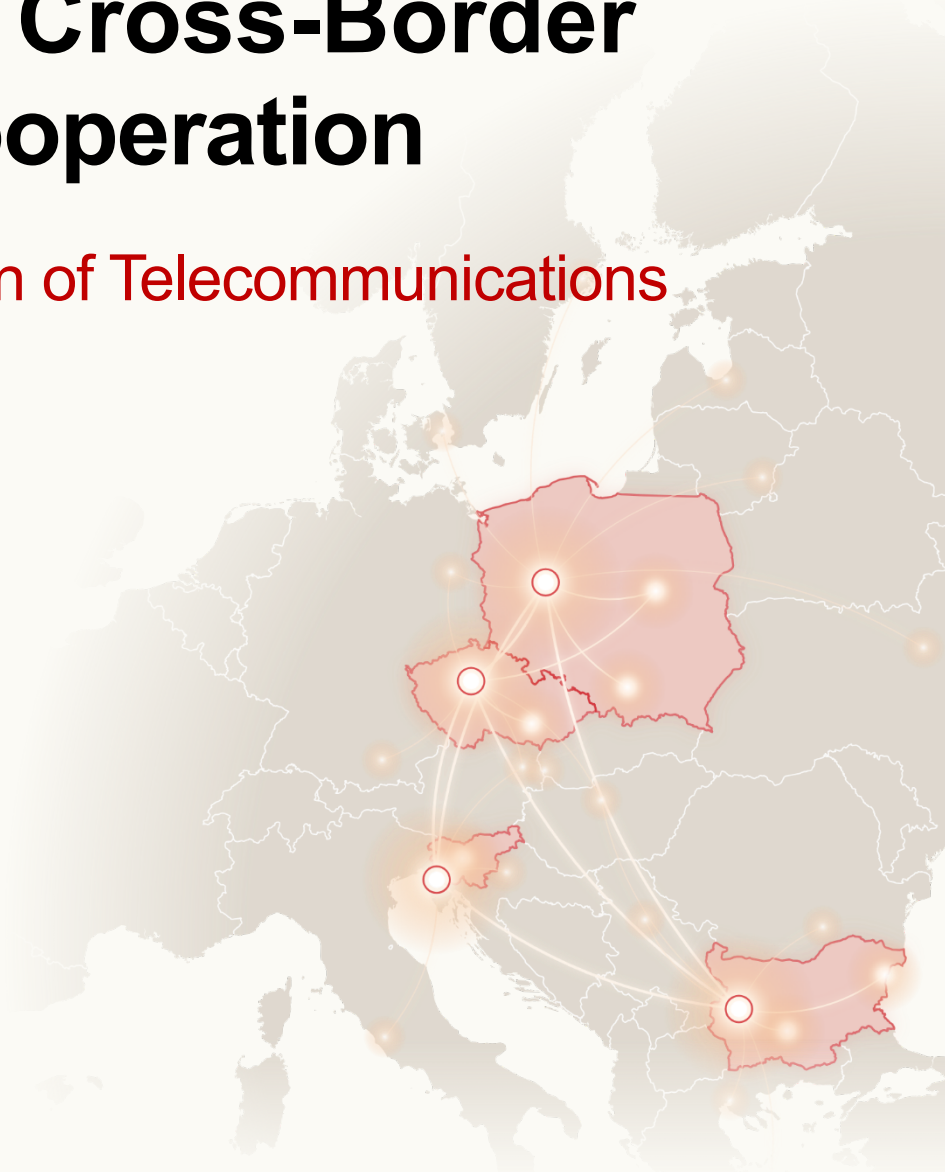
INCEPT

Manual for Cross-Border Judicial Cooperation

Use of Interception of Telecommunications



Funded by
the European Union

INCEPT Project: Supporting Cross-Border Judicial Cooperation in Cases Related to INterCEPTion of Telecommunications

The INCEPT Project is dedicated to enhancing judicial cooperation and the implementation of the European Investigation Order (EIO), particularly in cases involving the interception of telecommunications. By conducting targeted capacity-building initiatives and developing a comprehensive Manual and methodology, INCEPT seeks to bridge gaps in national standards, improve cross-border collaboration, and ensure the correct and effective application of the legal framework.

This manual provides practical guidance on the use of interception of telecommunications in the context of the European Investigation Order, bringing together legal analysis, procedural clarifications and practical examples for judicial authorities and legal practitioners across the European Union.

Developed within the INCEPT Project, the manual aims to support the effective and rights-compliant use of interception measures in cross-border cooperation, contributing to a more consistent and efficient application of EU law in practice.

INCEPT Project Consortium

- Law and Internet Foundation, Bulgaria
- CEELI Institute, Czech Republic
- Adam Mickiewicz University Poznań, Poland
- Science and Research Centre of Koper, Slovenia

Funded by
the European Union

This deliverable was funded by the European Union under Grant Agreement 101192923. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.

Table of Contents

Table of Abbreviations 7

Introduction 9

I. Overview of the Legal Framework 11

II. European Investigation Order 14

i. An Introduction to the European Investigation Order 14

ii. Interception of Telecommunications Under the EIO Directive 16

III. Overview of Case Law 18

i. ECtHR Case Law 18

ii. CJEU Case Law 24

IV. Practical Guidance to Help to Understand What 'Interception of Telecommunications' Means 30

V. Practical Guidance to Find Most Appropriate Cooperation Instrument 33

VI. Good Practices to Help Resolve the Most Common Challenges in Interception Cases and Cross-Border Cooperation 37

i. Legal Framework and Procedural Requirements 37

ii. Operational Cooperation and Institutional Capacity 40

iii. Access to Data and Technical Feasibility 44

iv. Handling and Transmission of Interception Materials 47

v. Evidentiary Use, Defence Rights and Judicial Scrutiny 49

VII. Changes Affecting International Cooperation in Matters of Telecommunications Interception in the Proposal to Amend the EIO Directive 52

VIII. Key Takeaways for Practice 55

Table of Abbreviations

Abbreviations	Descriptions
24/7	*24 hours a day, 7 days a week*
AB	Aktiebolag (Swedish legal form of a company)
BGs	Bundesgerichtshof (case number in the German Federal Court of Justice's case register)
B.V.	Besloten vennootschap met beperkte aansprakelijkheid (the Dutch form of a limited liability company)
CEELI	Central and Eastern European Law Initiative
CJEU	Court of Justice of the European Union
Crim	Criminal Division
E2EE	End-to-End Encryption
ECtHR	European Court of Human Rights
e.g.	*exempli gratia*
EIO	European Investigation Order
EJN	European Judicial Network
EN	English language
EPOC	European Production Order Certificate
EPOC-PR	European Preservation Order Certificate
EPPO	European Public Prosecutor's Office
esp.	*especially*
et al.	*et alii / et alia*
ETSI	European Telecommunications Standards Institute
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EWCA	England and Wales Court of Appeal
GmbH	Gesellschaft mit beschränkter Haftung (the German form of a limited liability company)
GPS	Global Positioning System
HI2	Handover Interface port 2
HI3	Handover Interface port 3
ID	*identification / identifier*

i.e.	*id est*
IMSI	International Mobile Subscriber Identity
incl.	including
IT	Information Technology
JHA	Justice and Home Affairs
Kft.	Korlátolt felelősségű társaság (the Hungarian form of a limited liability company)
LI	Lawful Interception
LIF	Law and Internet Foundation
MLA	Mutual Legal Assistance
No / Nos	*number / numbers*
para	*paragraph*
PCAP	Packet Capture
SHA-256	Secure Hash Algorithm, 256-bit
SIENA	Secure Information Exchange Network Application
SIM	Subscriber Identity Module
UAM	Uniwersytet im. Adama Mickiewicza w Poznaniu (Adam Mickiewicz University Poznań)
UN	United Nations
UTC	Coordinated Universal Time
v.	*versus*
ZRS	Znanstveno-raziskovalno središče Koper (Science and Research Centre Koper)

Introduction

The INCEPT project focused on cross-border judicial cooperation in cases related to the interception of telecommunications and the effective implementation of the European Investigation Order (EIO) in criminal matters, ensuring its proper application and the admissibility of the evidence collected through it. Its overall goal was to identify similarities, good practices, and challenges and therefore enhance cooperation between practitioners working on such cases. The initiative has taken a closer look at experiences from Bulgaria, the Czech Republic, Poland and Slovenia, i.e. the countries of the consortium partners.

