelines;
- the SIRIUS guidelines for completing the European Preservation Order Certificate (EPOC-PR).

Funded by the European Union

SIRIUS guidelines for completing the European Production Order Certificate

General guidance

- An EPOC should be **issued only if the conditions set out in the e-Evidence Regulation are fulfilled**.
- As a general rule, **JUDEX must be used for the transmission of an EPOC. Alternative means of transmission can be used only if communication through JUDEX is not possible** (e.g. owing to a lack of connection to JUDEX, technical limitations, disruption of the system, inability to reach a specific service provider through JUDEX or the nature of the transmitted material). The use of **paper-based forms or physical transmission** is limited to exceptional circumstances.
- The EPOC should be completed in a **language accepted by the addressee**.
- Ensure that the EPOC is **completed carefully and in full**. Incomplete, inconsistent or unclear information may prevent the execution of the order by the addressee or lead to requests for clarification, resulting in delays.
- If a section is not applicable, leave it blank. If transmitting the certificate other than through JUDEX, submit the whole form and do not omit any inapplicable sections.
- When completing the EPOC, ensure that the **electronic evidence requested is described in a clear, precise and unambiguous manner**, and that **sufficient identifiers** are provided to enable the addressee to identify the data.
- Particular attention should be paid to **free-text fields**. Where machine translation is used, inaccuracies may occur, especially in the description of the data requested. The use of **clear, simple and structured wording** is therefore recommended.

Under Regulation (EU) 2023/1543 of the European Parliament and of the Council the addressee of this European Production Order Certificate (EPOC) must execute this EPOC and must transmit the requested data in accordance with the deadline(s) specified in Section C of this EPOC to the competent authority indicated under point (a) of Section L of this EPOC.

In all cases, the addressee must, upon receipt of the EPOC, act expeditiously to preserve the data requested, unless the information in the EPOC does not allow it to identify those data. The data must continue to be preserved until the data are produced or until the issuing authority or, where applicable, the enforcing authority, indicates that it is no longer necessary to preserve and produce the data.

The addressee must take the necessary measures to ensure the confidentiality, secrecy and integrity of the EPOC and of the data produced or preserved.

Funded by the European Union

Section A: Issuing/validating authority

Purpose

✓ Section A identifies the authority issuing the EPOC and, where applicable, the validating authority. It also records the case reference numbers needed to ensure proper identification and case tracking.

General guidance

- This section **must always be completed**.
- You are only required to provide the issuing EU Member State, the issuing authority and, where applicable, the validating authority in Section A.
- Detailed contact and identification information (e.g. email address, telephone number) should be provided for the issuing authority in Section I and, where applicable, for the validating authority in Section J.
- Ensure the **consistency of the information provided in Sections A, I and J**.
- When using JUDEX, **verify any prefilled information** before submission.

Certificate Field	Guidance
Issuing State:	➢ Enter the **official name of the Member State** in which the order is issued. ➢ When using JUDEX, this field is prefilled based on the platform login (single sign-in).
Issuing authority:	➢ Enter the **official name of the competent authority** issuing the order. ➢ When using JUDEX, this field is prefilled based on the platform login (single sign-in).
Validating authority (where applicable:	➢ Complete this field **only if the order has been validated** pursuant to Article 4(1)(b) or Article 4(2)(b) of the e-Evidence Regulation. ➢ If the field is not applicable, leave it blank or indicate 'N/A' (not applicable) (for physical forms). ➢ Enter the **official name of the competent judicial authority** validating the order. ➢ When using JUDEX, select the validating authority from the list provided.

NB: details of issuing and validating authority to be provided at the end (Sections I and J.

Issuing State:	➢ Enter the **official name of the Member State** in which the order is issued. ➢ When using JUDEX, this field is prefilled based on the platform login (single sign-in).
File number of the issuing authority:	➢ This field is **not mandatory**, but it is **strongly recommended** that the official reference or file number assigned by the issuing authority be included. ➢ The file number provides a **clear and unique link** between the EPOC and the relevant proceedings in the issuing state. It enables the issuing authority to reliably trace the order to its case file and ensure consistency across correspondence and follow-up actions, and

Funded by the European Union

	facilitates communication with the addressee. ➢ Where multiple orders relate to the same case, including the file number helps to **facilitate continued oversight and avoid duplication of effort or confusion**.
File number of the validating authority:	➢ This field is **not mandatory**, but it is **strongly recommended** that the official reference or file number assigned by the validating authority be included, where applicable. ➢ Where provided, it serves the same purposes as the file number of the issuing authority, in particular by enabling the validating authority to **trace and manage the order effectively.**

Section B: Addressee

Purpose

✓ Section B identifies the entity to which the EPOC is addressed – the designated establishment or legal representative, or, in exceptional cases, a specified addressee. This ensures that the order reaches the correct legally responsible contact.

General guidance

➢ This section **must always be completed**.
➢ Indicate the **name and contact details of the designated establishment or legal representative**, or, in emergency cases, the specified addressee.
➢ Use the **European Court Database (CDB)**, which provides information on competent authorities / c**ourt**s, as the authoritative source for addressee information.
➢ When using JUDEX, **select the addressee from the list provided**. The CDB, linked to JUDEX, includes data regarding service providers' entity type (designated establishment or legal representative); their name; their territorial scope of designation/appointment, if a service provider is associated with several designated establishments or appoints several legal representatives; and their contact details (address/seat, phone number, email address, contact person).
➢ When not using JUDEX, some addressee data can be found in the **dedicated sections of the Judicial Library on the European Judicial Network** website.
➢ Provide information in the original language of the addressee (as included in the CDB). Do not translate names or official titles.
➢ If any contact information or the addressee's internal file number is unavailable, leave the corresponding fields blank or indicate 'Unknown' (for physical forms).

Addressee: ☐ Designated establishment ☐ Legal representative ☐ This order is issued in an emergency case to the specified addressee	➢ Enter the **full official name of the designated establishment or legal representative**, or, in emergency cases, the **specified addressee** (e.g. the parent company or a known operational contact). The latter applies only where the designated establishment or legal representative has not reacted by the deadline set in Article 10 of the e-Evidence Regulation, or has not been designated or appointed by the deadline set in Directive (EU) 2023/1544 (the e-Evidence Directive). The option of addressing the EPOC to a specified addressee is not

Funded by the European Union

because the designated establishment or the legal representative of a service provider did not react to the EPOC within the deadlines set out in Article 10 of Regulation (EU) 2023/1543 or has not been designated or appointed within the deadlines set out in Directive (EU) 2023/1544 of the European Parliament and of the Council	envisaged in Article 7 of the e-Evidence Regulation. ➢ Select the **appropriate entity type** (designated establishment or legal representative). ➢ When using JUDEX, select the addressee from the list.
Address:	➢ Provide the **complete postal address** of the addressee. ➢ Include the street name and number, city or municipality, postal code and country. ➢ When using JUDEX, this field is prefilled based on the addressee selected and data available in the CDB.
Tel. No/Fax No/email (if known):	➢ Enter the available **contact details of the addressee**. ➢ Provide the **full phone and fax numbers in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Use **official institutional email addresses** (no personal domains, such as @gmail or @yahoo) whenever possible. ➢ When using JUDEX, this field may be prefilled based on the addressee selected and data available in the CDB
Contact person (if known):	➢ Where a **specific person/entity at the addressee** is **responsible for EPOC-related matters** or relevant to the case, provide their full name and position or title. ➢ When using JUDEX, this field may be prefilled based on the addressee selected and data available in the CDB.
File number of the addressee (if known):	➢ Provide any **internal reference or case number** used by the addressee to track the case (e.g. when an EPOC has been previously issued to the addressee in the same case).
Service provider concerned (if different from addressee):	➢ If the **service provider is different from the addressee** (e.g. when the service provider concerned is not established in the EU and has appointed a legal representative in the EU), **specify the name of the service provider** (the actual natural or legal person providing the service). ➢ If the addressee is the service provider (e.g. if it is established in the EU and the designated establishment is the EU establishment, or if no separate representative is appointed), leave the field blank.

