INTERNET & JURISDICTION POLICY NETWORK

THE EU E-EVIDENCE REGULATION

A graphical explanation of its architecture and procedural workflows for Production Orders

Bertrand de LA CHAPELLE
Ajith FRANCIS

June 2023

internetjurisdiction.net

ABOUT THIS DOCUMENT

Access to electronic evidence (ie. data stored by service providers) has become an essential part of most if not all criminal investigations. While elaborate procedures exist in most national legislations regarding requests for access aimed at local companies, such data is increasingly handled by companies **located outside of the territory** of the investigating country. Existing procedures for cross-border access, in particular complex Mutual Legal Assistance Treaties (MLATs), are ill-adapted to the volume and time constraints of investigations.

Accordingly, on April 17, 2018, the European Commission proposed a **draft Regulation** establishing more efficient yet rights-protecting mechanisms to allow investigating authorities to send binding orders for production of such data directly to service providers located in another country. A **companion Directive** would impose an obligation on operators incorporated outside of the Union to designate a legal representative in one of the EU Member States.

After 5 years of intense negotiations and a Trilogue procedure, both Regulation and Directive have been **formally adopted by the EU Parliament and the Council in June 2023** and will fully apply in mid-2026.

Yet, this important and innovative new regime presents a **significant level of complexity**. It therefore seemed useful to present in a graphical manner the different key components and modular processes around which it is organized. In that regard, the present document focuses exclusively on the **main provisions of the Regulation** (but not the Directive) regarding **European Production Orders** (but not Preservation Orders).

We hope this will help everyone understand in an accessible manner the general architecture and modular nature of this new regime.

Bertrand de LA CHAPELLE
Executive Director, I&JPN

Ajith FRANCIS
Director, Policy Programs, I&JPN

ABOUT I&JPN

The **Internet & Jurisdiction Policy Network (I&JPN)** is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

Within I&JPN, the **Data & Jurisdiction Program** has focused on collectively defining high substantive and procedural standards for obtaining cross-border access to electronic evidence directly from service providers. This work seeks to structure the roles and responsibilities of the different actors in the process of such cross-border access as well as define the components of such cross-border regimes and develop applicable due process standards.

The **Data & Jurisdiction Program Contact Group**, consisting of experts from governments, internet companies, technical operators, civil society, leading universities and international organizations has, over the years, identified the key issues that structure new approaches to inform the debate on cross-border access to electronic evidence.

CITATION

Internet & Jurisdiction Policy Network - E-Evidence Regulation Graphical Workflows (2023)

DOCUMENT STRUCTURE

1. SCOPE OF THE REGULATION

- Four Key Actors
- Key Prerequisites
- A Framework of Rights and Obligations

2. A MODULAR STRUCTURE

- Key Modules
- Optimal Basic Workflow
- Requests for Clarifications and Review from Service Provider
- ES Review when Notified by IS
- Enforcement

3. DETAILED WORKFLOWS

- Issuing of Order
- Emergency Cases
- Clarifications and Challenges by SP
- ES Notification and Review
- Immunities & Privileges
- Conflicts with Third-Country Laws
- Enforcement Procedure
- Data Subject Notification and Available Remedies

1 SCOPE OF REGULATION

The Regulation defines interactions among key actors and the conditions, within a framework of rights, obligations and due process, under which orders for data access can be issued, executed, and enforced.

FOUR KEY ACTORS

IS

ISSUING STATE

The State with jurisdiction over the investigation, wanting access to the data.
Different procedural obligations apply, depending on the initiating authority in that State, the type of data to be accessed and the location of both suspect and crime.

SP

SERVICE PROVIDER

The company providing services in the Issuing State, but incorporated elsewhere, that stores the data sought.
Referred to as “the addressee” in the Regulation, it is expected to comply with a Production Order within a specific timeline. If located outside of the EU, it must (per a separate Directive) designate a legal representative in a EU Member State that is also part of Article 34 of the EU Treaty on mutual assistance in criminal matters between Union Member States.

ES

ENFORCING STATE

The State where the Service Provider is incorporated or has its Representative in the Union.
The Enforcing State (ES) can be asked by the Issuing State (IS) to enforce Orders in case of Service Provider (SP) non compliance. For some Orders, the ES is notified simultaneously with the SP, and evaluates if the Order should be rejected or adapted, with suspensive effect.

TP

TARGETED PERSON

The individual user whose data is sought.
The responsibility to inform the Targeted Person (TP) lies solely with the IS.

KEY PREREQUISITES | 1 OF 2

DOMESTIC MEASURE EQUIVALENCE

An European Production Order may only be issued if it could have been ordered under the same conditions in a similar domestic case.

NECESSITY AND PROPORTIONALITY

A European Production Order has to be necessary and proportionate for the purpose of the proceedings.

TYPES OF ELECTRONIC EVIDENCE

European Productions Orders can be issued for four categories of data:

- **Subscriber Data:** The identity of a subscriber or customer, including names and birthdates, but also technical information such as the technical measure and interface used by the user at the time of registration or activation, excluding passwords.
- **Data requested for the sole purpose of identifying the user:** Data points such as IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information that can be used solely for identifying a user.
- **Traffic Data:** Data that provides context or additional information such as the source and destination of communications, location data and time-stamps on communications.
- **Content Data:** Data pertaining to the actual content of communications.

KEY PREREQUISITES | 2 OF 2

TYPES OF CRIMES COVERED

For subscriber data and data requested for the sole purpose of identifying a user, Orders may be issued for all criminal offences as well as for the execution of a custodial sentence or a detention order of at least 4 months.

For Traffic and Content data, Orders may only be issued for either criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or a specific set of offences covered in Article 5.4.

INITIATING AUTHORITY IN ISSUING STATE

A judge, a court, or an investigating judge competent in the case can issue orders for all types of electronic evidence.

Other designated competent authorities defined by the Issuing State may also issue orders in their capacity as an investigating authority in criminal proceedings. However, orders by such authorities have to be validated by a judge, a court or an investigating judge in the issuing State.

As an exception, for Subscriber Data and Data requested for the sole purpose of identifying the user, orders can also be issued by a competent public prosecutor. For such orders issued by a another competent authority defined by the Issuing State, public prosecutors can also validate them (in addition to a judge, a court or an investigating judge).

PROVIDERS COVERED

European Production Orders can be addressed to Service Providers defined in Art 3.3, providing services in the EU and established or, if not established, represented by a legal representative in a Member State different from the Issuing State. Entities covered are: a) Providers of Electronic Communication Services; b) Internet domain name and IP numbering services; c) Certain other information services defined in Directive (EU) 2015/1535.