The project started by conducting data collection activities covering the legal framework at national and EU levels and case law from domestic courts, the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). This in-depth desk research phase significantly helped with the next tasks foreseen in the project, including the development of a standardised questionnaire. The survey enabled us to gather data on how the rules governing the cross-border interception of telecommunications are applied in practice, identify gaps between legal provisions and their practical application, diagnose specific operational bottlenecks, common errors, and areas of divergence between participating countries, as well as provide empirical data to shape the Methodology. Moreover, consolidating the previously gathered knowledge in the Methodology laid the groundwork for the national and international capacity-building activities, helping define the scope of the training and prepare the materials. The training sessions became a forum for the exchange of practical expertise and mutual learning. This was carried out at domestic events, which took place in each partner country (two per country), as well as at two international events organised in Sofia and Poznan.

This Manual builds upon the data collected throughout the INCEPT project, and particularly the practitioner-participants' experiences voiced at the events organised during the project. The different backgrounds and origins of the target groups (mainly judges, prosecutors and other LEAs' representatives, not only from the partner countries, but also from Belgium, Germany, Italy and Romania) enabled a cross-professional and international panorama of good practices and gaps to be collected and compiled. This Manual is therefore based on different points of view, which will help to give a better understanding of how to make cross-border cooperation in interception cases more effective and generally easier for the benefit of all parties and the criminal proceedings themselves.

I. Overview of the Legal Framework

EU Legal Instruments and other Documents	
Directive (EU) 2014/41 of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters	Articles 1–7, 9–16, 19–21, 28–32 and 34; Annexes A–D. In particular, Articles 30–31 and Part H7 of Annex A
Proposal for a Directive of the European Parliament and of The Council regarding the European Investigation Order in criminal matters and the European Remote Participation Order (recast)	Articles 21, 30, 31, 33, 34, 35
Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union	Articles 1, 4, 6–7, 13–14 and 17–23. In particular, Articles 18–20 and Article 23
Council Framework Decision of 13 June 2002 on joint investigation teams	Article 1, in particular paragraphs 7–10
Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings	Articles 1–13, 16–19 and 34; Annexes I–II. In particular, Article 3(8), Articles 4–11 and 18
Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings	Articles 1–4 and 6–7
Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA	Article 1(3)–(4), Articles 3–10, 13–14 and 22

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA	Articles 3–4, 7, 18–20 and 25–26
Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA	Articles 2–4 and 8
Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network	Articles 2–4 and 7–9
Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')	Articles 30–32 and 42, in particular Article 30(1)(c) and (e)
Charter of Fundamental Rights of the European Union	Articles 7–8, 47–48 and 50–52
Council of Europe Legal Documents	
European Convention on Mutual Assistance in Criminal Matters of 20 April 1959	Articles 1–3, 14–16, 19 and 26
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8 November 2001	Articles 4, 8, 19–20 and 25–26
Convention on Cybercrime of 23 November 2001	Articles 14–15, 20–21, 23–28 and 33–35
Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence of 12 May 2022 Not yet in force	Articles 2–5, 10 and 12–16, in particular Article 12
Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 19 September 2025 Not yet in force	Articles 1, 3–7 and 9–10, in particular Articles 3–4
Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 as amended by Protocols Nos. 11, 14 and 15 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16	Articles 8, 6 and 13

UN Legal Documents	
United Nations Convention against Transnational Organized Crime of 15 November 2000	Articles 3, 18–20 and 27
United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes of 24 December 2024 Not yet in force	Articles 23–24, 29–30, 35–36, 40–41, 45–48 and 65, in particular Articles 45–46

II. European Investigation Order

i. An Introduction to the European Investigation Order

The European Investigation Order (EIO) was established by Directive 2014/41/EU of 3 April 2014, which was subsequently implemented by the Member States into their domestic laws. It is an instrument of judicial cooperation based on the principle of mutual recognition. It enables a competent authority in one Member State to obtain evidence by carrying out specific measures in another Member State or by having that State's authorities provide material already in their possession.

The European Investigation Order (EIO)

OVERVIEW

1 Subject-matter

EIO enables the competent authority of one Member State to request the authorities of another Member State to carry out investigative measures or to provide evidence already in their possession.

2 Issuing authority

The issuing authority may be a judge, a court, an investigating judge, or a public prosecutor with jurisdiction over the case in question. An EIO may also be issued by another authorised investigative authority. Domestic law may also grant this power to other investigative authorities. In such cases, before the EIO is forwarded to the other State, one of the aforementioned judicial authorities must approve it, verifying that the conditions for its issue have been met.

3 Executing authority

The executing authority is the competent authority under the law of the State to which the EIO is addressed. It decides whether to recognise the order and ensures that the requested measures are carried out. If a particular measure requires court authorisation in that State, such authorisation must be obtained in accordance with its law.

4 Terms of issue

The issuance of an EIO must be necessary and proportional to the purpose of the proceedings, whilst taking into account the rights of the suspect or accused person. The measure in question must be permissible under the same conditions in a similar domestic case. The issuing authority assesses whether these conditions are met in each individual case.

5 Form and submission

An EIO shall be drawn up using the form set out in Annex A, setting out, amongst other things, the facts of the case, the purpose and grounds for the order; the measures requested and the evidence to be obtained. The form must be signed, and translated into a language accepted by the executing State. Generally, the EIO is transmitted directly to the competent executing authority in a manner that ensures a written record is retained, and the authenticity of the document to be established.

6 Recognition and execution

As a general rule, the executing authority recognises the EIO without any further formalities. It carries out the requested action in the same way as it would in a similar domestic case. It must also take into account the specific requirements of the issuing authority, unless these conflict with the fundamental principles of law of the executing State or the Directive provides otherwise.

The EIO establishes a joint procedure for obtaining evidence, including a standard form, time limits for recognition and execution, and specific grounds for refusal. Its application also requires due regard to national law, in particular the jurisdiction of the authorities and the conditions for the admissibility of specific measures. The instrument applies between EU Member States, with the exception of Denmark and Ireland.

The European Investigation Order (EIO)

OVERVIEW

7

Key dates

Receipt of the EIO must be confirmed without delay, and at the latest within one week, using the form in Annex B. A decision on recognition or execution is taken within 30 days of the competent executing authority receiving the EIO, and the measure is carried out without delay, generally within 90 days of that decision. The Directive provides for exceptions and procedures in the event of a delay. The need for a shorter deadline or for the measure to be carried out on a specific date must be indicated and justified in the EIO.

8

Carrying out an alternative measure

If the requested measure does not exist under the law of the executing State or would be inadmissible in a similar domestic case, the executing authority should, where possible, apply an alternative measure. It may also choose a measure that is less intrusive on the rights of the individual, provided that it achieves the same result. Before applying an alternative measure, the issuing authority should be informed of such an approach, and may withdraw or amend the EIO.

9

Refusal or deferral

Recognition or execution of an EIO may be refused, for example, on the grounds of immunity, the principle of ne bis in idem, or the risk of a breach of fundamental rights. In certain cases, refusal must be preceded by consultation with the issuing authority.

Execution may be deferred if it would prejudice ongoing proceedings or if the evidence is being used in another case.

10

Handling over the evidence

Evidence must be forwarded to the issuing State without undue delay. If an appeal has been lodged, the forwarding of the evidence may, in certain cases, be suspended until the appeal has been determined.

The executing State may request the return of the evidence once it is no longer required in the issuing State.