Funded by the European Union

Any other relevant information:	➢ Add **details that may assist in identifying or contacting the correct entity**, such as its preferred language of communication, or a specific point of contact or department. ➢ If the **addressee is not the designated establishment or legal representative,** briefly explain their role and relationship to the service provider and why the EPOC is addressed to them.

Funded by the European Union

Section C: Deadlines (tick the appropriate box and complete additional sections, if necessary)

Purpose

✓ Section C specifies the deadlines by which the addressee must respond to the EPOC and produce the requested data. It ensures that the addressee is clearly informed of the applicable legally binding time frame and enables the issuing authority to monitor timely execution.

General guidance

- **Complete** this section by selecting the applicable **deadline for the execution of the EPOC**. If this section is left blank, the default deadline of 10 days applies, as set out in the e-Evidence Regulation.
- Before selecting the deadline, **assess** if the case is an **emergency**, as defined in Article 3(18) of the e-Evidence Regulation, and whether the enforcing authority needs to be **notified**.
- **Issue the EPOC as soon as possible.**

Upon receipt of the EPOC, the data requested must be produced	➢ Tick **only one** of the options below, selecting the applicable deadline
☐ as soon as possible and at the latest within 10 days (no notification to the enforcing authority)	➢ Select this option if the enforcing authority **does not need to be notified**. ➢ The data must be produced **as soon as possible and no later than 10 days** after receipt of the EPOC.
☐ in the case of notification to the enforcing authority: at the end of the 10 days, where the enforcing authority has not raised a ground for refusal within that time period, or upon confirmation by the enforcing authority before the end of the 10 days that it will not raise a ground for refusal, as soon as possible and at the latest at the end of the 10 days	➢ Select this option if the enforcing authority **needs to be notified** under Article 8 of the e-Evidence Regulation. ➢ The data may be produced: • at the end of the 10-day period, unless a ground for refusal has been raised; • earlier, but only if the enforcing authority confirms that no ground for refusal will be raised. ➢ If no such confirmation is received, the addressee must wait until after the 10-day period to produce the data.
☐ without undue delay and at the latest within eight hours in an emergency case involving: ☐ an imminent threat to the life,	➢ Select this option (‘**emergency deadline**’) in **emergency cases** involving an imminent threat to the life, physical integrity or safety of a person and/or an imminent threat to critical infrastructure, as defined by Council Directive 2008/114/EC. ➢ If applicable, both emergency situations may be ticked. ➢ The data must be produced **without undue delay and at**

Funded by the European Union

physical integrity or safety of a person ☐ an imminent threat to a critical infrastructure as defined in Article 2, point (a), of Council Directive 2008/114/EC, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core functions of the State.	**the latest within eight hours** of the receipt of the EPOC. ➢ Justify labelling the case as an emergency in the 'additional information' field below.
Please indicate whether there are any procedural or other deadlines which should be taken into account for the execution of this EPOC:	➢ Complete this field only if **additional deadlines** relevant to the execution of the EPOC are set (e.g. national procedural deadlines). ➢ These deadlines **do not replace or modify the deadlines set out in Article 10 of the e-Evidence Regulation** (10 days or 8 hours), but may be taken into account by the addressee for prioritisation. ➢ Insert date(s) using the format **DD/MM/YYYY**. ➢ Describe the **reason(s) for each deadline**, such as: • the suspect or accused is in custody; • the trial date of the accused is imminent; • a preservation order is close to expiring; • a statute of limitations is about to expire; • execution of the EPOC must be coordinated with other national or cross-border measures. ➢ Where multiple deadlines apply, explain each separately.

Funded by the European Union

Please provide additional information where relevant:	➢ Provide any **relevant contextual information** not already included above, such as: • justify labelling the case as an emergency, specifying the nature and timing of the threat and how access to the data requested will help to address it; • clarifications regarding coordination with other authorities or orders.

Funded by the European Union

Section D: Relation to a previous production/preservation request (tick and complete if applicable and information is available)

Purpose

✓ Section D indicates whether the EPOC relates to a previous production or preservation request. It enables the addressee and authorities to link the current order to earlier requests, avoiding the duplication of efforts and ensuring continuity in handling the same or related data.

General guidance

- Complete this section only **where applicable** and if the relevant information is **available**. If the section is not applicable, do not delete it – leave it blank or indicate 'N/A' (for physical forms).
- Do not leave the section blank if a **preservation or production request** has already been issued in relation to the data requested in this EPOC.
- Use **precise dates and reference numbers** to enable the addressee to identify and link related records efficiently.
- When using JUDEX, previously issued EPOC or EPOC-PR instruments registered in the system can be selected and linked to the current EPOC. This will automatically populate relevant fields (e.g. issuing authority, date of transmission), reducing administrative burden and the risk of errors.

☐ The requested data were totally/partially preserved in accordance with an earlier request for preservation	➢ Tick this box if the **service provider has already been asked to preserve** all or some of the data concerned. ➢ When using JUDEX, select EPOC-PR from the 'Instrument' drop-down menu.
issued by … (indicate the authority and the file number)	➢ Enter the **official name of the issuing authority** that made the preservation request. ➢ When using JUDEX, select the authority from the list provided if not prefilled. ➢ Provide the internal reference or file number of that request.
on … (indicate the date of issuance of the request)	➢ Enter the **date** on which **the preservation request was officially issued**. ➢ Use the format **DD/MM/YYYY**.
and transmitted on … (indicate the date of transmission of the request)	➢ Enter the **date** on which **the preservation request was officially transmitted**. ➢ Use the format **DD/MM/YYYY**.
to … (indicate the service provider/ legal representative/ designated establishment/competent	➢ Enter the **name of the addressee** and, if applicable, the official name of the competent authority to which the preservation request was transmitted. ➢ If available, include the **internal reference or file number** used by the addressee.