A FRAMEWORK OF RIGHTS AND OBLIGATIONS

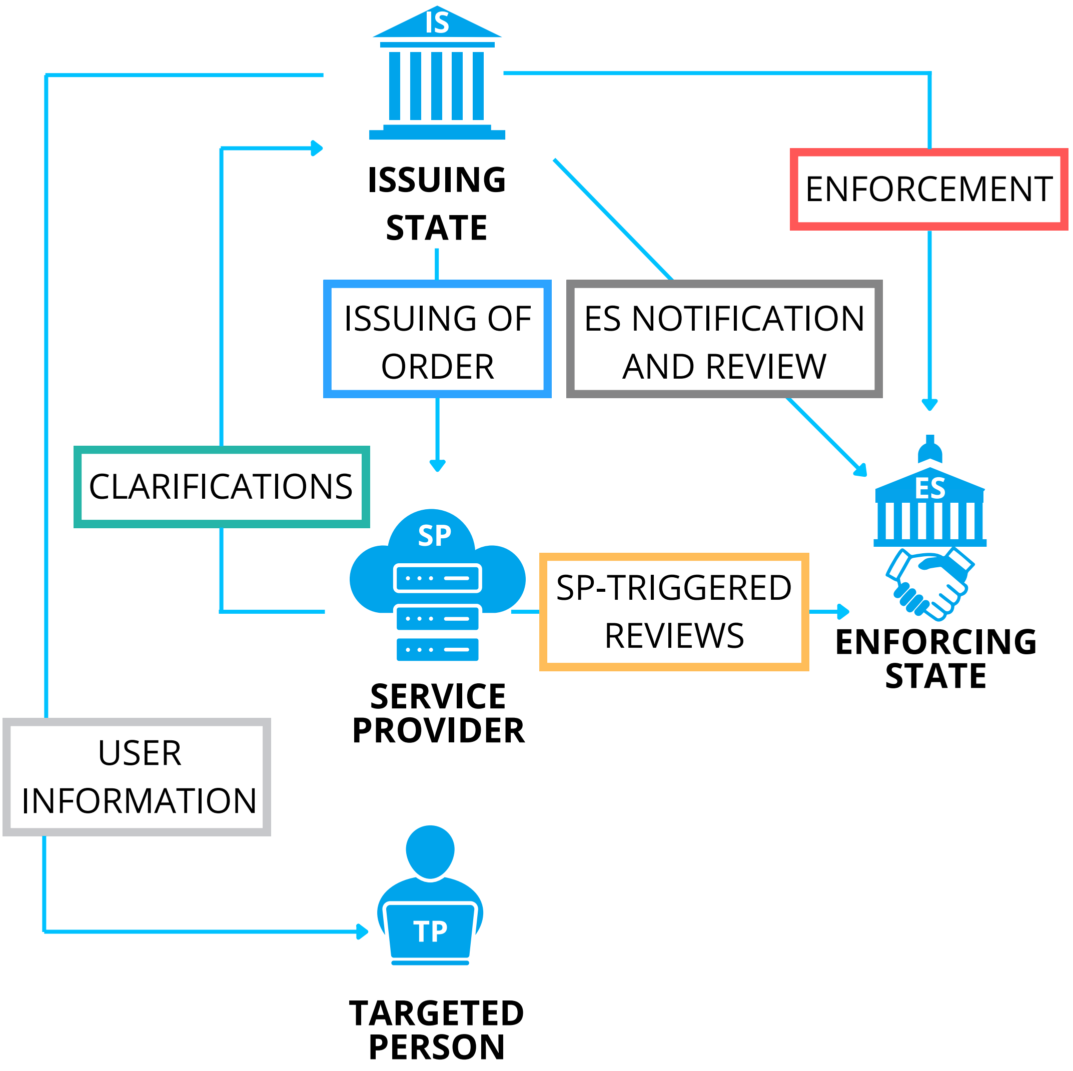
KEY ACTORS	RIGHTS	OBLIGATIONS
ISSUING STATE	• Capacity to issue binding orders to obtain electronic evidence from foreign Service Providers • Obtain enforcement, when justified, in case of non-compliance by Service Provider	• Respect scope and due process when issuing Orders and provide sufficient information and justifications for order to be executed • Notify ES of orders for traffic and content data when the subject or crime is outside IS jurisdiction • Evaluate the interest of third party countries • Notify Targeted Person, without undue delay
SERVICE PROVIDER	• Procedure to obtain clarification if the order is not implementable or incomplete • Capacity to raise issues regarding: ○ Immunities and privileges ○ Conflict with third country laws	• Designate a representative in the Union • Produce Data within set deadlines, unless justified objection; possible sanctions for non-compliance • Ensure confidentiality and secrecy of the order
ENFORCING STATE	• Authority to evaluate orders by IS and to decide on recognition or not, either when simultaneously notified, or upon request by SP, or during enforcement	• When notified because the data subject or crime are located outside the Issuing State, review Orders according to specific grounds for non-recognition • Review Order if objection by Provider • Ensure enforcement of legitimate Orders
TARGETED PERSON	• Right to be informed of the data production by the Issuing State, unless confidentiality is justifiably imposed during a limited period • Right to effective remedies	

2 A MODULAR ARCHITECTURE

The general architecture of the Regulation can be described around six key modules, succinctly illustrated in the following graphics

KEY MODULES

The regulation structures the interactions between the actors across six different sub-processes, each serving a specific purpose.



ISSUING OF ORDER

Procedures regarding the preparation and transmission of Orders, including in situations of emergency.

CLARIFICATIONS

Procedures for SP to request clarifications from IS if the Order is incomplete, impossible to implement, or if a deadline extension is necessary.

SP-TRIGGERED REVIEWS

Procedure for SP to alert IS and ES if SP considers the execution of the Order raises issues of immunities and privileges, or conflict with third country laws.

ES NOTIFICATION & REVIEW

Simultaneous notification of SP and ES for traffic and content data (except if TP is resident in IS and the crime is committed in IS territory) and procedure for review by ES on specific grounds for objection.

ENFORCEMENT

If SP does not comply with the Order, procedure for IS to ask ES to enforce it. SP has opportunity to object to enforcement. ES can issue sanctions to SP in case of ultimate non compliance.

USER INFORMATION

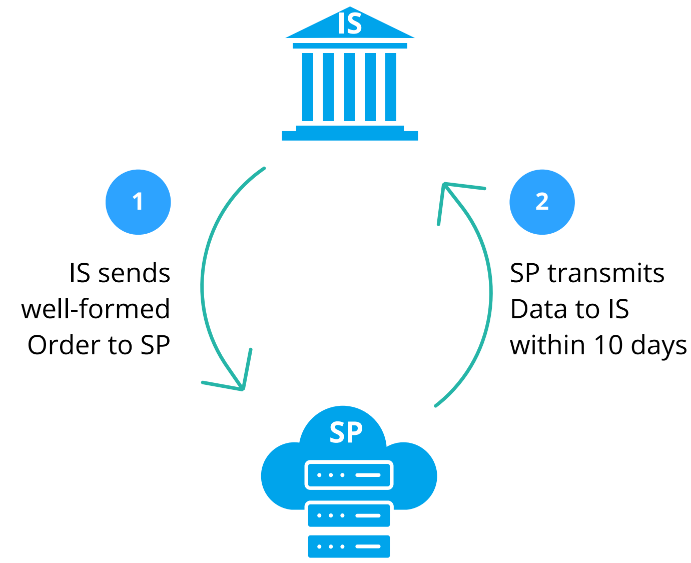
Applicable rules for imposing confidentiality, including when and by whom the TP is informed of the Data transfer.

OPTIMAL BASIC WORKFLOW

In the optimal functioning of the regulation, a Service Providers (SP) transmits **within 10 days** the requested data to the Issuing State (IS). Still, two distinct procedures apply on Order issuance, depending upon data type and locations.

FOR ANY DATA IF BOTH THE SUBJECT AND THE CRIME ARE LOCATED IN THE IS

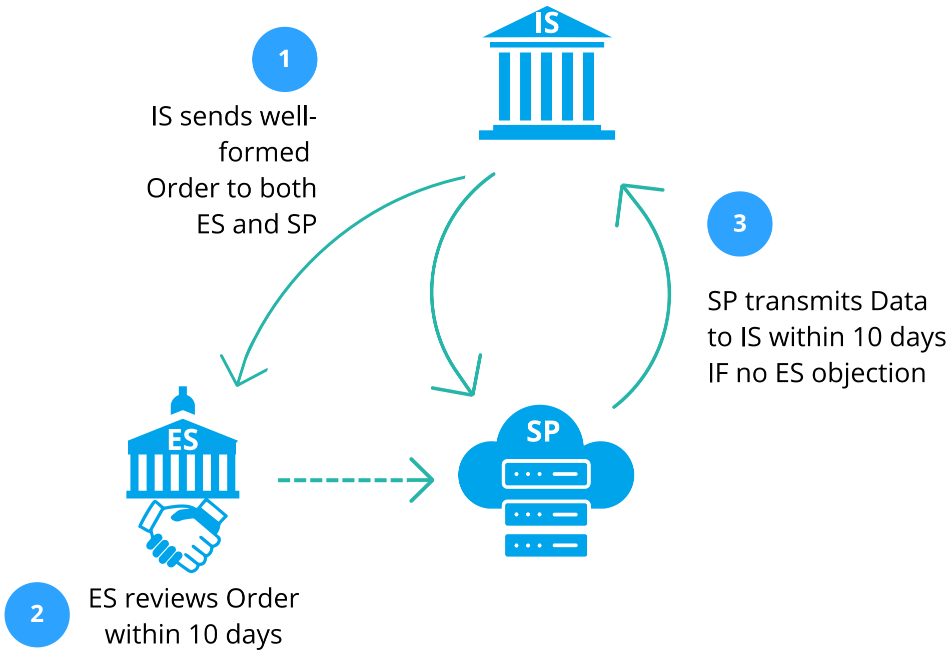
(Also Orders for Subscriber Data and Data solely for identifying users, even when the subject or crime are outside the IS)



1 IS sends well-formed Order to SP

2 SP transmits Data to IS within 10 days

FOR TRAFFIC AND CONTENT DATA IF THE SUBJECT OR THE CRIME ARE OUTSIDE THE IS



1 IS sends well-formed Order to both ES and SP

2 ES reviews Order within 10 days

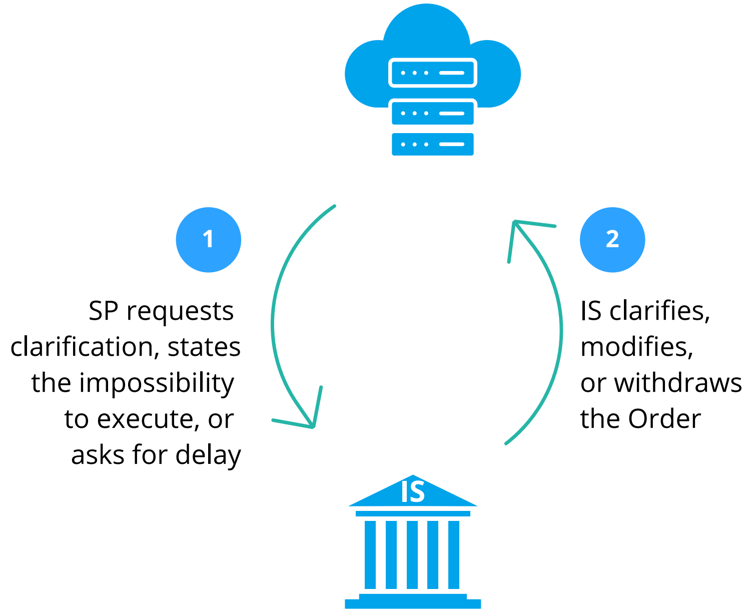
3 SP transmits Data to IS within 10 days IF no ES objection

In **emergency situations**, the delay for data transmission by the service provider (SP) is **8 hours** instead of 10 days and the review by the notified Enforcing State (ES) must be conducted within **96 hours** instead of 10 days.