11

Fundamental rights and legal remedies

The issuance and execution of an EIO must respect fundamental rights, including the right to a defence and to a fair trial. These rights are also taken into account when assessing the admissibility of evidence. The person concerned must be guaranteed the same opportunities to challenge the proceedings as in a similar domestic case. The legality of the EIO is challenged in the issuing State. However, this does not deprive the individual of the protection provided for in the executing State.

ii. Interception of Telecommunications Under the EIO Directive

In cases concerning the interception of telecommunications, the general rules are supplemented by Article 30, where technical assistance from another Member State is required, and by Article 31, which establishes a separate mechanism for notifying the State in whose territory the person subject to interception is located, where its technical assistance is not required.

Interception of telecommunications

COMPARISON (PART 1)

	Interception of telecommunications with technical assistance from another Member State	Interception of telecommunications without technical assistance from another Member State
What is this option used for?	To **request assistance** from another State that is necessary to carry out an interception.	To enable the State in which the person subject to interception is located to **verify whether such an interception would be authorised** in a similar domestic case.
Does the intercepted person have to be in the country to which the EIO or notification is being sent?	This is **not a condition** for the application. The EIO is addressed to the State whose technical assistance is required. The location of the person will be a factor when choosing between several States capable of providing assistance.	**Yes,** the obligation to notify arises when the person whose communications have been intercepted is in a country other than the one carrying out the interception. This obligation may arise before interception begins or while it is ongoing.
Does the cooperation involve only traditional telephone calls?	**No,** it may include the content of communications and related traffic and location data, regardless of the service provider, including internet communications.	**No,** it may include the content of communications and related traffic and location data, regardless of the service provider, including internet communications.
Who decides and who is the decision addressed to?	An EIO is issued and authorised in accordance with the national law of the issuing State. It is addressed to the competent authority of the executing State, which executes it in accordance with its own national law.	The interception must be authorised by the competent authority of the intercepting State. The notification is sent to the authority designated by the notified State, which need not be the same authority to which EIOs are generally addressed.
Which form should be used?	Annex A, in which the section on interception must be completed.	Annex C.

Interception of telecommunications

COMPARISON – PART 2

	Interception of telecommunications with technical assistance from another Member State	Interception of telecommunications without technical assistance from another Member State
What conditions must be met?	An EIO must be necessary and proportionate, and the measure in question must be admissible under the same conditions in a similar domestic case in the executing State. Furthermore, its relevance to the proceedings must be explained.	There must be a valid national basis for interception and authorisation from the competent authority. Notification alone does not authorise interception. As it is not an EIO, the conditions governing the issuance of an EIO do not automatically apply to it.
How many countries should the documents be sent to?	If several countries are able to provide all the necessary assistance in the same operation, one must be chosen. Priority is given to the country in which the person is or will be located. Where full assistance requires the involvement of several countries, EIO may be issued to more than one.	Every country in which the intercepted person is located must be notified. The person's movements may result in further notification of obligations.
When should the document be sent?	Well in advance, allowing sufficient time for the EIO to be approved, the necessary consents to be obtained and technical preparations to be made.	Before initiating the interception, if it is already known at the time of ordering the interception that the person is or will be abroad. If this is established later — immediately upon becoming aware of it, either during the operation or after it has been completed. A subsequent notification should not be regarded as an alternative.
What are the response times for the other State?	The general time limits for the recognition and execution of EIOs apply.	The notified State may impose a restriction or prohibition **without delay,** or at the latest within 96 hours of receiving the notification. This does not, however, mean that the intercepting State should wait 96 hours before starting the operation.

The case concerning these two procedures was reviewed by the French Court of Cassation on 17 June 2025, No. 24-87.110, in which a mobile phone subject to remote data retrieval had travelled, amongst other places, to Spain and the Czech Republic. Technical assistance from those countries was not required; however, the authorities issued an EIO. The Court highlighted the obligation to provide notification. In this specific case, the Court considered the transmitted EIO, although unnecessary, to fulfil the function of notification, whilst acknowledging that the States had not reported any restrictions and eventually found the evidence obtained in this way to be admissible.

III. Overview of Case Law

i. *ECtHR Case Law*

The following section provides an overview of the key points stemming from the case law of the European Court of Human Rights relating to communications interception.

Lawful Interception of Telecommunications and Effective Oversight of its Use	
***Roman Zakharov v. Russia* App No 47143/06, 4 December 2015**, §§ 171, 257-267	Interception has to be targeted, meaning that there must be an effective way to verify whether there is a reasonable suspicion concerning a specific person. Otherwise, the mere threat of general surveillance to which anyone may be subjected restricts freedom of communication. Necessity and proportionality must be assessed while the interception is authorised, as well as the availability of effective legal remedies against secret surveillance and the existence of judicial oversight.
***Dragojević v. Croatia* App No 68955/11, 15 January 2015**, §§ 95, 97-98	The justification for the interception must be specific, referring to the details of the case, and not only to the fact that evidence cannot be obtained by any other means. The reasons for its use must be provided in advance, not retrospectively. In other words, even the fact that incriminating recordings have been obtained does not justify the decision to initiate interception.
***Szabó and Vissy v. Hungary* App No 37138/14, 12 January 2016**, §§ 71-73	Interception of telecommunications has to be ‚necessary in a democratic society' and ‚strictly necessary' in order to be lawful. Such an intrusive measure cannot be simply justified by usefulness for criminal proceedings.

***Matanović v. Croatia* App No 2742/12, 4 April 2017**, § 151 ***Ekimdzhiev and Others v. Bulgaria* App No 70078/12, 11 January 2022**, §§ 313, 327-329, 332, 343, 344	The supervisory body has to be guaranteed unfettered access to all relevant materials, including data not relevant to the criminal proceedings, data relating to third parties, and data containing surplus information in order to assess the legality and proportionality of the interception measure. It must also be able to react to violations. Access to both incriminating and exonerating evidence should also be guaranteed for the defence, including evidence which law enforcement agencies find to be irrelevant.
***Pietrzak and Bychawska-Siniarska and Others v. Poland* App Nos 72038/17 and 25237/18, 28 May 2024**, §§ 207, 208, 213, 231, 238-240	The body authorising interception must give reasons for its decision, especially when authorisation is granted and not only when it is refused. Court oversight cannot be limited to the authorisation phase only but must also extend to the implementation of the measure. The legal framework should also contain a deletion procedure and oversight of this kind of procedure as well as adequate safeguards governing the emergency procedure. Interception that is lawful also requires notification and effective remedies.
Protection of the Confidentiality of Communications	
***Kopp v. Switzerland* App No 23224/94, 25 March 1998**, §§ 73-75	While intercepting conversations covered by legal professional confidentiality, it has to be made clear under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel'. Independent judicial supervision is also recommended in such cases.

***Podchasov v. Russia* App No 33696/19, 13 February 2024**, §§ 77-79	When access to encrypted communication is granted, the consequences for all users should be taken into consideration, especially whether weakening end-to-end encryption affects people not posing a threat. Granting such access should also not create ,backdoors that may be exploited by criminal networks and would seriously compromise the security of all users' electronic communications'. Decrypting communications is disproportionate if it weakens encryption for all the users.
Bulk Interception	
***Big Brother Watch and Others v. United Kingdom* App Nos 58170/13, 62322/14 and 24960/15, 25 May 2021**, §§ 350-361 ***Centrum för rättvisa v. Sweden* App No 35252/08, 25 May 2021**, §§ 266-275	Bulk interception is permissible as long as the prior authorisation is granted by a body independent of the executive, ongoing supervision is ensured, and *ex post facto* review is carried out. While granting authorisation for bulk interception, the authority should take into consideration the criteria set out in para 361 of the Big Brother Watch ruling. To use bulk interception, it is also required to specify in the interception request criteria that enable a particular individual's communications to be targeted. These criteria, called selectors and strong selectors, are subject to supervision as well. An effective remedy is also crucial when it comes to bulk interception, including a remedy which is not dependent on notification.