Funded by the European Union

authority to which the request was transmitted and, if available, the file number given by the addressee).	➢ When using JUDEX, select the addressee and authority from the lists provided if not prefilled
☐ The requested data are related to an earlier request for production	➢ Tick this box if the same **service provider has already been asked to produce** all or some of the data concerned (e.g. reissued EPOC due to the case now being considered an emergency case under the e-Evidence Regulation or updated legal grounds), or if an earlier EPOC was issued for the same account but for different data categories or datasets (e.g. if the previous EPOC was issued only for subscriber data, while the current EPOC requests traffic or content data). ➢ When using JUDEX, select EPOC from the 'Instrument' drop-down menu.
issued by … (indicate the authority and the file number)	➢ Enter the **official name of the issuing authority** that made the production request. ➢ When using JUDEX, select the authority from the list provided if not prefilled. ➢ Provide the internal reference or file number of the previous request.
on … (indicate the date of issuance of the request)	➢ Enter the **date** on which **the production request was officially issued**. ➢ Use the format **DD/MM/YYYY**.
and transmitted on (indicate the date of transmission of the request)	➢ Enter the **date** on which **the production request was officially transmitted**. ➢ Use the format **DD/MM/YYYY**.
to … (indicate the service provider/ legal representative/ designated establishment/competent authority to which it was transmitted and, if available, the file number given by the addressee).	➢ Enter the **name of the addressee** and, if applicable, the official name of the competent authority to which the production request was transmitted. ➢ If available, include the **internal reference or file number** used by the addressee. ➢ When using JUDEX, select the addressee and authority from the lists provided if not prefilled.
Any other relevant information:	➢ Use this field to **clarify the relationship between the current and the previous request**. ➢ Indicate the status of the earlier request, where known (e.g. fully executed, partially executed, refused, pending). ➢ Indicate if preserved data are close to expiry (e.g. approaching the 60-day preservation deadline). ➢ Where relevant, **refer to related instruments**, such as: • voluntary cooperation requests; • emergency disclosure requests; • European investigation orders; • requests for mutual legal assistance; • requests for expedited preservation of stored computer data through the 24/7 Network under the

Funded by the European Union

	Budapest Convention; • other requests issued in the same case. ➢ This field may also be used to indicate whether parallel EPOCs have been sent to multiple addressees concerning the same service provider in the same or different Member States.

Funded by the European Union

Section E: Information to support the identification of requested data (complete based on the information that is known and to the extent necessary to identify the data)

Purpose

- ✓ Section E provides the key information that enables the service provider to accurately identify the data requested in the EPOC. Providing precise and complete identifiers helps to prevent errors, delays or the disclosure of unrelated data, and ensures efficient, lawful and proportionate execution of the order.

General guidance

- ➢ This section **must always be completed** (**at least one identifier** must be provided).
- ➢ When using JUDEX, select the appropriate type of identifier from the drop-down menu (available options include Internet Protocol (IP) address version 4 (IPv4); IP address version 6 (IPv6); IP address range; IP blocks; email address; telephone number; International Mobile Equipment Identity (IMEI) number; Media Access Control (MAC) address; the user or another unique identifier, such as a username, login ID or account name; and other) and provide the identifier itself.
- ➢ If more than one user or account is concerned, provide the **identifier type and the identifier itself for each**.
- ➢ When using JUDEX, select 'Add another identifier' to add additional users or accounts.
- ➢ When not using JUDEX, number each identifier and ensure that the numbering corresponds to the information provided in Section F.
- ➢ Where necessary, combine multiple identifiers to ensure that the data requested can be accurately identified (e.g. account name together with a telephone number or IP address).
- ➢ **Double-check all entries.** Incomplete or incorrect identifiers may result in delays, refusals or the production of incorrect data.
- ➢ Note that service providers may use **specific identifiers** for each of their services.
- ➢ The **CDB** provides **information on services** covered by the e-Evidence Directive for each service provider and may also include **identifiers linked to those services** (service providers may submit this additional information on a voluntary basis).
- ➢ The **SIRIUS platform** provides practical guidance on more than 80 service providers, including examples of valid identifiers.

IP address(es) and timestamps (incl. date and time zone):	➢ Provide the **full IP address(es)** (IPv4 or IPv6) together with the **precise timestamp** (date and time). ➢ Use the format **DD/MM/YYYY** to report the date, **and clearly specify the time and the time zone used** (e.g. 15/09/2025, 13:45 Coordinated Universal Time (UTC)).
Tel No:	➢ Provide the **full phone number in international format**, including the country code (e.g. +31 XX XXX XXXX).
Email address(es):	➢ Provide the **complete email address(es)**.
IMEI number(s):	➢ Provide the **full IMEI number(s)**, identifying the physical mobile device used to access the service.

Funded by the European Union

MAC address(es):	➢ Provide the **complete MAC address(es)**, identifying the specific hardware used to access the service.
The user(s) or other unique identifier(s) such as user name(s), login ID(s) or account name(s):	➢ Provide any **unique identifiers not listed above**.
Name(s) of the relevant service(s):	➢ **Specify the service** concerned (e.g. platform or application name). ➢ This information is **essential for service providers offering multiple services**, as it enables accurate and timely processing of the EPOC.
Other:	➢ Provide any **additional technical or account identifiers**. These may include: • account recovery details (e.g. a recovery phone number or email address); • subscriber identifiers (e.g. International Mobile Subscriber Identity (IMSI), Integrated Circuit Card Identifier); • payment details linked to an account (e.g. credit card details (first six and last four digits together with a transaction date, amount and expiry date)); • vehicle identifiers (e.g. licence plate numbers); • internal user or device IDs utilised by the service provider; • registrar identifiers (e.g. registrar name, Internet Assigned Numbers Authority ID, reseller name, associated account or ticket number); • domain-related identifiers (e.g. domain name; registry domain ID; server name; dates of registration, update and expiry).
If applicable, the time range of the data for which production is requested:	➢ Provide the **time frame for any data with a temporal component** and specify the identifier to which the frame relates. ➢ Specify **start and end dates**, including the **time zone**. ➢ Use the format: • **start date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 15/09/2025, 13:45 UTC); • **end date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 18/09/2025, 13:45 UTC). ➢ **Be realistic and proportionate.** Excessively broad time frames may lead to delays, legal challenges or practical difficulties due to the volume of data requested.
Additional information if needed:	➢ Provide any **contextual or clarifying information** that may assist the addressee in identifying the data requested, such as: • links between multiple accounts; • specific features or usage patterns of the service. ➢ When using JUDEX, use this field to explain, if applicable,

Funded by the European Union

	that multiple identifiers relate to the same user or account to ensure the accurate identification of the data requested. ➢ Avoid repeating information already provided in this section.

Funded by the European Union

Section F: Electronic evidence to be produced

Purpose

✓ Section F specifies the electronic evidence that the addressee is required to produce in response to the EPOC. Clearly identifying the data requested ensures that the addressee can deliver the correct information promptly, accurately and in compliance with applicable legal safeguards.