CLARIFICATIONS AND REVIEW REQUESTS BY SERVICE PROVIDER

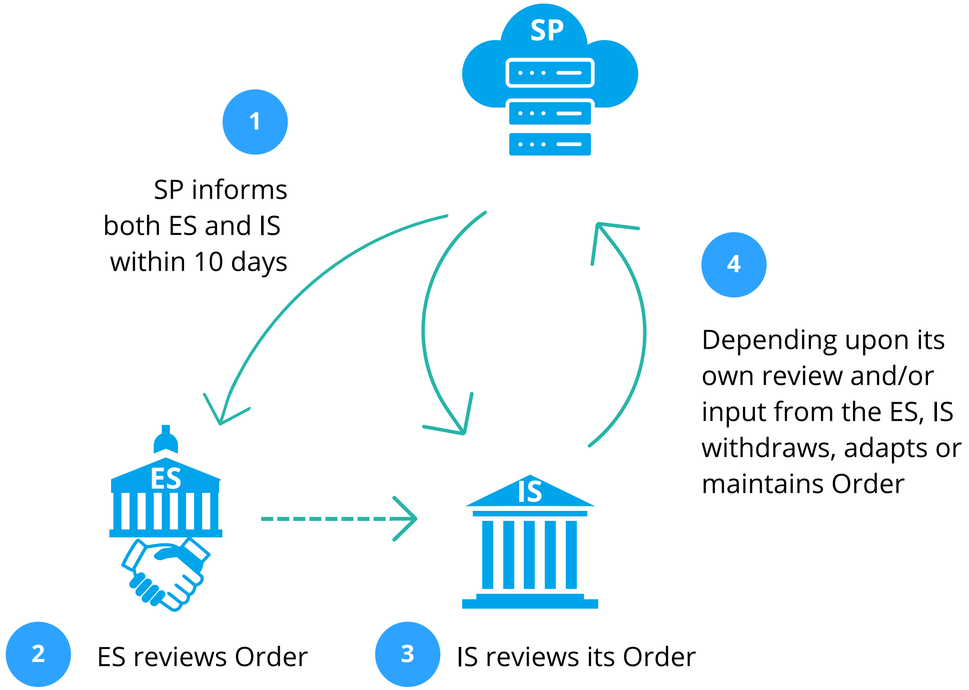
CLARIFICATIONS

A Service Provider (SP) can request clarifications from the Issuing State (IS) if the Order appears **incomplete or is impossible to execute** within the deadline or at all.


1
SP requests clarification, states the impossibility to execute, or asks for delay
2
IS clarifies, modifies, or withdraws the Order
IS

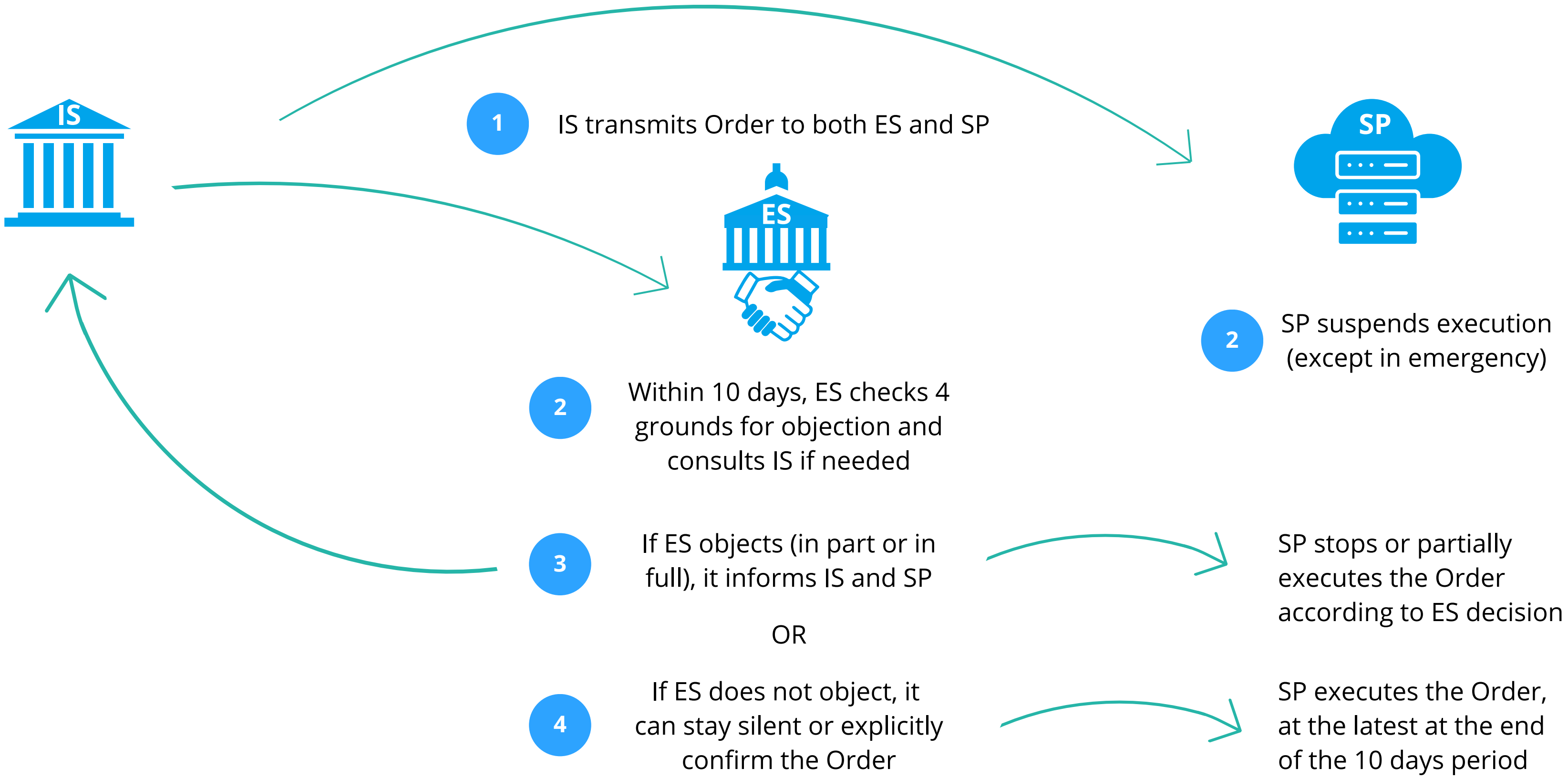
SP-TRIGGERED REVIEW

SP can also alert both IS and Enforcing State (ES) on possible issues regarding **immunities and privileges, or conflicts with third country laws.**


SP
1
SP informs both ES and IS within 10 days
4
Depending upon its own review and/or input from the ES, IS withdraws, adapts or maintains Order
ES
IS
2
ES reviews Order
3
IS reviews its Order

ES REVIEW WHEN NOTIFIED BY IS

The Issuing State (IS) must transmit the Order both to the Service Provider (SP) and the Enforcing State (ES) if it concerns traffic and content data, unless the targeted person (TP) resides in the IS AND the crime was, is being, or is likely to be committed in the IS. Upon notification, the ES conducts a review of 4 objection grounds within 10 days.