The Admissibility of Evidence Obtained Through Interception of Telecommunications	
***Schenk v. Switzerland* App No 10862/84, 12 July 1988**, §§ 46-49	The use of evidence obtained unlawfully, even through telephone interception, does not in itself violate the right to a fair trial.
***Khan v. United Kingdom* App No 35394/97, 12 May 2000**, §§ 37-38	A violation of privacy because of surveillance is not equal to a violation of the right to a fair trial, even if evidence obtained through interception is the only evidence or if other evidence is significantly weaker.
***Bykov v. Russia* App No 4378/02, 10 March 2009**, §§ 95, 98, 102-105	The assessment of fair trial guarantees should moreover include the possibility of challenging the evidence, the whole context of the conversation, and the voluntary nature of the recorded conversation.
***Allan v. United Kingdom* App No 48539/99, 5 November 2002**, §§ 50-53	It is contrary to the principle of a fair trial to use a police informer to obtain information from a suspect who previously exercised his right to remain silent.

***Karabeyoğlu v. Turkey* App No 30083/10, 7 June 2016**, §§ 114-117, 119 ***Ships Waste Oil Collector B.V. and Others v. the Netherlands* App Nos 2799/16, 2800/16, 3124/16 et al., 1 April 2025**, § 160	The fact that evidence was lawfully obtained in criminal proceedings and is admissible does not mean that it can also be used in disciplinary proceedings (or any other proceedings) if domestic law does not specifically provide for such use. Moreover, the potential transfer has to be necessary and proportionate and subject to oversight.
***Seppern v. Estonia* App No 31722/22, 16 September 2025**, §§ 48-53	Finding the evidence inadmissible does not automatically exclude the use of an intercepted telephone call to assess the defendant's credibility and potentially exclude his statement as unreliable, if the defendant has the right to explain himself and question the authenticity, reliability or accuracy of that evidence either before the domestic courts, or in the proceedings before it, and there is also other evidence justifying the conviction.

Cross-border Interception of Telecommunications and Cooperation	
***Wieder and Guarnieri v. United Kingdom* App Nos 64371/16 and 64407/16, 12 September 2023**, § 95	If the intercepting, searching and examining of the intercepted data take place in a particular State, the fact that the person under surveillance is outside its borders does not exclude the State's responsibility for interfering with the data.
***Centrum för rättvisa v. Sweden* App No 35252/08, 25 May 2021**, § 276	Cooperation between States in cases of bulk interception requires some additional safeguards, such as: - specifying in domestic law conditions under which data may be transferred, - ensuring that the receiving State can safeguard the data from abuse and disproportionate interference, - restricting onward disclosure of transferred data, - a special safeguard for confidential communications, - independent judicial control of the transfer.
***Knopp v. Hungary* App No 22931/18**, case pending, submitted to the Grand Chamber	The case concerns interception carried out at the request of a third country and the associated guarantees and safeguards. In particular, it addresses the defendant's access to data collected by his State of nationality on behalf of another State.

ii. *CJEU Case Law*

The following section provides an overview of the key points stemming from the case law of the Court of Justice of the European Union relating to communications interception and cross-border cooperation in such cases.

Competent Authority, Consent and Judicial Oversight	
Case C-584/19, Criminal proceedings against A and Others, 8 December 2020, §§ 74-75	The terms ‚judicial authority' and ‚issuing authority' under the EIO Directive include prosecutors or, more broadly, public prosecutor's offices of a Member State, notwithstanding the fact that they may be subject to instruction from the executive.
Case C-746/18, Prokuratuur, 2 March 2021, §§ 51-54	A prosecutor, as an authority conducting criminal proceedings, is not neutral in those proceedings and therefore is not able to carry out the prior oversight required for getting access to data relating to electronic communications.
Case C-724/19, Criminal proceedings against HP, 16 December 2021, §§ 35, 39-45, 47-55	An EIO can only be issued by the authority competent to order a particular measure under domestic law. The executing authority cannot remedy the defect in an EIO issued by an incompetent authority in the issuing State by carrying it out.

Case C-349/21, HYA and Others I, 16 February 2023, §§ 50-54 **Case C-229/23, HYA and Others II, 13 June 2024**, §§ 42-44	Request for special investigative measures (incl. interception of telecommunications) should include grounds for the application so that the court could assess whether the conditions are met. Because of that, the ruling court is not obliged to provide its own written reasons. It is assumed that it adopts the grounds for application as its own unless the domestic provision provides otherwise. This by no means implies that domestic courts can dispense with the requirement for written reasons under EU law, nor does it imply that a domestic provision imposing such an obligation is contrary to the EU law.
Case C-635/23, WBS GmbH, 10 July 2025, §§ 44, 65	The EIO can be issued by another competent authority specified by the issuing State (e.g. an administrative authority), if this body acts as an investigative authority in criminal proceedings and its investigative measures involving an interference with the fundamental rights of the person concerned must, in accordance with national law, first be authorised by a judicial authority.
Necessity, Proportionality and Scope of Intervention	
Case C-207/16, Ministerio Fiscal, 2 October 2018, §§ 57-61	Competent authorities can access personal data (i.e. name, surname and address), excluding communications content to identify an owner of a particular SIM card, even in cases involving minor offences.
Case C-623/17, Privacy International, 6 October 2020, §§ 78-82	Traffic and location data access in a general and indiscriminate way cannot be found strictly necessary under EU law, even if the reason for such access is national security.
Case C-746/18, Prokuratuur, 2 March 2021, §§ 38-40	Access to traffic and location data is, in principle, a serious interference with an individual's right to privacy, as it makes it possible to obtain precise information about their personal life, and therefore it is all the more essential to justify such access in terms of proportionality and strict necessity.

Case C-140/20, Commissioner of An Garda Síochána, 5 April 2022, §§ 98-100	When traffic and location data are obtained as part of general and indiscriminate retention for national security reasons, they cannot also be used to fight serious offences simply because they were already obtained.
Case C-162/22, Lietuvos Respublikos generalinė prokuratūra, 7 September 2023, §§ 41, 44	Lawful access to telecommunications data by investigative authorities to combat serious crimes does not mean that the data can also be used in different proceedings of lesser importance.
Case C-178/22, Procura della Repubblica presso il Tribunale di Bolzano, 30 April 2024, §§ 50-58, 60-62	The term 'serious offence' may be defined by reference to the statutory penalty, and this does not in itself violate the principle of proportionality. However, such a definition cannot prevent the competent authorities from refusing to grant access to telecommunications data if the offence turns out not to be serious in practice even though the statutory penalty meets the relevant threshold. In other words, the assessment of whether the offence is serious cannot be limited to the statutory penalty.
Case C-548/21, Bezirkshauptmannschaft Landeck, 4 October 2024, § 110	Access to telephone data can be obtained to prevent, investigate, detect and prosecute all crimes if the catalogue of crimes is precisely defined in national law, the requirements of the principle of proportionality are met, and the use of the measure is subject to prior independent review.

Retrieving and Transferring Data from Encrypted Platforms	
Case C-670/22, EncroChat, 30 April 2024	• A prosecutor can issue an EIO to obtain data, if they are competent to order the transmission of that evidence in a domestic case (§§ 73, 77). • An EIO can be issued only if the transmission could have been ordered under the same conditions in a similar domestic case (§§ 91-93). • If the issuing authority wants only to obtain already gathered evidence, it is not entitled to assess the correctness of the procedure under which the evidence was obtained in the executing State (§ 100). • A measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitutes an 'interception of telecommunications' (§ 119). • If the notifying State cannot identify the competent authority to be notified of the interception without technical assistance, it can notify any authority that it considers suitable, and the notification should be forwarded to the competent authority (§§ 117-118). • To protect its sovereignty and individual rights, the notified State can object to interception if such interception would not be possible in a similar domestic case (§§ 123-124). • An EIO seeking the transfer of evidence already collected in another Member State can be issued even if, at the issuing stage, the integrity of the data cannot be verified because of the confidentiality of the interception technology (§ 90). This does not prejudge the subsequent assessment of the evidence's reliability, authenticity or admissibility. The right to a fair trial must be safeguarded in the subsequent criminal proceedings, incl. the defence's ability to challenge the evidence (§§ 128–131).