General guidance

- This section **must always be completed** (**at least one data category and corresponding dataset** (subcategory) must be selected).
- Tick **only the box(es) strictly necessary** for the case. Avoid using vague terms such as 'all data' or 'all content'.
- **Be realistic and proportionate in terms of scope and time frame.** Excessively broad requests may lead to delays, legal challenges or practical difficulties due to the volume of data requested and limitations of data transfer methods.
- The predefined subcategories may not fully correspond to the data held by the service provider. Use the 'Other' field only where necessary and describe the data requested clearly to avoid ambiguity.
- **Certain types of data may fall under different data categories** depending on the **service provider**, based on the nature of the data in relation to the services provided. For example, a date of birth, albeit usually considered subscriber data, could be considered content data for a service when the data go beyond the identification of the user / subscription holder.
- Keep in mind that requests involving traffic or content data may involve additional legal considerations or notification requirements.
- When using JUDEX, subscriber and identification data (points (ab), respectively) cannot be combined with traffic or content data (points (c) and (d), respectively) in a single EPOC (only points (a) and (b) or (c) and (d) should be filled out). When data from both groups are being requested, separate EPOCs must be issued and a clear indication given in Section D. If data are requested for multiple users or accounts in Section E, Section F must be completed separately for each user or account, including at least one data category and the corresponding dataset for each user or account.
- When not using JUDEX, if data are requested for multiple users or accounts, ensure that the information regarding the data requested corresponds to the identifiers provided for each user or account in Section E. Section F must clearly specify, for each individual user or account, at least one data category and the corresponding dataset.
- **Cross-check all dates and time frames** for consistency with Section E.
- Ensure that the EPOC seeks data that can actually be sought from this service provider.
- The CDB may contain information on the types of data available for each service, including the data (sub)categories and retention periods. Service providers may submit this additional information on a voluntary basis.
- The **SIRIUS platform** provides practical guidance on more than 80 service providers, including information on how some of these providers categorise data.

This EPOC concerns (tick the relevant box(es)): (a) ☐ subscriber data: ☐ name, date of birth, postal or	• Specify any **additional relevant subscriber data or identifiers** (e.g. account recovery keys). • **For registries and registrars**, this may include registrant name, contact details, technical and administrative contacts, dates of domain creation

Funded by the European Union

geographic address, contact information (email address, phone number) and other relevant information pertaining to the identity of the user/subscription holder ☐ date and time of initial registration, type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber ☐ type of service and its duration, including identifier(s) used by or provided to the subscriber at the moment of initial registration or activation (e.g. phone number, SIM-card number, MAC address) and associated device(s) ☐ profile information (e.g. user name, screen name, profile photo) ☐ data on the validation of the use of service,	and updating, status, server name, billing information and abuse contact information. • **Be specific and concise**.

Funded by the European Union

such as an alternative email address provided by the user/subscription holder ☐ debit or credit card information (provided by the user for billing purposes), including other means of payment ☐ PUK-codes ☐ other:	
(b) ☐ data requested for the sole purpose of identifying the user as defined in Article 3, point (10), of Regulation (EU) 2023/1543: ☐ IP connection records such as IP addresses / logs / access numbers together with other technical identifiers, such as source ports and time stamps or equivalent, the user ID and the interface used in the context of the use of the service, please specify, if necessary: ☐ time range of the data for which production is requested (if different from Section E):	➢ Provide the time frame only if it differs from that specified in Section E. ➢ Use the format: • **start date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 15/09/2025, 13:45 UTC); • **end date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 18/09/2025, 13:45 UTC).
☐ other:	

Funded by the European Union

(c) ☐ traffic data: (i) for (mobile) telephony: ☐ outgoing (A) and incoming (B) identifiers (phone number, IMSI, IMEI) ☐ time and duration of connection(s) ☐ call attempt(s) ☐ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection ☐ bearer / teleservice used (e.g. UMTS, GPRS) ☐ other:	➢ Specify any **additional relevant telephony traffic data** (e.g. call-forwarding settings, roaming indicators). ➢ **Be specific and concise.**
ii) for internet: ☐ routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID) ☐ base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection(s) ☐ volume of data ☐ date and time of connection(s)	

Funded by the European Union

☐ duration of connection or access session(s) ☐ other:	
(Specify any **additional relevant internet traffic data** (e.g. language preferences).	➢ **Be specific and concise.**
(iii) for hosting: ☐ logfiles ☐ tickets ☐ other:	➢ Specify any **additional relevant hosting-related traffic data** (e.g. administrative notes, access tokens, back-end logs). ➢ **Be specific and concise.**
(iv) other: ☐ purchase history ☐ prepaid balance charging history ☐ other:	➢ Specify any **additional relevant traffic data** (e.g. login rewards history). ➢ **Be specific and concise.**
(d) ☐ content data: ☐ (web)mailbox dump ☐ online storage dump (user-generated data) ☐ pagedump ☐ message log/backup ☐ voicemail dump ☐ server contents ☐ device backup ☐ contact list ☐ other:	➢ Specify any **additional relevant content data** (e.g. calendar entries, drafts folder). ➢ **Be specific and concise.**
☐ Additional information in case necessary to (further) specify or limit the range of the requested data:	➢ Use this field to **refine, limit or clarify** the scope of the data requested. ➢ Do not repeat information already provided in the section. ➢ Where relevant, specify the time frame and time zone using the format: • **start date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 15/09/2025, 13:45 UTC); • **end date (DD/MM/YYYY), clearly specifying the time and the time zone used** (e.g. 18/09/2025, 13:45 UTC).

Funded by the European Union

Section G: Information on the underlying conditions

Purpose

✓ Section G sets out the legal and factual conditions underlying the issuance of the EPOC. It ensures that the addressee understands the legal basis, the type of offence or proceedings concerned and any conditions relevant to the validity and execution of the EPOC.

General guidance

➢ This section **must always be completed**.
➢ If the EPOC covers multiple data categories, ensure that the applicable legal conditions and procedural requirements (e.g. notification of the enforcing authority) are fulfilled for each category.

(a) This EPOC concerns (tick the relevant box(es)):	➢ One or both boxes may be ticked, depending on the context. Provide any supporting details under point (e).
☐ criminal proceedings in respect of a criminal offence(s);	➢ Select this option if the EPOC relates to the investigation or prosecution of a criminal offence.
☐ execution of a custodial sentence or a detention order of at least four months following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.	➢ Select this option if the EPOC relates to the enforcement of a custodial sentence or detention order of at least four months, imposed following criminal proceedings not in absentia, where the convicted person has absconded.
(b) Nature and legal classification of the offence(s) in relation to which the EPOC is issued and the applicable statutory provision:	➢ Specify the **legal classification of the offence(s)** and cite the **relevant statutory provisions** under national law. ➢ Use the **official offence title(s) and precise legal references**. ➢ Briefly describe the nature of the offence(s). ➢ Include **definitions of key legal or technical terms** where necessary. ➢ Ensure consistency between the offence(s) described here and the selections made under point (c). ➢ When the EPOC relates to the execution of a custodial sentence or detention order, indicate (in points (b) and (c), where applicable) the offence(s) for which the sentence was imposed. ➢ Avoid reproducing full legal provisions unless strictly necessary. ➢ Example: 'Computer fraud under Article 298(1) of the Criminal Code (maximum sentence: five years). Offence