1 IS transmits Order to both ES and SP

2 Within 10 days, ES checks 4 grounds for objection and consults IS if needed

2 SP suspends execution (except in emergency)

3 If ES objects (in part or in full), it informs IS and SP

SP stops or partially executes the Order according to ES decision

OR

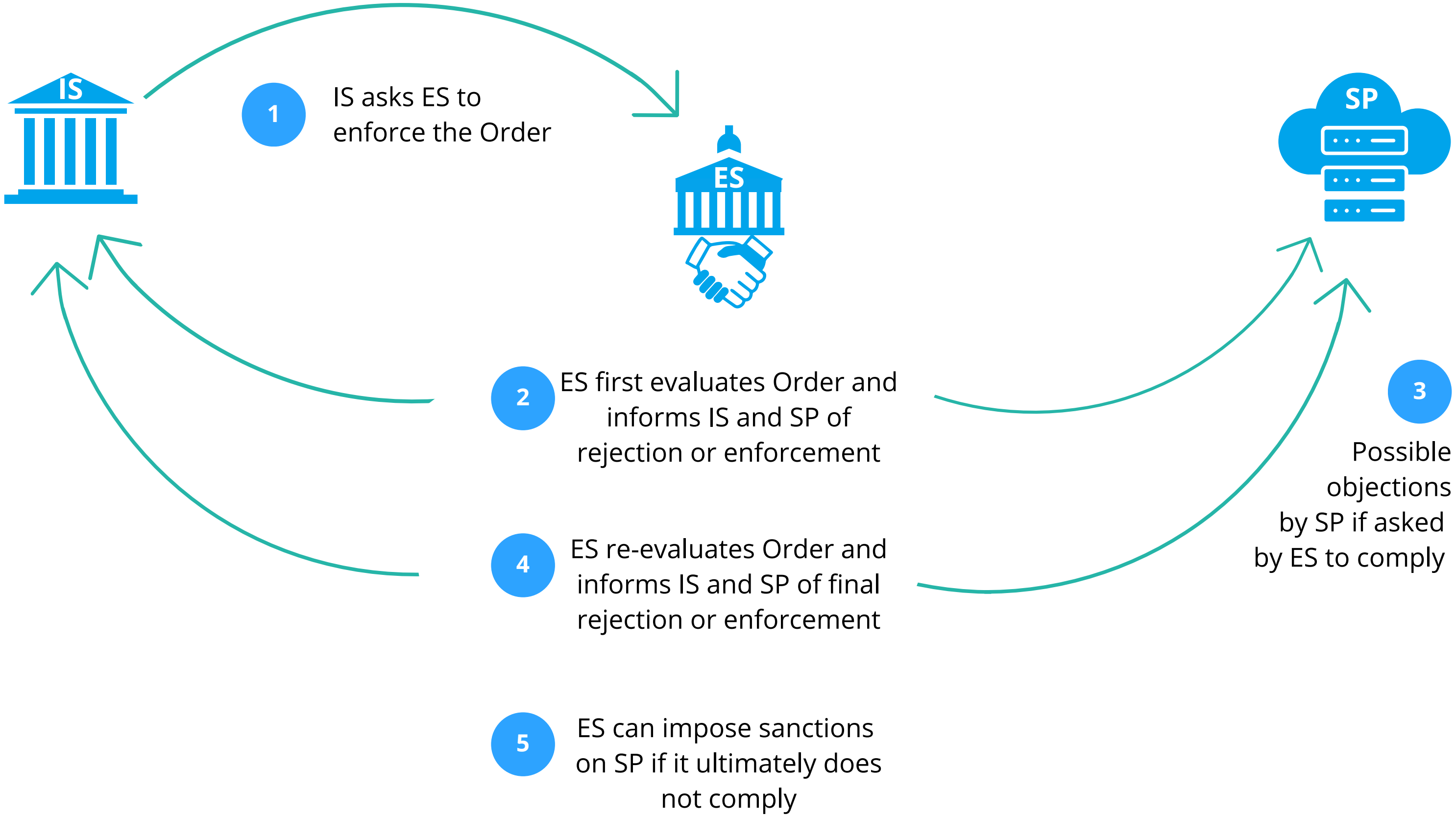
4 If ES does not object, it can stay silent or explicitly confirm the Order

SP executes the Order, at the latest at the end of the 10 days period

In **emergency situations**, the delay for review by the Enforcing State is 96 hours instead of 10 days and the execution of the Order by the SP is not suspended. The Issuing State must delete the data received if the ES expressed objections after the SP has already transmitted it (SP delay is 8 hours vs. 96 for the review by ES).

ENFORCEMENT

If the Service Provider (SP) fails to comply with the Order without acceptable reasons, the Issuing State (IS) can ask the Enforcing State (ES) to enforce the Order, unless the ES was notified and had previously raised grounds for objection. During the enforcement process the SP can object but is susceptible of sanctions if it has not complied in the end with a confirmed Order by the ES.



1 IS asks ES to enforce the Order

2 ES first evaluates Order and informs IS and SP of rejection or enforcement

3 Possible objections by SP if asked by ES to comply

4 ES re-evaluates Order and informs IS and SP of final rejection or enforcement

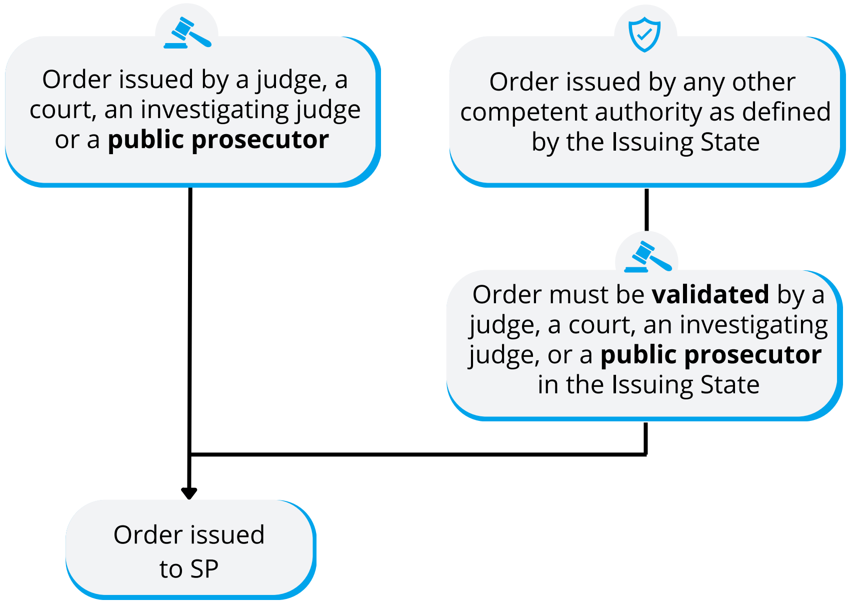
5 ES can impose sanctions on SP if it ultimately does not comply

3 DETAILED WORKFLOWS

The following illustrations describe in graphic form the concrete decision-making workflows corresponding to the different modular processes.

ISSUING OF ORDER

ACCESS TO SUBSCRIBER INFORMATION OR DATA REQUESTED FOR THE SOLE PURPOSE OF IDENTIFYING THE USER (Art. 4.1)



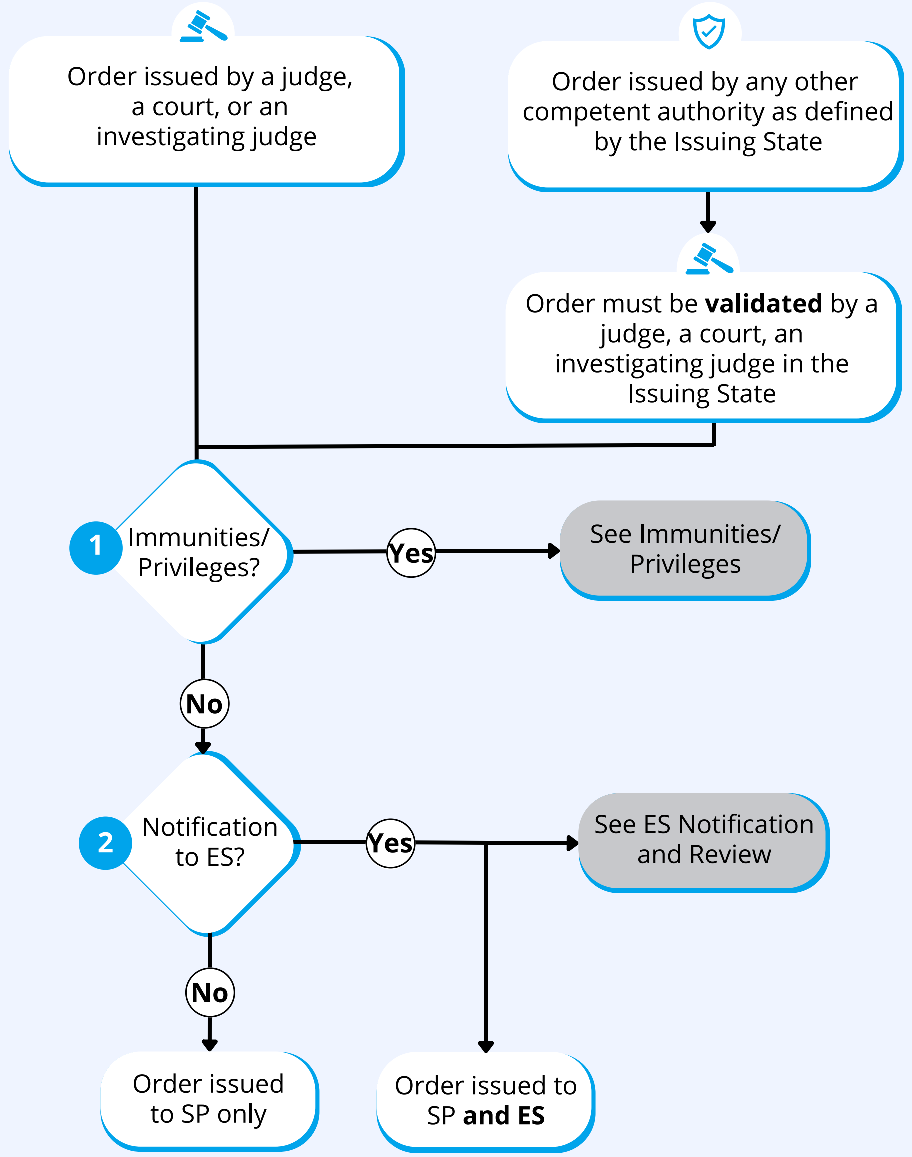
Order issued by a judge, a court, an investigating judge or a **public prosecutor**