Admissibility and the Possibility of Challenging the Evidence	
Case C-419/14, WebMindLicences Kft., 17 December 2015, § 91	The judicial authority is obliged to disregard the evidence if it is not possible to assess whether it was lawfully obtained. The court should also take into consideration (esp. when the evidence was obtained in different proceedings) whether the party had assessed that evidence and could potentially challenge it in the current proceedings. If not, it should be disregarded.
Joint cases C-203/15 and C-698/15, Tele2 Sverige AB, 21 December 2016, § 120	The individual should be informed about data retention for purposes of criminal proceedings when doing so no longer endangers the proceedings, in order to guarantee that person an effective legal remedy.
Case C-310/16, Dzivev and Others, 17 January 2019, §§ 37-39	The court can disregard evidence under a domestic provision when the measure (incl. telecommunications interception) requires prior judicial authorisation and the authorisation was granted by a court that lacked jurisdiction, even if using the evidence would have made the criminal proceedings more efficient.
Case C-189/18, Glencore Agriculture Hungary Kft., 16 October 2019, §§ 51-56, 65	The ability to challenge the evidence requires an opportunity to review it personally, incl. evidence that the investigative authority does not use but that may be useful to the defence. However, the party's right of access to the evidence is not absolute and can be restricted. This also applies to the court.
Case C-746/18, Prokuratuur, 2 March 2021, § 44	The assessment of evidence should be carried out through the prism of compliance with EU law, in particular the risk of breach of the adversarial principle and, therefore, of the right to a fair trial. If a court takes the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and that is likely to have a preponderant influence on the findings of fact, it must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement.

Case C-852/19, Gavanozov, 11 November 2021, §§ 56, 62	The lack of an effective legal remedy against an EIO in the issuing State that enables the individuals to challenge, at the very least, the substantive reasons for issuing that EIO constitutes an infringement of the right to an effective remedy and therefore precludes the issuing State from issuing such an EIO.
Case C-670/22, EncroChat, 30 April 2024, § 131	National criminal courts are required to disregard information and evidence in criminal proceedings against a person suspected of having committed criminal offences if that person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.
Case C-548/21, Bezirkshauptmannschaft Landeck, 4 October 2024, §§ 120-121	The competent national authorities should inform the data subjects of the grounds on which that authorisation was based, as soon as such information is not liable to jeopardise the investigations carried out by those authorities, and make available to them all the information referred to in Article 13(1) of Directive 2016/680. That information is indeed necessary to enable those persons to exercise, inter alia, the right to a remedy.

IV. Practical Guidance to Help to Understand What 'Interception of Telecommunications' Means

Assessing what to consider interception of telecommunications helps choose the appropriate framework and the associated level of safeguards, which differ from those applicable to other, less intrusive measures.

Below are a few examples of what 'interception of telecommunications' entails:

- A prosecutor is aware that the suspect in the case he is handling is currently in Slovenia and is using that country's telecommunications networks. He is therefore requesting that Slovenia intercept and forward any future telephone calls made by that person.
- The investigating authorities have ordered a specific telephone number to be monitored for the next two weeks in order to record all text messages sent and received during that period.
- Two suspects agreed on the details of a drug shipment via WhatsApp, and the investigating authorities gained access to the conversation whilst it was taking place.
- Members of an organised criminal group exchange messages via group chats on Messenger or Signal, whilst the investigating authorities, unbeknownst to them, receive the newly sent messages.
- The authorities covertly gain access to the suspect's mobile phone and, using software installed on it, intercept their communications via an online messaging service[1].
- As part of a covert phone surveillance operation, the authorities collect data on communications via an internet service: call durations, callers' IDs, and their associated locations, but they do not obtain the content of the calls.
- A public prosecutor's office has asked foreign authorities to intercept communications for a month.

[1] Classifying this measure as interception for the purposes of EU judicial cooperation does not establish its permissibility under national law. Such measures require a specific domestic legal basis and appropriate safeguards, which may differ significantly between Member States.

- Whilst driving, the suspect calls an accomplice. The authorities, with the help of the telecoms operator, intercept the call.

The following will not be regarded as 'interception of communications':

- Investigating authorities request the disclosure of existing telephone bills, call logs or historical traffic and location data already held by a telecommunications provider[2].
- The police use a GPS tracking device fitted to a car solely for the purpose of monitoring the route taken, without accessing any correspondence.
- The police seize the suspect's mobile phone, thereby gaining access to text messages, chat messages and emails.
- Investigating authorities are granted access to the mobile phone in order to obtain stored data, not data relating to correspondence.
- Investigating authorities decrypt data that has already been lawfully collected through interception and transmitted.

Borderline cases:

- Authorities install a microphone in the car. The passengers talk without using their mobile phones. The recording is transmitted in real time to the police, and the car enters another Member State.
- The user taps 'Send'. The software copies the message from the phone's memory before it is encrypted and sent over the network. It copies it again on the recipient's device shortly after the transmission is complete.
- The authorities receive up-to-date information about the base station to which the phone is connected or use an IMSI catcher to identify the device. They do not intercept calls or messages.
- The programme records keystrokes or takes screenshots. The suspect writes a message but deletes it and never sends it.

[2] An EIO seeking historical traffic and location data is dealt with under the general EIO regime, as indicated in recital 30 of Directive 2014/41/EU.

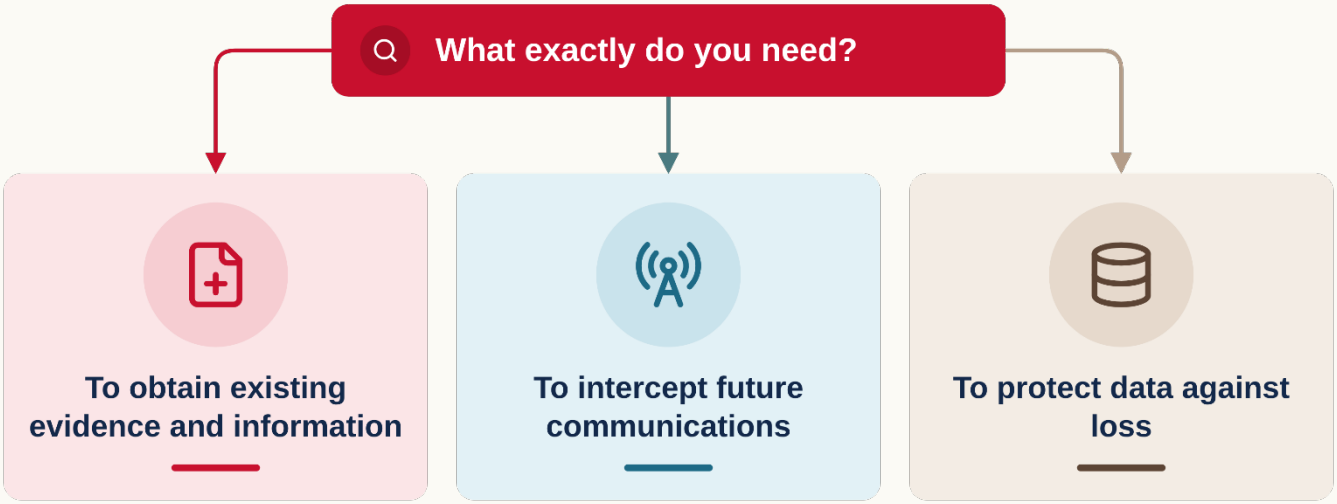
In the above cases, neither the law nor case law allows for an unequivocal determination as to whether interception is taking place. It should be noted, however, that the term ‘interception of telecommunications’ is being interpreted ever more broadly. The best approach in such cases will therefore be to make use of the consultation mechanism and agree on a course of action with the State whose cooperation is required, taking into account domestic provisions.