Funded by the European Union

	committed through a phishing attack targeting an online banking service.'
(c) This EPOC is issued for traffic data which are not requested for the sole purpose of identifying the user, or for content data, or both, and concerns (tick the relevant box(es), if applicable):	➢ **Complete** this part only **if requesting traffic data not solely for user identification, and/or content data**. ➢ Tick the relevant box(es) and ensure consistency with point (b).
☐ criminal offence(s) punishable in the issuing State by a custodial sentence of a maximum of at least three years;	➢ Select this option if the minimum sentence threshold (three years) is met under national law.
☐ one or more of the following offences, if wholly or partly committed by means of an information system:	➢ Select this option if the minimum sentence threshold is not met but the offence (or offences) was (or were) committed by means of an information system and falls under one of the specific categories of offence below as per the issuing Member States' criminal law.
☐ offence(s) as defined in Articles 3 to 8 of Directive (EU) 2019/713 of the European Parliament and of the Council;	➢ Select this option if any of the following criminal offences in the area of fraud and counterfeiting of non-cash means of payment, as defined in Directive (EU) 2019/713, have been committed: • fraudulent use of non-cash payment instruments (Article 3), • fraudulent use of corporeal non-cash payment instruments (Article 4), • fraudulent use of non-corporeal non-cash payment instruments (Article 5), • fraud related to information systems (Article 6), • facilitation of the use of tools to commit the above offences (Article 7), • incitement, aiding and abetting, and attempt (Article 8) in relation to the above offences.
☐ offence(s) as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council;	➢ Select this option if any of the following criminal offences in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes, as defined in Directive 2011/93/EU, have been committed: • offences concerning sexual abuse (Article 3), • offences concerning sexual exploitation (Article 4), • offences concerning child pornography (Article 5), • solicitation of children for sexual purposes (Article 6), • incitement, aiding and abetting, and attempt (Article 7) in relation to the above offences.

Funded by the European Union

offence(s) as defined in Articles 3 to 8 of Directive 2013/40/EU of the European Parliament and of the Council;	➢ Select this option any of the following criminal offences in the area of attacks against information systems, as defined in Directive 2013/40/EU, have been committed: • illegal access to information systems (Article 3), • illegal system interference (Article 4), • illegal data interference (Article 5), • illegal interception (Article 6), • facilitation of the use of tools to commit the above offences (Article 7), • incitement, aiding and abetting, and attempt (Article 8) in relation to above offences.
☐ criminal offences as defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council.	➢ Select this option if any of the following criminal offences in the area of terrorist offences, offences related to a terrorist group and offences related to terrorist activities, as defined in Directive (EU) 2017/541, have been committed: • terrorist offences (Article 3), • offences relating to a terrorist group (Article 4), • public provocation to commit a terrorist offence (Article 5), • recruitment for terrorism (Article 6), • provision of training to perform or help conduct acts of terrorism (Article 7), • receipt of training to perform or help conduct acts of terrorism (Article 8), • travelling for the purpose of terrorism (Article 9), • organising or otherwise facilitating travelling for the purpose of terrorism (Article 10), • terrorist financing (Article 11), • other offences related to terrorist activities (Article 12), • aiding and abetting, inciting and attempting (Article 14) in relation to the above offences.
(d) Controller/processor: European Production Orders shall be addressed to service providers acting as controllers. By way of exception, the European Production Order may be addressed directly to the service provider that processes the data on behalf of the controller.	➢ As a general rule, **address the EPOC to the service provider, acting as the controller** (i.e. the entity determining the purposes and means of processing the personal data requested). ➢ **Complete** this part only **if the EPOC is directly addressed to a service provider that stores or otherwise processes the data on behalf of the controller**. ➢ Identify the correct controller for the user concerned. Note that service providers may have multiple entities acting as controllers depending on the service or jurisdiction. ➢ Where the data requested relate to a service provider (e.g. a company, an academic institution) using another service provider to store electronic communications or other records, the EPOC should normally be addressed to the former service provider, as the controller.

Funded by the European Union

	➢ A service provider storing or processing data on behalf of the controller (e.g. cloud service provider) is typically acting as a **processor**. ➢ **Address the EPOC to a processor only in exceptional cases**, where the controller cannot be identified despite reasonable efforts (e.g. if you would need to interpret very complex contractual frameworks providing, in a specific case, for the allocation of different tasks and roles with regard to a particular set of data to various service providers) or if addressing the controller could be detrimental to the investigation (e.g. because the controller is a suspect or an accused or convicted person or there are indications that the controller could be acting in the interest of the person that is the subject of the investigation). ➢ Maintain a record of the reasons for addressing the EPOC to a processor in the case file. ➢ Where relevant, coordinate parallel or related requests involving multiple jurisdictions through the **European Union Agency for Criminal Justice Cooperation** to avoid giving conflicting instructions, in particular when the processor is requested not to inform the controller about the production of data.
Tick where appropriate:	➢ Tick only one of the boxes.
☐ This EPOC is addressed to the service provider acting as controller.	➢ Select this option if the EPOC is addressed to the service provider acting as the controller.
☐ This EPOC is addressed to the service provider who is or, in the case of situations where the controller cannot be identified, is possibly processing the data on behalf of the controller, because: ☐ the controller cannot be identified despite reasonable efforts on the part of the issuing authority ☐ addressing the controller might be detrimental to the investigation	➢ Select this option if the EPOC is addressed to the service provider acting as the processor. ➢ Select one of the two reasons below for addressing the EPOC to the processor. ➢ Provide further explanation under point (e), where applicable.

Funded by the European Union

If this EPOC is addressed to the service provider processing data on behalf of the controller:	➢ Complete this part only if the EPOC is addressed to a processor. ➢ Tick only one of the boxes.
☐ the processor shall inform the controller about the data production	➢ Select this option if the processor should inform the controller that they are providing data.
☐ the processor shall not inform the controller about the data production until further notice, as it would be detrimental to the investigation. Please provide a short justification:	➢ Select this option if the processor is requested to refrain from informing the controller about the production of data, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings. ➢ Provide a short justification (e.g. risk of data being deleted or suspect being alerted). ➢ Maintain a record of the reasons in the case file.
☐ (e) Any other relevant information:	➢ Provide any contextual information necessary to explain or justify the choices made in this section. ➢ Include, where relevant, explanations of sensitivities (e.g. involvement of the controller in the investigation).

Funded by the European Union

Section H: Information for the user

Purpose

✓ Section H indicates whether the issuing authority will delay informing the person whose data are requested about the provision of those data. It ensures that the addressee understands that the issuing authority remains responsible for notifying the person concerned and that any delay complies with the legal conditions set out in the e-Evidence Regulation.

General guidance

- Complete this section only **if the issuing authority decides to delay informing the user** about the production of data.
- Ensure that any delay complies with the applicable legal conditions and is necessary and proportionate.
- Where several EPOCs concerning the same user are pending or envisaged, ensure consistency across all orders regarding any delays in notification. Where other authorities are involved (in particular in other Member States), inform them of the existence and duration of any delays to prevent inadvertent or premature disclosure of data.
- Where relevant, coordinate parallel or related requests involving multiple jurisdictions through the **European Union Agency for Criminal Justice Cooperation** to avoid implementing conflicting measures or unintentionally notifying users.