Order issued by any other competent authority as defined by the Issuing State

Order must be **validated** by a judge, a court, an investigating judge, or a **public prosecutor** in the Issuing State

Order issued to SP

ACCESS TO TRAFFIC DATA (EXCEPT FOR SOLELY IDENTIFYING THE USER) AND CONTENT DATA (Art. 4.2)



Order issued by a judge, a court, or an investigating judge

Order issued by any other competent authority as defined by the Issuing State

Order must be **validated** by a judge, a court, an investigating judge in the Issuing State

1 Immunities/ Privileges?

Yes

See Immunities/ Privileges

No

2 Notification to ES?

Yes

See ES Notification and Review

No

Order issued to SP only

Order issued to SP **and ES**

1

Art 5.7

Does Issuing State have reason to believe that the data is protected by immunities and privileges granted under:
a) the law of the Member State where the service provider is addressed, OR
b) it is subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media

2

Art 7a

Order is sent to Provider AND Enforcing State, unless:
a) the offence has been committed, is being committed or is likely to be committed in the issuing State; AND
b) the person whose data are sought resides in the issuing State

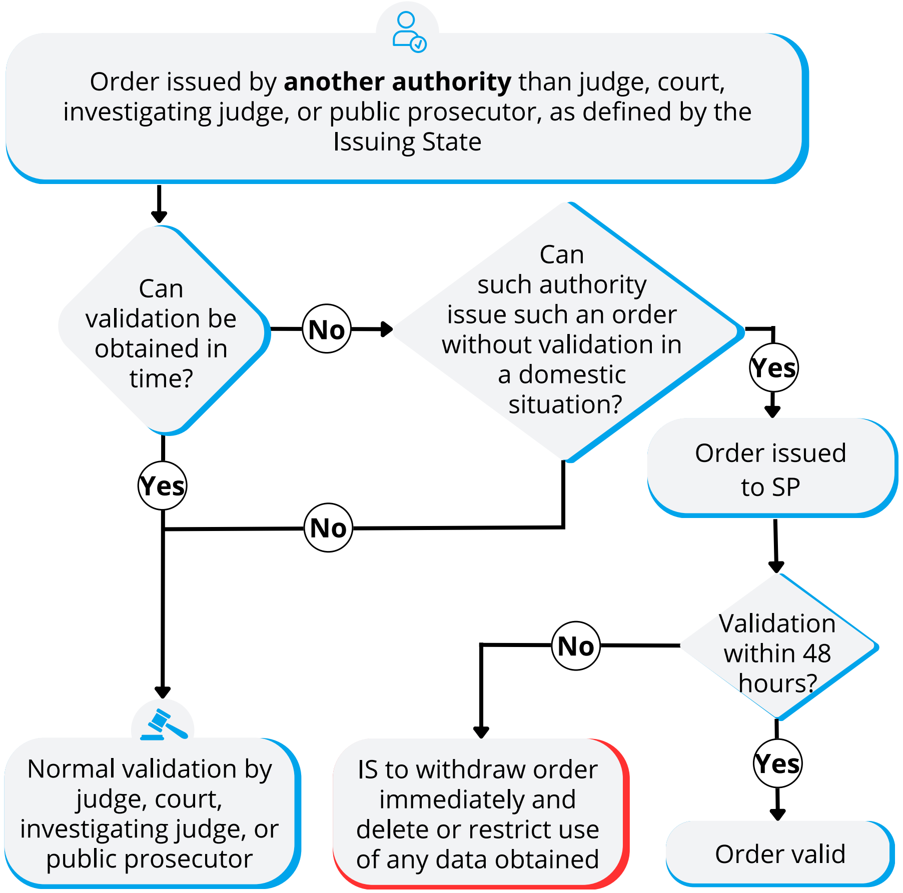
DELAYED VALIDATION AND EMERGENCY CASES

As an exception, some orders for subscriber data or solely for user identification can be validated post issuance, if within 48h.

“Emergency cases” cover imminent threat to life or physical integrity or safety of a person, or to a critical infrastructure (Art. 2.15). ES notification has no suspensive effect.

EXCEPTION: DELAYED VALIDATION IN IS (Art. 4.5)

Access to subscriber data or data solely for identification



Order issued by **another authority** than judge, court, investigating judge, or public prosecutor, as defined by the Issuing State

Can validation be obtained in time?

No

Can such authority issue such an order without validation in a domestic situation?

Yes

Order issued to SP

Yes

No

Validation within 48 hours?

No

Yes

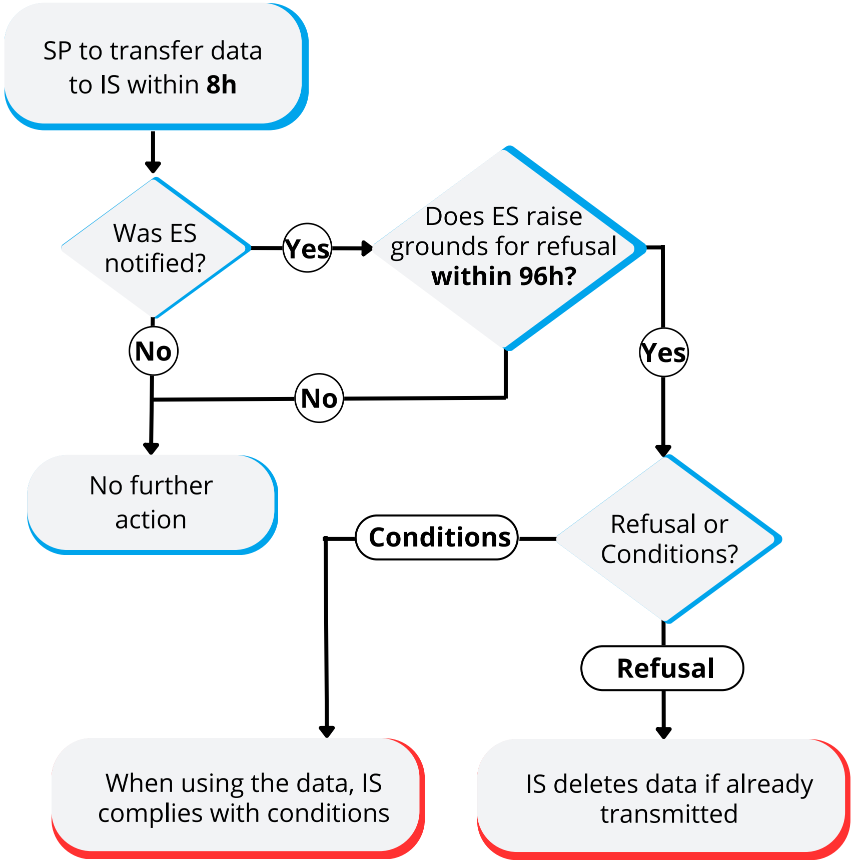
Normal validation by judge, court, investigating judge, or public prosecutor

IS to withdraw order immediately and delete or restrict use of any data obtained

Order valid

GENERAL EMERGENCY PROCEDURE (Art. 10.4)

Orders for all types of data



SP to transfer data to IS within **8h**

Was ES notified?

Yes

Does ES raise grounds for refusal **within 96h?**

No

No

Yes

No further action

Refusal or Conditions?