What if the investigating authorities in one Member State wish to access communications data that has already been collected in another Member State, but which was obtained through the interception of telecommunications?

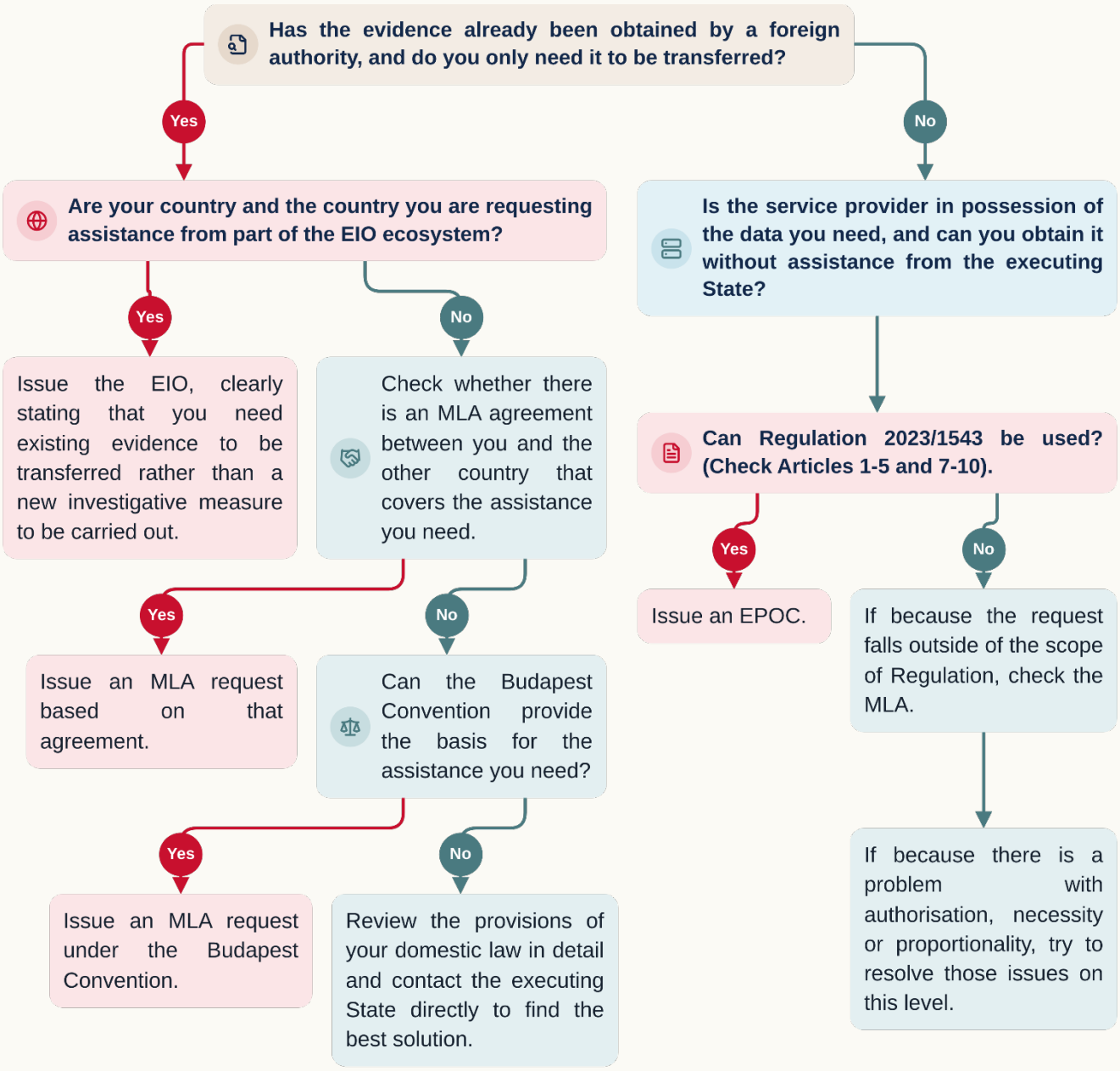
In such a case, it would be appropriate to make use of the general EIO regime. However, such action must not be intended to circumvent the restrictions imposed by national law. For example, if, in the case for which the evidence is being obtained, the interception would not have been permissible, the evidence obtained in this way may prove to be inadmissible.

V. Practical Guidance to Find Most Appropriate Cooperation Instrument

Choosing the appropriate measure is a crucial step once it becomes clear that cooperation with another State is needed and may involve interception of telecommunications. Making the right choice can simplify and accelerate the procedure but requires navigating a complex set of rules. It is therefore useful to begin by answering the following questions:



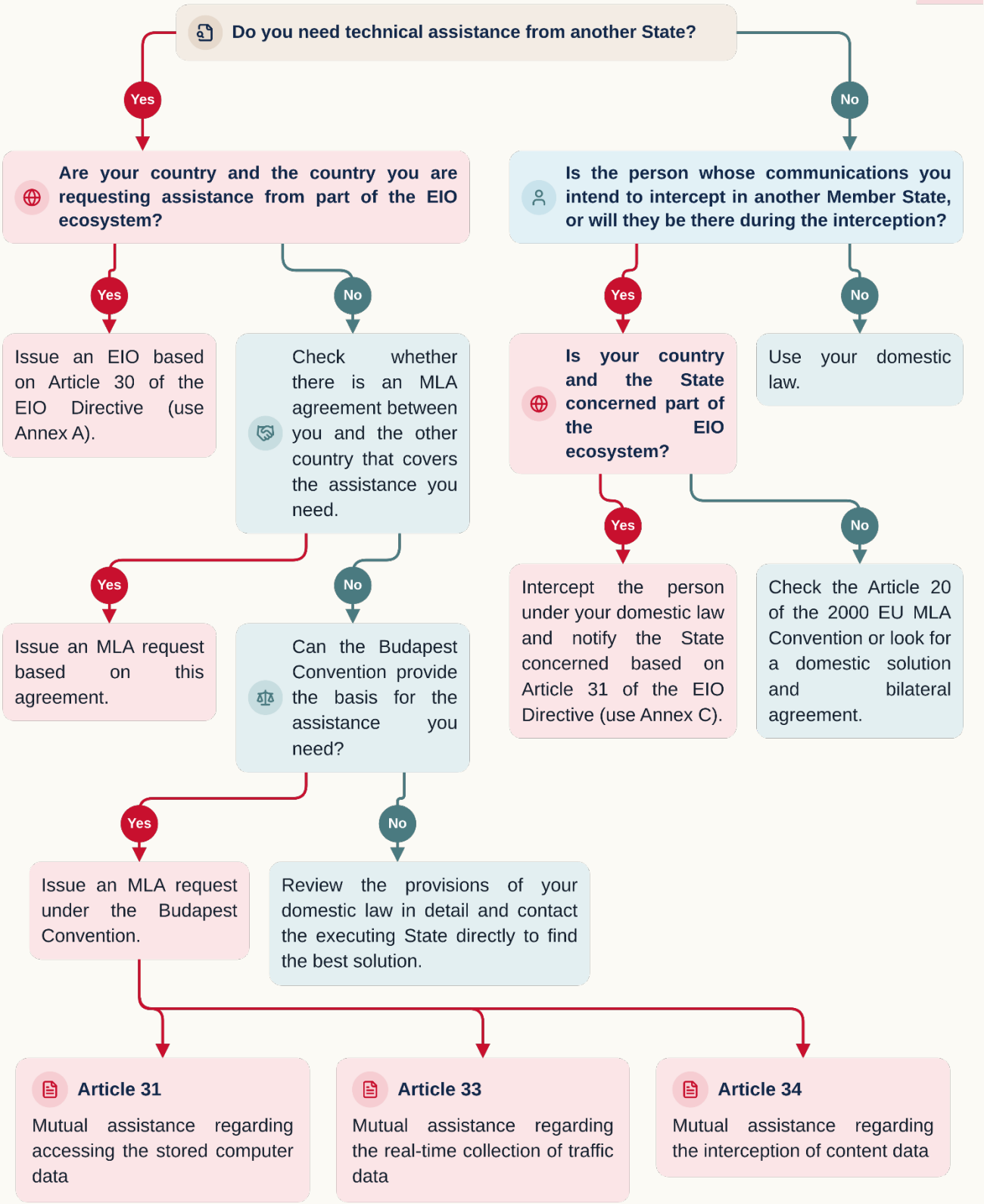
If you need to obtain existing evidence and information