The addressee shall in any event refrain from informing the person whose data are being requested. It is the responsibility of the issuing authority to inform that person, without undue delay, about the data production. Please note that (tick where appropriate):	➢ If the issuing authority decides to delay informing the person concerned, tick the corresponding box and **select all applicable legal grounds justifying the delay**. ➢ Multiple grounds may be selected where relevant. ➢ Maintain a record of the justification for any delay in the case file, for the purpose of review or challenge. ➢ Ensure that the person concerned is informed without undue delay once those conditions no longer apply.
☐ the issuing authority will delay informing the person whose data are being requested, for as long as one or several of the following conditions are met: ☐ it is necessary to avoid obstructing official or legal inquiries, investigations or procedures; ☐ it is necessary to avoid prejudicing the prevention, detection, investigation or	

Funded by the European Union

prosecution of criminal offences or the execution of criminal penalties; ☐ it is necessary to protect public security; ☐ it is necessary to protect national security; ☐ it is necessary to protect the rights and freedoms of others.	

Funded by the European Union

Section I: Details of the issuing authority

Purpose

✓ Section I provides the identification and contact details of the issuing authority. It enables the addressee and any enforcing authority to verify the origin and authenticity of the EPOC, establish secure communication and ensure proper execution and follow-up.

General guidance

➢ This section **must always be completed** (including at least the name of the issuing authority).
➢ When using JUDEX, the information on the issuing authority and the file number provided in Section A is automatically copied to this section.
➢ When not using JUDEX, ensure consistency with the information provided for the issuing authority in Section A.
➢ Provide accurate and up-to-date contact details to facilitate communication, particularly in urgent cases.

The type of issuing authority (tick the relevant box/boxes): ☐ judge, court, or investigating judge ☐ public prosecutor ☐ other competent authority as defined by the issuing State	➢ Select the appropriate authority type in accordance with national law.
If validation is necessary, please fill in also Section J.	
Please note that (tick if applicable):	➢ Tick this option (regarding **emergency issuance without prior validation**) only if the EPOC concerns subscriber data or data requested solely for the purpose of identifying the user, in a validly established emergency. ➢ All the following conditions must be met: • immediate action is necessary due to an imminent threat, as set out in Article 3(18) of the e-Evidence Regulation; • prior validation could not be obtained in time; • the issuing authority could issue such an order in a comparable domestic case without prior validation. ➢ Maintain a record of justification in the case file. ➢ Seek *ex post* validation within 48 hours.
☐ This EPOC was issued for subscriber data, or for data requested for the sole purpose of	

Funded by the European Union

identifying the user, in a validly established emergency case without prior validation, because the validation could not have been obtained in time, or both. The issuing authority confirms that it could issue an order in a similar domestic case without validation, and that *ex post* validation will be sought without undue delay, at the latest within 48 hours (please note that the addressee will not be informed).	
Details of the issuing authority, or its representative, or both, certifying the contents of the EPOC as accurate and correct:	➢ When using JUDEX, certain fields may be prefilled based on the platform login (single sign-in). ➢ Where possible, provide **contact details of a representative familiar with the case** and able to communicate in a relevant language. ➢ If any contact information or the file number is unavailable, leave the corresponding fields blank or specify that the information is 'Unknown' (for physical forms).
Name of authority:	➢ Provide the **official name of the competent authority issuing the EPOC**.
Name of its representative:	➢ Provide the **name of the judge or prosecutor, or the name or personal identification number** (for law enforcement personnel) **of the official signing the EPOC**.
Post held (title/grade):	➢ Indicate the **title or rank** of the person signing the EPOC (e.g. judge, public prosecutor, senior investigating officer).
File number:	➢ This field is **not mandatory**, but it is **strongly recommended** that the official reference or file number assigned by the issuing authority be included. ➢ The file number provides a **clear and unique link** between the EPOC and the relevant proceedings in the issuing Member State. It enables the issuing authority to

Funded by the European Union

	reliably trace the order to its case file and ensure consistency across correspondence and follow-up actions, and facilitates communication with the addressee.
Address:	➢ Provide the **complete postal address** of the issuing authority. ➢ Include the street name and number, city or municipality, postal code and country.
Tel. No: (country code) (area/city code):	➢ Provide the **full phone number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the issuing authority and/or its representative can be **reached 24/7** or provide an alternative contact point.
Fax No: (country code) (area/city code):	➢ Provide the **full fax number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the issuing authority and/or its representative can be **reached 24/7** or provide an alternative contact point.
Email:	➢ Use an **official institutional email address** (no personal domains such as @gmail or @yahoo). ➢ Ensure that the mailbox is regularly monitored.
Language(s) spoken:	➢ Indicate the **languages in which the issuing authority and/or its representative can communicate**.
If different from above, authority/contact point (e.g. central authority) which can be contacted for any question related to the execution of the EPOC:	➢ Where necessary, provide **contact details of another authority or contact point** that can answer follow-up questions. ➢ Where possible, indicate a **person familiar with the case** who is easily **reachable** and **able to communicate** in a relevant language. ➢ Apply the same requirements for contact details as previously set out in this section. ➢ If any contact information is unavailable, leave the corresponding fields blank or specify that the information is 'Unknown' (for physical forms).
Name of the authority/name:	
Address:	
Tel. No: (country code) (area/city code):	
Fax No: (country code) (area/city code):	
Email:	
Signature of the issuing authority or its representative certifying the content of the EPOC as accurate and correct:	

Funded by the European Union

Date:	➢ Provide the **date of signature** in the format **DD/MM/YYYY**.
Signature:	➢ Sign the EPOC using a **qualified electronic signature**, as defined in Regulation (EU) No 910/2014. ➢ When not using JUDEX, also add an official stamp, electronic seal or equivalent form of authentication. ➢ When signing the certificate manually, use black or blue ink.

Funded by the European Union

Section J: Details of the validating authority (complete if applicable)

Purpose

✓ Section J provides the identification and contact details of the validating authority. It enables the addressee and any enforcing authority to verify the origin and authenticity of the validation, establish secure communication and ensure proper execution and follow-up.

General guidance

➢ **Complete** this section only **if validation is required**. In this case, information on the validating authority (at least its official name) must be provided. If the section is not applicable, do not delete it – leave it blank (for physical forms).
➢ When using JUDEX, the information on the validating authority and the file number provided in Section A is automatically copied to this section.
➢ When not using JUDEX, ensure consistency with the information provided about the validating authority in Section A.
➢ Provide accurate and up-to-date contact details to facilitate communication, particularly in urgent cases.