Conditions

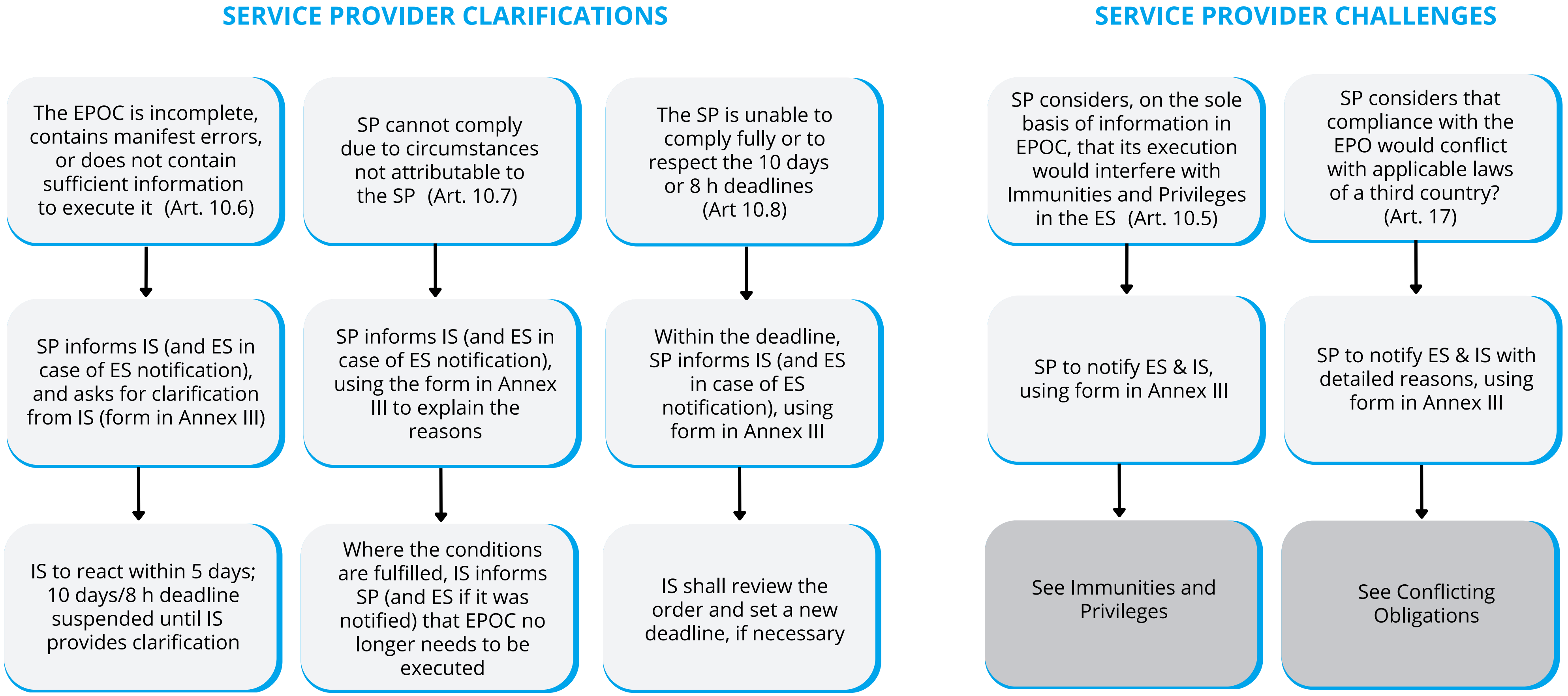
Refusal

When using the data, IS complies with conditions

IS deletes data if already transmitted

CLARIFICATIONS & CHALLENGES BY SP

Reminder: When the ES is being simultaneously notified (Art 8), this notification has a suspensive effect on the addressee’s obligations outlined in Art 10, except for emergency cases. When there is such a simultaneous notification to SP and ES, SP may only disclose the data if the ES has not raised any grounds for objection within the set time limit or it has notified the SP to proceed with the disclosure (Art 10.2).



SERVICE PROVIDER CLARIFICATIONS

The EPOC is incomplete, contains manifest errors, or does not contain sufficient information to execute it (Art. 10.6)

SP informs IS (and ES in case of ES notification), and asks for clarification from IS (form in Annex III)

IS to react within 5 days; 10 days/8 h deadline suspended until IS provides clarification

SP cannot comply due to circumstances not attributable to the SP (Art. 10.7)

SP informs IS (and ES in case of ES notification), using the form in Annex III to explain the reasons

Where the conditions are fulfilled, IS informs SP (and ES if it was notified) that EPOC no longer needs to be executed

The SP is unable to comply fully or to respect the 10 days or 8 h deadlines (Art 10.8)

Within the deadline, SP informs IS (and ES in case of ES notification), using form in Annex III

IS shall review the order and set a new deadline, if necessary

SERVICE PROVIDER CHALLENGES

SP considers, on the sole basis of information in EPOC, that its execution would interfere with Immunities and Privileges in the ES (Art. 10.5)

SP to notify ES & IS, using form in Annex III

See Immunities and Privileges

SP considers that compliance with the EPO would conflict with applicable laws of a third country? (Art. 17)

SP to notify ES & IS with detailed reasons, using form in Annex III

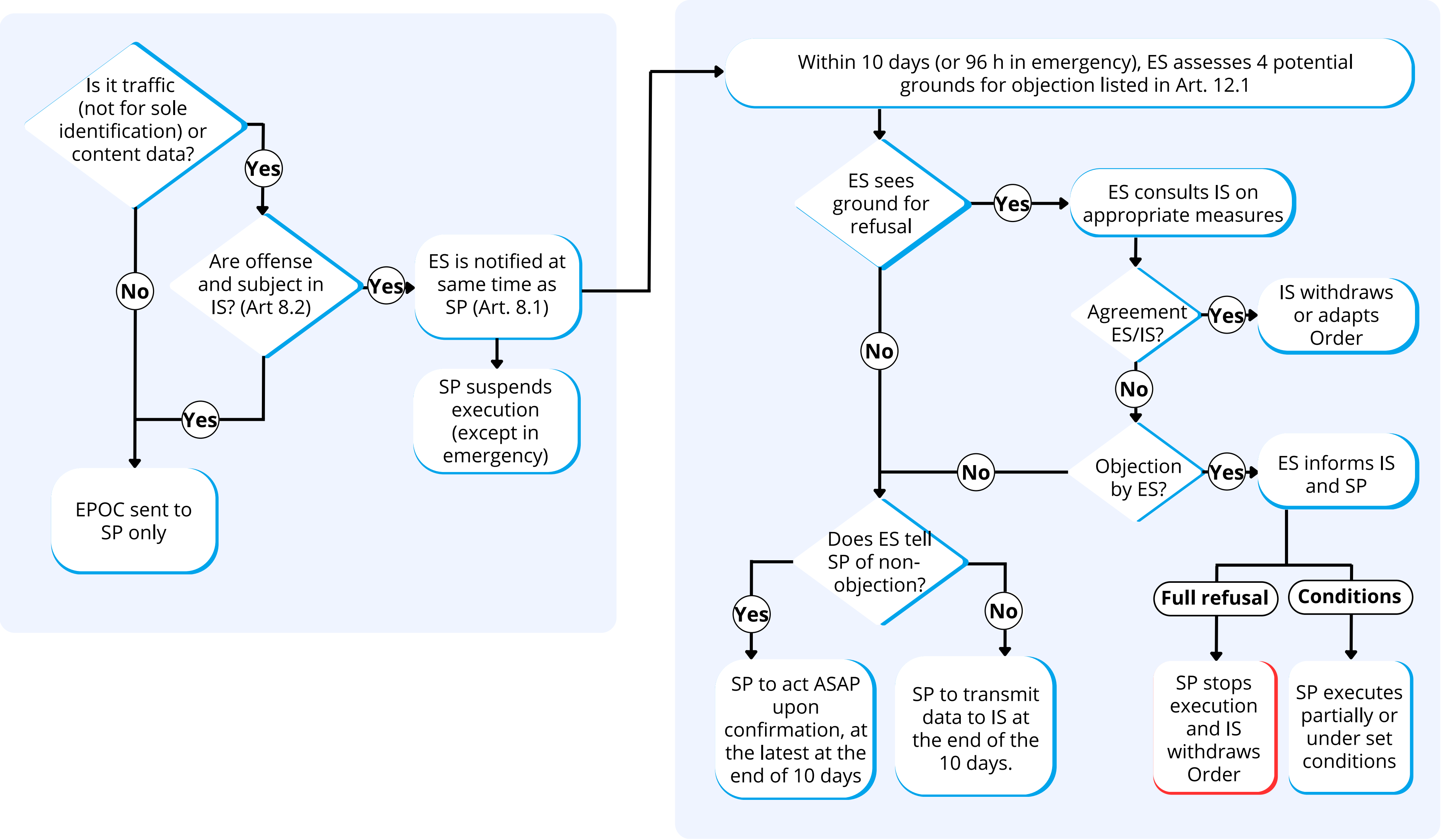
See Conflicting Obligations

Note: The Service Provider may also challenge the enforcement of an Order pursuant to grounds listed under Article 16.4 (points a-f). For the corresponding workflow regarding such challenges, see Enforcement Procedure.

ES NOTIFICATION & REVIEW

ISSUING STATE NOTIFICATION TO ENFORCING STATE (Art. 8)

ORDER REVIEW BY ENFORCING STATE UPON NOTIFICATION (Art. 12)



Is it traffic (not for sole identification) or content data?