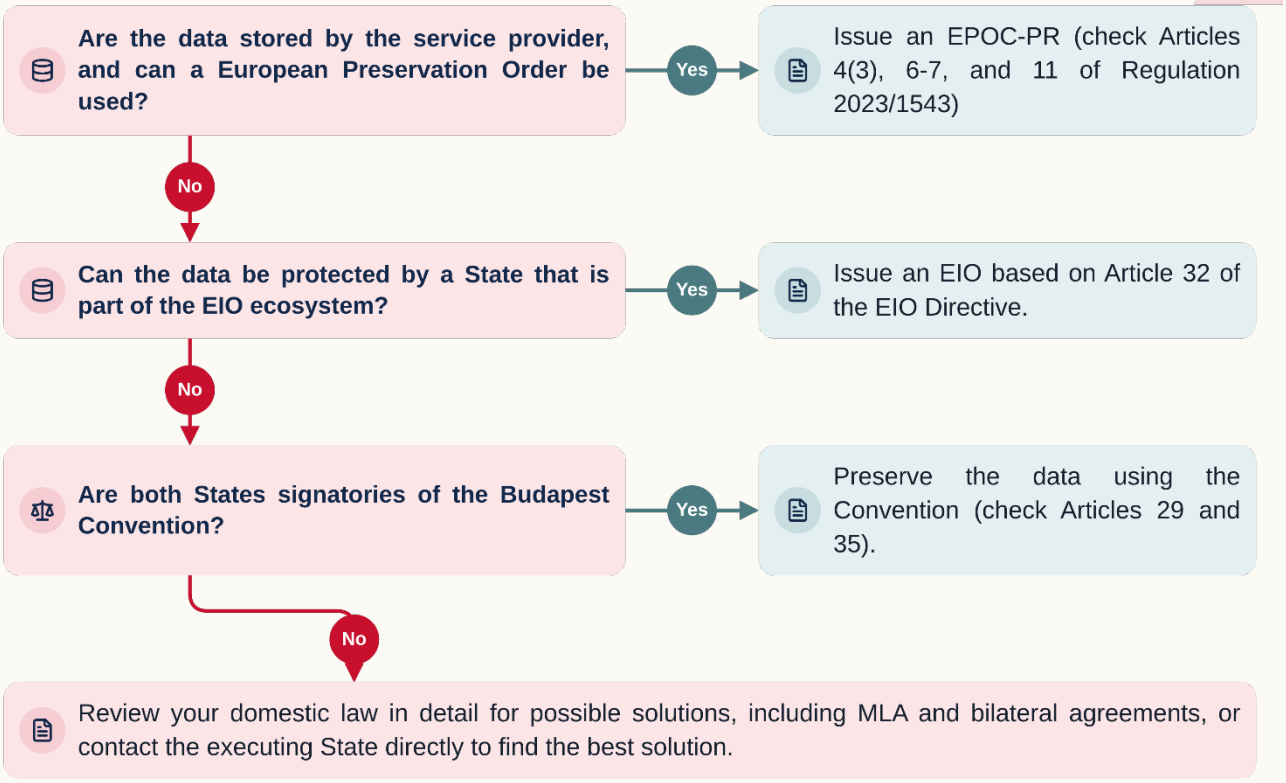
If you only need to obtain existing operational information (e.g. name, ID, or connection between individuals) that may be held by the police department, consider using SIENA Network (if already implemented), provided that the police in your country are also involved. It offers a much faster way to obtain information and also enables contact with Europol. You can also use this channel to check whether the evidence you need exists.

However, it is worth noting that Directive 2023/977 does not in itself authorise the use of the information obtained as evidence, although the executing authority can grant such permission.

If you need to intercept future communication



If you need to protect data against loss



VI. Good Practices to Help Resolve the Most Common Challenges in Interception Cases and Cross-Border Cooperation

i. Legal Framework and Procedural Requirements

Identifying the Competent Authorities and Ensuring Valid Judicial Involvement

Recommended Approach:

- Before drawing up an EIO, check the national legislation to determine which authority should issue the EIO in the case in question and whether national legislation requires the EIO to be approved by any other authority.
- Use the Atlas and Fiches Belges compiled by the EJN to identify the competent authority, the legal framework and any special requirements (https://www.ejn-crimjust.europa.eu/ejn2021/AtlasChooseCountry/EN).
- Find out in the country to which your EIO is being sent, who exactly will carry it out, and try to establish immediately whether the form is complete or whether the national law of the executing country requires any additional documents.
- If you receive an EIO intended for another authority in your country, forward it to the competent authority and inform the issuing State of this, rather than returning the EIO on the grounds of lack of jurisdiction. This is one of the good practices often highlighted in the INCEPT project, as returns for this reason continue to occur, causing delays in cooperation.

Reconciling Different National Conditions for Interception

Recommended Approach:

Before drafting an EIO, clearly identify what you need to establish and which data will help you do so:

Subscriber data —> Who is the number or account registered to?

For example, the subscriber's name and registration details. This does not necessarily identify the person who actually used it.

Location data —> Where is or was the device at the relevant time?

For example, data indicating a phone's location when a call was made.

Traffic data —> Which numbers or accounts communicated, when, and for how long?

For example, call logs showing the numbers involved, the date, time, and duration of the calls.

Content data —> What was actually said, written, or sent?

For example, a recorded conversation, the text of a message, or an email attachment.

- Before issuing the EIO, try to establish what the grounds for interception are in the executing State, for which offences it may be used, and whether there are any specific requirements or restrictions. A good approach recommended by practitioners is, where possible, to run prior consultations with the executing State and also use informal channels of communication with the authorities of the executing State in order to obtain information about the conditions of the measure prior to the issue of an EIO.

- Using Annex A, explain the purpose for which you need to carry out the interception, the subject matter of the case in question, how the persons being intercepted are connected to it, and why this measure is necessary to obtain the data.

- Specify precisely who is to be intercepted, or who, under the national law of the issuing State, may not be intercepted, in order to avoid, for example, a situation in which interception is carried out as an alternative measure against a witness, the admissibility of which varies from country to country.

- Indicate at the initial stage, preferably in the application for the measure, whether you would accept the use of an alternative measure, provided it achieves the same evidential purpose.
- In the case of a refusal to execute the measure, clarify directly with the executing State the grounds for the refusal and whether there is an alternative measure available under the executing State's domestic law that could be used to achieve similar results. If necessary, seek advice from the relevant units at Eurojust or Europol.
- Before submitting another EIO to a particular country, find out what problems arose with its execution previously, what was required to carry it out, and take the necessary steps in advance.

Divergent Application of Article 31 and Annex C

Recommended Approach:

- Identify the correct recipient of Annex C before initiating the operation.
- If it is known during the authorisation that a person is abroad, notify this before the operation begins (this is a preferable way). In all other cases, notify immediately upon receiving the relevant information.
- Retain the delivery confirmation and designate a person who is available to provide clarification promptly.
- As the notified State, clarify any omissions without delay and communicate any decision under Article 31(3) within the prescribed time limit.
- Communicate any decision to terminate the interception or restrict the use of the material immediately to the issuing State.