The type of validating authority: ☐ judge, court or investigating judge ☐ public prosecutor	➢ Select the appropriate authority type in accordance with national law.
Details of the validating authority, or its representative, or both, certifying the contents of the EPOC as accurate and correct:	➢ When using JUDEX, certain fields may be prefilled based on the platform login (single sign-in). ➢ Where possible, provide **contact details of a representative familiar with the case** and able to communicate in a relevant language. ➢ If any contact information or the file number is unavailable, leave the corresponding fields blank or indicate 'Unknown' (for physical forms).
Name of the authority:	➢ Provide the **official name of the competent authority validating the EPOC**.
Name of its representative:	➢ Provide the **name of the judge or prosecutor signing the EPOC**.
Post held (title/grade):	➢ Indicate the **title** of the person signing the EPOC (judge or public prosecutor).

Funded by the European Union

File number:	➢ This field is **not mandatory**, but it is **strongly recommended** that the official reference or file number assigned by the validating authority be included here. ➢ The file number provides a **clear and unique link** between the EPOC and the relevant proceedings in the issuing Member State. It enables the issuing authority to reliably trace the order to its case file and ensure consistency across correspondence and follow-up actions, and facilitates communication with the addressee.
Address:	➢ Provide the **complete postal address** of the validating authority. ➢ Include the street name and number, city or municipality, postal code and country.
Tel. No: (country code) (area/city code).	➢ Provide the **full phone number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the validating authority and/or its representative can be **reached 24/7** or provide an alternative contact point.
Fax No: (country code) (area/city code):	➢ Provide the **full fax number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the validating authority and/or its representative can be **reached 24/7** or provide an alternative contact point.
Email:	➢ Use an **official institutional email address** (no personal domains, such as @gmail or @yahoo). ➢ Ensure that the mailbox is regularly monitored
Language(s) spoken:	➢ Indicate the **languages in which the validating authority and/or its representative can communicate.**
Date:	➢ Provide the **date of signature** in the format **DD/MM/YYYY**.
Signature:	➢ Sign the EPOC using a **qualified electronic signature**, as defined in Regulation (EU) No 910/2014. ➢ When not using JUDEX, also add an official stamp, electronic seal or equivalent form of authentication. ➢ When signing manually, use black or blue ink.

Funded by the European Union

Section K: Notification and details of the enforcing authority (if applicable)

Purpose

✓ Section K provides the identification and contact details of the enforcing authority notified of the EPOC. It informs the addressee of the notification and facilitates coordination, follow-up and communication between the issuing authority, the enforcing authority and the addressee.

General guidance

- **Complete** this section only **if an enforcing authority is notified**. In this case, also complete Section M. If the section is not applicable, do not delete it – leave it blank or indicate 'N/A' (for physical forms).
- **Carefully assess whether notification is necessary.** Unnecessary notification may delay the execution of the EPOC.
- Notification is required if the EPOC concerns traffic data not requested solely for the purpose of user identification and/or content data, unless the issuing authority has reasonable grounds to believe that both of the following conditions are met at the time of issuing the EPOC:
  - the offence has been committed, is being committed or is likely to be committed in the issuing state;
  - the person whose data are requested resides in the issuing state.

☐ This EPOC is notified to the following enforcing authority:	➢ Provide the **official name of the notified enforcing authority**. ➢ When using JUDEX, select the enforcing authority from the list provided. ➢ When not using JUDEX, **information on competent authorities** can be found in the **dedicated section of the Judicial Library on the European Judicial Network** website.
Please provide contact details of the notified enforcing authority (if available):	➢ Provide any **available contact details** of the enforcing authority. ➢ When using JUDEX, these fields may be prefilled based on the authority selected. ➢ If any contact information is unavailable, leave the corresponding fields blank or indicate that the information is 'Unknown' (for physical forms).
Name of the enforcing authority:	➢ Provide the **official name of the enforcing authority.**
Address:	➢ Provide the **complete postal address** of the enforcing authority. ➢ Include the street name and number, city or municipality, postal code and country.

Funded by the European Union

Tel. No: (country code) (area/city code).	➢ Provide the **full phone number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the enforcing authority can be **reached 24/7**.
Fax No: (country code) (area/city code).	➢ Provide the **full fax number in international format**, including the country code (e.g. +31 XX XXX XXXX). ➢ Where possible, indicate a number at which the enforcing authority can be **reached 24/7.**
Email:	➢ Use an **official institutional email address** (no personal domains, such as @gmail or @yahoo).

Funded by the European Union

Section L: Transfer of data

Purpose

Section L specifies the authority to which the data requested must be transferred and any preferred format or means of transmission. It ensures that the data are delivered to the correct authority efficiently, securely and in accordance with applicable procedural requirements.

General guidance

- Complete this section where:
  - the **data requested are to be transmitted to an authority other than the issuing authority**; and/or
  - **alternative means of data transfer (to JUDEX) are to be used**.
- As a general rule, **data requested through the EPOC should be transmitted through JUDEX**, provided that the total size of a single transfer does not exceed **25 megabytes**.
- Use an **alternative means of transfer only if data cannot be transmitted through JUDEX**. This may, in particular, be due to:
  - technical limitations (e.g. file size exceeding 25 megabytes or causing disproportionate delays);
  - the nature of the transmitted material (e.g. if data are stored on physical media and their extraction or transfer by electronic means is not appropriate or not technically feasible, or may pose a risk to data integrity);
  - disruption to or unavailability of JUDEX;
  - forensic requirements applicable to the data requested;
  - other exceptional circumstances.

In such cases, select **the most appropriate alternative means available**.

- Any alternative method must ensure that the **transfer remains swift, secure and reliable**. It must also be **possible for the recipient to establish the authenticity and integrity of the transmitted data**. The e-Evidence Regulation remains otherwise applicable, and any alternative means have to respect the other provisions of the regulation, without modifying workflows (e.g. an alternative means for transmitting an EPOC to a service provider does not cover a transmission channel involving an authority in the enforcing state).
- **The most appropriate alternative means of communication should be determined on a case-by-case basis**, taking into account the following circumstances:
  - the nature, format and volume of the data requested;
  - technical interoperability;
  - the required level of security;
  - speed and reliability;
  - the recipient's ability to verify authenticity.
- Cost and efficiency may also be considered, provided that they do not compromise security, reliability or data integrity.

(a) Authority to whom the data have to be transferred	➢ Indicate the **authority that should receive the requested data**. ➢ Ensure that the **authority selected and the contact details supplied are suitable for receiving the data**. Provide a functional email address, as service providers often use secure links requiring an active and monitored inbox with sufficient storage capacity. ➢ Where the issuing or validating authority is selected, ensure that the contact details provided in the relevant section are complete and suitable for data transfer (e.g.