Yes

No

Are offense and subject in IS? (Art 8.2)

Yes

Yes

EPOC sent to SP only

ES is notified at same time as SP (Art. 8.1)

SP suspends execution (except in emergency)

Within 10 days (or 96 h in emergency), ES assesses 4 potential grounds for objection listed in Art. 12.1

ES sees ground for refusal

Yes

ES consults IS on appropriate measures

Agreement ES/IS?

Yes

IS withdraws or adapts Order

No

No

Objection by ES?

Yes

ES informs IS and SP

No

Full refusal

Conditions

SP stops execution and IS withdraws Order

SP executes partially or under set conditions

Does ES tell SP of non-objection?

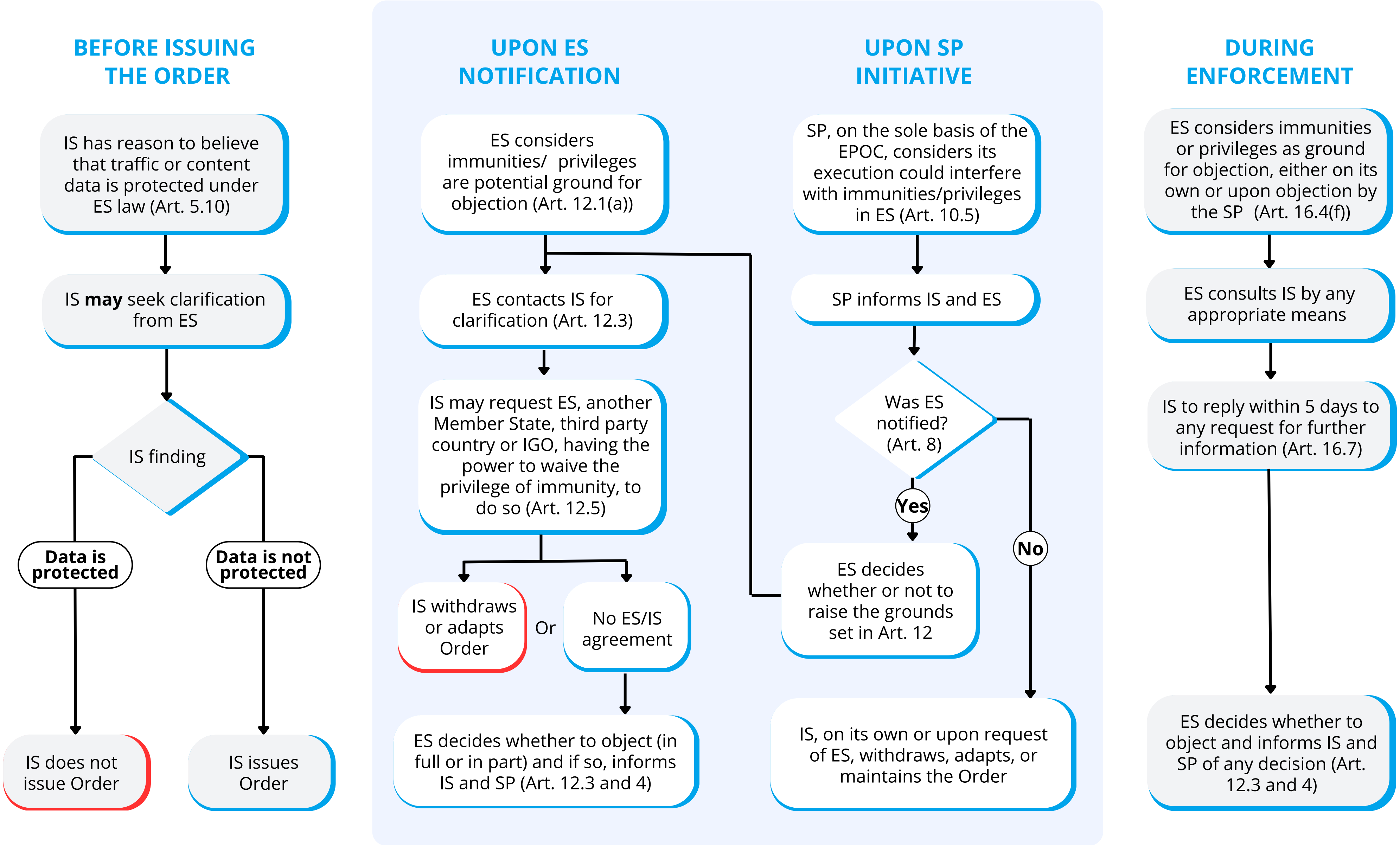
Yes

No

SP to act ASAP upon confirmation, at the latest at the end of 10 days

SP to transmit data to IS at the end of the 10 days.

IMMUNITIES & PRIVILEGES



BEFORE ISSUING THE ORDER

IS has reason to believe that traffic or content data is protected under ES law (Art. 5.10)

IS **may** seek clarification from ES

IS finding

Data is protected

IS does not issue Order

Data is not protected

IS issues Order

UPON ES NOTIFICATION

ES considers immunities/ privileges are potential ground for objection (Art. 12.1(a))

ES contacts IS for clarification (Art. 12.3)

IS may request ES, another Member State, third party country or IGO, having the power to waive the privilege of immunity, to do so (Art. 12.5)

IS withdraws or adapts Order

Or

No ES/IS agreement

ES decides whether to object (in full or in part) and if so, informs IS and SP (Art. 12.3 and 4)

UPON SP INITIATIVE

SP, on the sole basis of the EPOC, considers its execution could interfere with immunities/privileges in ES (Art. 10.5)

SP informs IS and ES

Was ES notified? (Art. 8)

Yes

ES decides whether or not to raise the grounds set in Art. 12

No

IS, on its own or upon request of ES, withdraws, adapts, or maintains the Order

DURING ENFORCEMENT

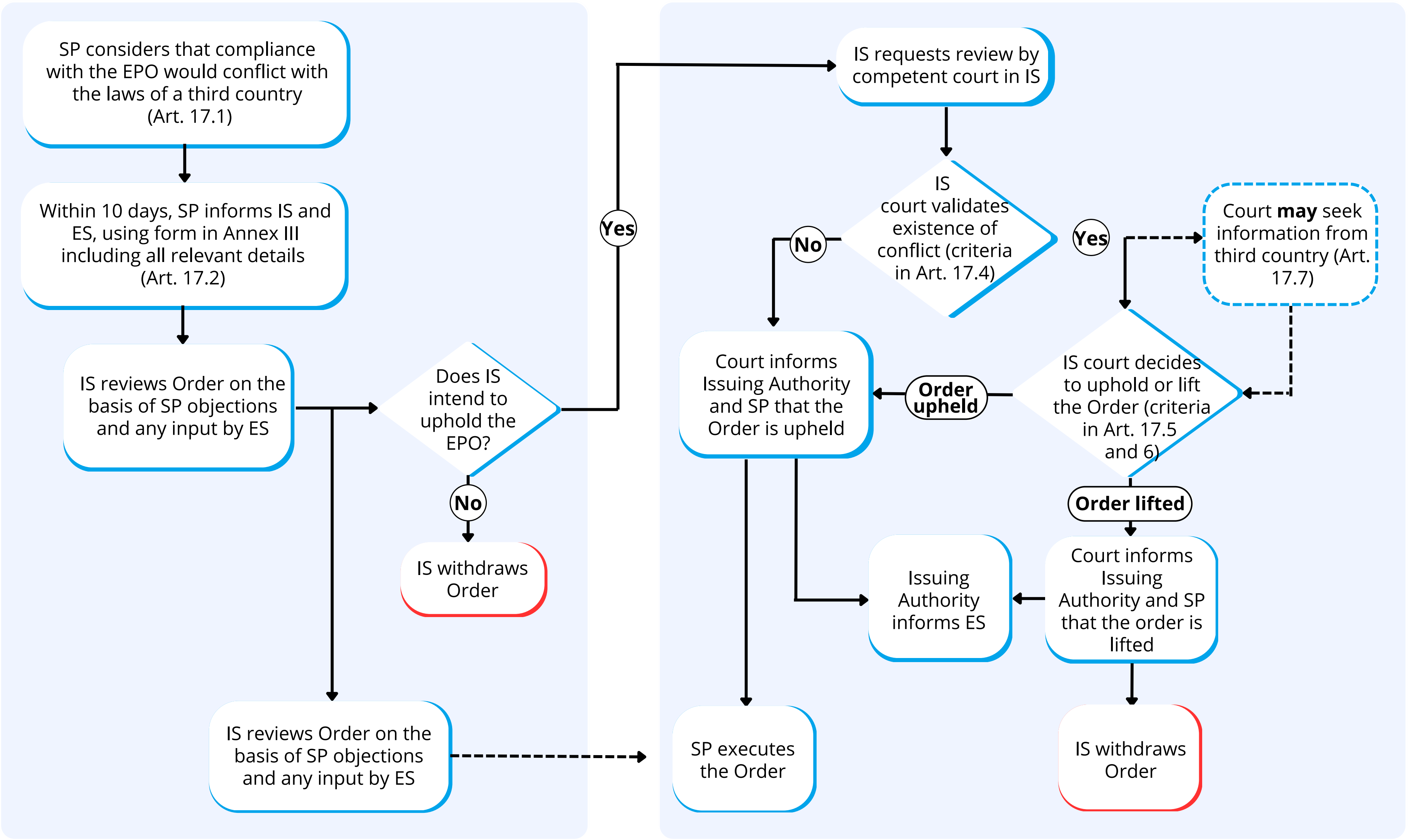
ES considers immunities or privileges as ground for objection, either on its own or upon objection by the SP (Art. 16.4(f))