Funded by the European Union

	the file size is compatible and there are no technical constraints).
☐ issuing authority;	➢ Select this option if the data are to be transferred to the issuing authority.
☐ validating authority;	➢ Select this option if the data are to be transferred to the validating authority (where applicable).
☐ other competent authority (e.g. central authority).	➢ Select this option if the data are to be transferred to another designated authority involved in the case.
☐ Name and contact details:	➢ Provide the official name (or, where applicable, personal identification number, for law enforcement personnel) and full contact details (telephone number in international format, including the country code, and email address). ➢ If data are transferred from JUDEX, these details are essential to ensure secure and verifiable delivery.
(b) Preferred format in which or means by which the data have to be transferred (if applicable):	➢ **Complete** this field only **if data cannot be transferred through JUDEX**. ➢ **Indicate any preferred format or means of transfer** where necessary. Note that service providers may not always be able to accommodate specific preferences. For security, integrity or liability reasons, certain transfer methods (e.g. physical delivery through courier services) may not be supported by all service providers. ➢ Possible **alternative formats or means of transfer** may include (electronic means are generally preferred): • electronic transmission: ○ qualified, registered electronic delivery services, ○ secure Secure/Multipurpose Internet Mail Extensions email, ○ dedicated online portals established by certain service providers for voluntary cooperation, ○ secure cloud storage services (e.g. object storage solutions), ○ encrypted file transfer protocols (e.g. Secure File Transfer Protocol, Hypertext Transfer Protocol); • physical delivery (where supported): ○ encrypted digital storage media (e.g. USB drives, hard disks), ○ printed materials sent via secure channels (e.g. diplomatic pouch); • any other appropriate means of ensuring security, integrity and authenticity. ➢ Where **encryption** is required, specify this clearly and provide the necessary information (e.g. X.509 public certificate for asymmetric encryption and decryption instructions). Ensure compatibility between the chosen

Funded by the European Union

	transfer method and the receiving authority's technical systems. ➢ Include **any additional procedural or technical requirements** (e.g. authentication steps, checksum verification and secure communication of passwords or decryption keys).

Funded by the European Union

Section M: Further information to be included (not to be sent to the addressee – to be provided to the enforcing authority in the event that it needs to be notified)

Purpose

Section M provides additional legal and factual information supporting the issuance of the EPOC. It is intended solely for the enforcing authority where notification is required, enabling it to assess the order, including any potential grounds for refusal.

General guidance

- **Complete** this section only **if an enforcing authority is notified of the EPOC** in accordance with Article 8 of the e-Evidence Regulation.
- **Do not transmit this section to the addressee.**
- When using JUDEX, this section should be completed and signed separately from the part of the EPOC that is transmitted to the addressee.
- Be **concise** but thorough: include all necessary legal and factual elements without excessive detail.
- Use **short, clear sentences** that are easy to translate. **Avoid using legal jargon** unless essential.
- Ensure **consistency with the facts, reasoning and legal references** provided in other sections of the EPOC.

The grounds for determining that the **European Preservation Order** fulfils the conditions of necessity and proportionality:	➢ Explain why the **EPOC is strictly necessary to achieve the legitimate aim of obtaining data** that are relevant as evidence in the individual case. ➢ Describe how the **request is limited in scope and time** (e.g. data are related to a single user account or restricted to a specific date range), demonstrating that no broader data are sought than necessary. ➢ Clarify why the **electronic evidence is required at this procedural stage** (e.g. to identify a suspect, confirm presence at a location or link communications to the offence). ➢ Demonstrate **proportionality** to the purpose of the criminal proceedings or, where applicable, to the execution of a custodial sentence or detention order. The explanation should reflect a balanced assessment of: • the seriousness of the offence; • the relevance and evidential value of the data requested; • the impact on the rights of individuals and/or service providers.
A summary description of the case:	➢ Present the **essential facts in a clear and chronological manner** (what happened, when and where, and who was involved). ➢ Include, where relevant: • the offence(s) under investigation;

Funded by the European Union

	• the suspected account(s) or person(s); • the time, place and method of commission; • the stage of proceedings and any risk factors justifying the urgency of the request; • the link between the offence, the person and the data requested. ➢ Avoid reproducing entire case files; provide a concise summary focused on evidential relevance.
Is the offence for which the European Production Order is being issued punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years and included in the list of offences set out below (tick the relevant box/boxes)? ☐ participation in a criminal organisation; ☐ terrorism; ☐ trafficking in human beings; ☐ sexual exploitation of children and child pornography; ☐ illicit trafficking in narcotic drugs and psychotropic substances; ☐ illicit trafficking in weapons, munitions and explosives; ☐ corruption; ☐ fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council (12); ☐ laundering of the proceeds of crime; ☐ counterfeiting currency, including the euro; ☐ computer-related crime;	➢ Tick only if **both conditions** are met: • the offence is punishable in the issuing state by a custodial sentence or detention order of at least three years; • the offence is covered by one or more of the offences listed below. ➢ If both conditions are fulfilled, the enforcing state cannot invoke dual criminality as a ground for refusal. ➢ Tick all applicable boxes.

Funded by the European Union

- ☐ environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties;
- ☐ facilitation of unauthorised entry and residence;
- ☐ murder or grievous bodily injury;
- ☐ illicit trade in human organs and tissue;
- ☐ kidnapping, illegal restraint or hostage-taking;
- ☐ racism and xenophobia;
- ☐ organised or armed robbery;
- ☐ illicit trafficking in cultural goods, including antiques and works of art;
- ☐ swindling;
- ☐ racketeering and extortion;
- ☐ counterfeiting and piracy of products;
- ☐ forgery of administrative documents and trafficking therein;
- ☐ forgery of means of payment;
- ☐ illicit trafficking in hormonal substances and other growth promoters;
- ☐ illicit trafficking in nuclear or radioactive materials;
- ☐ trafficking in stolen vehicles;
- ☐ rape;
- ☐ arson;
- ☐ crimes within the jurisdiction of the International Criminal Court;

Funded by the European Union

☐ unlawful seizure of aircraft or ships; ☐ sabotage.	
Where appropriate, please add any additional information that the enforcing authority may need to evaluate the possibility of raising grounds for refusal:	➢ Provide any **legal, jurisdictional or procedural considerations that may assist the enforcing authority** in assessing potential grounds for refusal. ➢ Where relevant, address the following. • **Immunities or privileges.** Indicate whether any privileges (e.g. parliamentary, diplomatic, professional secrecy) may apply and confirm that these have been assessed and ruled out under the law of the issuing state. • **Freedom of the press or expression in other media.** Indicate whether the data requested may relate to journalistic sources or communications protected by freedom of expression guarantees, and explain how these guarantees have been safeguarded. • **Fundamental rights.** Where relevant, outline safeguards applied and confirm that there are no substantial grounds to believe that execution of the order would result in a manifest breach of fundamental rights. • ***Ne bis in idem*.** Where similar facts are already subject to criminal proceedings or final judgment in the issuing or another Member State, confirm that no final decision has been rendered for the same offence. • **Dual criminality.** Where the offence does not fall within the list exempted from dual criminality verification and this could be raised by the enforcing authority, confirm that the underlying conduct is also criminalised in the enforcing state or explain its legal qualification. ➢ Where appropriate, indicate any **requests for cooperation** (e.g. assistance in waiving immunities or privileges). ➢ Include any **other procedural or jurisdictional clarifications that may assist the enforcing authority in assessing the order** (e.g. data stored on behalf of a public authority in the issuing state, or coordination with mutual legal assistance requests).

Funded by the European Union