ES consults IS by any appropriate means

IS to reply within 5 days to any request for further information (Art. 16.7)

ES decides whether to object and informs IS and SP of any decision (Art. 12.3 and 4)

CONFLICTS WITH 3RD COUNTRY LAWS (SP-TRIGGERED REVIEW)



ASSESSMENT BY ISSUING AUTHORITY

Article 17.1, 2 and 3

SP considers that compliance with the EPO would conflict with the laws of a third country (Art. 17.1)

Within 10 days, SP informs IS and ES, using form in Annex III including all relevant details (Art. 17.2)

IS reviews Order on the basis of SP objections and any input by ES

Does IS intend to uphold the EPO?

No

IS withdraws Order

Yes

IS reviews Order on the basis of SP objections and any input by ES

REVIEW BY COURT IN ISSUING STATE

Article 17.4 to 17.10

IS requests review by competent court in IS

IS court validates existence of conflict (criteria in Art. 17.4)

No

Yes

Court **may** seek information from third country (Art. 17.7)

IS court decides to uphold or lift the Order (criteria in Art. 17.5 and 6)

Order upheld

Court informs Issuing Authority and SP that the Order is upheld

Order lifted

Court informs Issuing Authority and SP that the order is lifted

Issuing Authority informs ES

SP executes the Order

IS withdraws Order

ENFORCEMENT PROCEDURE

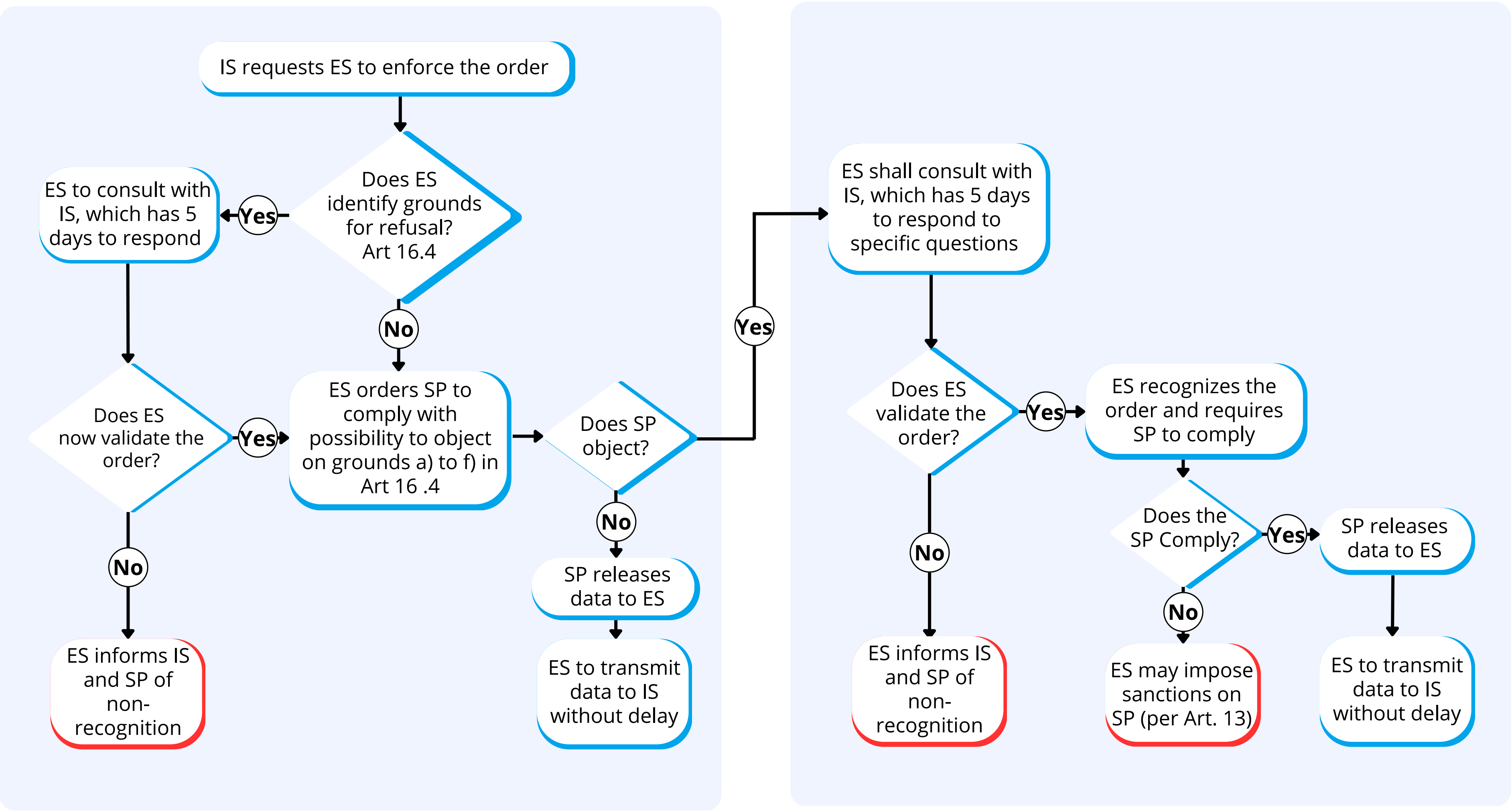
If SP did not comply without providing a reason and a notified ES has not previously invoked grounds for non-recognition or objection, IS can request ES to enforce the order. But SP can object to such enforcement.

ISSUING STATE REQUEST TO ENFORCING STATE TO ENFORCE THE ORDER

Art. 16.1 & 16.2

SERVICE PROVIDER OBJECTION TO ENFORCEMENT

Art. 16.6



IS requests ES to enforce the order

Does ES identify grounds for refusal? Art 16.4

Yes: ES to consult with IS, which has 5 days to respond

Does ES now validate the order?

No: ES informs IS and SP of non-recognition

Yes / No: ES orders SP to comply with possibility to object on grounds a) to f) in Art 16 .4

Does SP object?

No: SP releases data to ES

ES to transmit data to IS without delay

Yes: ES shall consult with IS, which has 5 days to respond to specific questions

Does ES validate the order?

No: ES informs IS and SP of non-recognition

Yes: ES recognizes the order and requires SP to comply

Does the SP Comply?

No: ES may impose sanctions on SP (per Art. 13)

Yes: SP releases data to ES

ES to transmit data to IS without delay

DATA SUBJECT NOTIFICATION AND AVAILABLE REMEDIES

IS informs user without delay of data production

The Issuing Authority shall notify the person whose data are being sought without undue delay about the data production (Art 13.1). **Note**: this obligation mentions "data production", ie. post-disclosure information rather than a delay starting from the issuance of the order.

SP ensures confidentiality and secrecy

The addressees and, if different, the service providers shall take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved (Art 13.3).

IS includes information about available remedies

When informing the person, the issuing authority shall include information about available remedies pursuant to Article 18 (Art 13.4).

Informed user can seek remedies in a court of the IS

Any persons whose data were sought via a European Production Order shall have the right to effective remedies against this Order (Art 18.1). The right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law (Art 18.2).

IS may delay Notification

The issuing authority may, in accordance with national law, delay, restrict or omit informing the person whose data are being sought, to the extent that, and for as long as the conditions in Article 13(3) of Directive (EU) 2016/680 are met, in which case, the issuing authority shall indicate in the case file the reasons for the delay, restriction or omission. A short justification shall also be added in the Certificate (Art 13.2).

REFERENCE

Complete information on the process that led to the adoption of the Electronic evidence regime (European Production and Preservation Orders and Legal Representatives Directive) can be found here:

- 'Electronic evidence regulation: European production and preservation orders for electronic evidence in criminal matters' (2018/0108(COD))
- 'Electronic evidence in criminal proceedings: legal representatives directive' (2018/0107(COD))

The texts of the Regulation and Directive adopted by the EU Parliament on June 13, 2023 can be found here and here respectively.

CITATION

Bertrand de La Chapelle, Ajith Francis
Internet & Jurisdiction Policy Network - E-Evidence Regulation Graphical Workflows (2023)