However, it is noteworthy that one of the problems identified in the INCEPT project is the ineffectiveness of Annex C. Practitioners pointed out that they practically never receive it, and they themselves rarely send it unless technical assistance is needed.

The issue of the consequences of notification's failure remains a significant problem. For example, the Berlin Regional Court, in its order of 1 July 2021 (525 KLs 10/21), explicitly stated that a breach of the obligation to provide notification in the context of legal assistance alone renders the evidence obtained inadmissible. Similarly, Berlin Regional Court I in its judgment of 19 December 2024 (525 KLs 8/22, 279 Js 30/22), held that a breach of Article 31 results, in this specific case, in the evidence being inadmissible. However, both judgments were set aside by higher courts for various reasons. In turn, in proceedings before the Supreme Court of the Czech Republic, the defendants invoked the inadmissibility of the evidence on the grounds of a failure to provide notification. However, in its judgment of 21 April 2026 (11 Tdo 178/2026), the Court did not uphold the objections concerning the use of Sky ECC communications.

ii. Operational Cooperation and Institutional Capacity

Preparing Requests that are Sufficiently Clear, Complete and Technically Precise

This is one of the issues that recurred most frequently at various stages of the INCEPT project and was raised both by representatives of the issuing authorities, who have difficulties completing the forms, and by representatives of the executing authorities, who often struggle to understand what the cooperation is supposed to involve. By combining these two perspectives, it has been possible to develop a number of good practices in this area, which may prove useful not only for EIOs relating to interception, but also for completing Annex A in general.

Recommended Approach:

- Describe in detail the offence allegedly committed by the suspect. This is important for any EIO, but it is particularly crucial in the case of interception, as this is an operational measure used only in relation to specific types of offences, which are often set out in an enclosed list that may vary from country to country.

- It will not be sufficient to state the domestic legal qualification or to describe the act using only statutory categories. Limiting the description to the content of the charge may also prove insufficient. In this section, the focus should be on the facts: it is necessary to specify exactly what the proceedings concern and what the alleged perpetrator is accused of. The description should be factual, not legal.

- It is best to use language that is as simple as possible, so that the authority in the executing State can understand the subject matter of the case without undue difficulty and relate the circumstances described to its own domestic law. This will enable it to determine whether it could authorise interception in a similar case. For if interception were not permissible in a similar domestic case, this would constitute one of the grounds for refusing to execute an EIO relating to interception. The description of the offence is therefore intended to persuade the executing authority to carry out this measure, rather than merely to formally indicate which offence is at issue.

- Describe in detail what actions you expect the executing State to take, by when they should be carried out, what outcomes are intended to be achieved, and in what form and format you would like to receive those outcomes. In this way, it can be ensured that the EIO will not only be executed but will also provide expected results. A detailed description of how the measure is actually to be carried out will also help the executing State to identify the most appropriate legal basis for its execution under domestic law.

- Attach the domestic authorisation, if one was issued in the case, together with a translation. If the national ruling was issued with a justification, also attach that justification, together with a translation.

- Submit any other relevant supporting documents, together with their translations, alongside the EIO. Whilst this is not a requirement, it certainly speeds up the process and reduces the need for additional correspondence, which is not always necessary.

- If you anticipate complications, explain in advance how privacy is protected and how the right to a fair trial is guaranteed. Also indicate how the proportionality and necessity of the measure have been assessed in the specific case, and why these conditions are met. In this instance too, refer to the specific circumstances of the case.

- Involve a digital forensics expert as soon as the decision to request interception is taken, not only after the material has been received. The expert should take part in drafting the EIO, not merely review it afterwards.

Meeting Operational Urgency Despite Delays in Cooperation

Recommended Approach:

- One of the problems identified in the INCEPT project was that urgency is indicated without any justification and, as it often turns out later, unnecessarily. This leaves the executing authorities unable to prioritise their actions. If a request for cooperation is genuinely urgent, it must be marked as such, and the urgency must be justified by specific circumstances (Section B of Annex A). Otherwise, such a designation should be omitted. The preferred or required deadline for carrying out the measures should also be specified, particularly if there is a risk that the suspect may change their whereabouts. Whilst this will not resolve the systemic problem, highlighted throughout the project, of excessively long deadlines for executing an EIO, it may help to obtain the desired information in a timely manner.

- Name a specific contact person for matters relating to the issued EIO and identify such a person in the executing State, so that the exchange of information can take place as efficiently as possible. Better coordination of communication, particularly by basing it on direct contact between the designated persons, can also help to resolve any issues that arise efficiently.

- Agree with the executing State on a channel for communication regarding this matter.

- Follow up to monitor progress and any delays in implementation and take remedial action.

- In the case of significant difficulties or problems, seek assistance from the EJN or Eurojust.

- In case of delays or no reply, if you know the service provider's data, check whether it is possible to use EPOC to retrieve the existing data or EPOC-PR to secure it. Although it is not possible to carry out interception on this basis, in certain cases existing data can be obtained within 8 hours.

- As the executing State, send confirmation of receipt of the EIO immediately upon its delivery (Annex B). The lack of information as to whether the EIO had reached the executing State was one of the problems identified in the INCEPT project.

Coordinating Execution, Renewals and Responsibilities Across Jurisdictions

Recommended Approach:

- As the executing State, inform the issuing State of any potential difficulties that might result in the interception being interrupted, before they arise, if possible.
- As the executing State, if it is not possible to carry out the action requested in the case and you decide to carry out an alternative action, consult the issuing State first. Reaching a consensus on this matter should be the basis for proceeding, and communication should be efficient so that the measure can be implemented as soon as possible.
- As the executing State, determine whether live transmission is required, or whether it is acceptable to record the results and transmit them later, if this has not been specified in the application.
- As the issuing State, appoint a person responsible for monitoring the duration of the measures and for assessing whether cooperation will still be required after that time.
- As the issuing State, take action well in advance in case it becomes necessary to extend the application of the measures; check with the executing State whether this is possible and under what conditions.

iii. Access to Data and Technical Feasibility

Obtaining Effective Cooperation from Service Providers

Recommended Approach:

- Before sending a request, identify the relevant service provider, data categories, and time period.
- Check the correct channel and whether the service provider is likely to hold the type of data you are seeking.
- If your request is refused, establish the reason: incorrect recipient, lack of account identification, data deletion, incorrect legal basis, or a technical obstacle. Only then should you amend the request or change the method of cooperation.

Encryption and Uncertainty About Technically Feasible, Lawful Alternatives

- Messaging apps such as WhatsApp, Signal and iMessage offer their users end-to-end encryption (E2EE). This means that only the sender and recipient have access to the content of the messages, as only they possess the special keys required to decrypt them. These keys may be one-off, meaning that even if a device and the key are obtained, it may not be possible to access the message content (e.g. Signal). At present, however, an even bigger problem is so-called ‘disappearing messages’, which are automatically deleted after a certain period of time.
- Encryption, even E2EE, whilst it is true that it prevents access to the content of a conversation, does not prevent the retrieval of information regarding whether a conversation took place, between whom, and when.
- E2EE may remain effective against both passive and active network interception. Infiltrating an endpoint, such as a user’s device, may instead provide access to plaintext before encryption or after decryption. This is a distinct investigative technique requiring a specific domestic legal basis and appropriate safeguards, which may differ between Member States.

- E2EE does not cover a backup copy of a message if one is created and not manually secured.
- Messages used by other applications that may be linked to messaging apps, such as those offering auto-correct services, will also not be covered by E2EE.
- Different operators use different technologies, particularly email providers. Basic email services use encryption in transit, which means that it is the data in transit that is encrypted, not the data stored in accounts; consequently, the email provider or cloud operator has access to the data in such cases. It is therefore worth trying to gather messages exchanged using different types of encryption.
- Encryption does not necessarily have to be overcome at the time of interception. The material intercepted may be decrypted at a later date, as in the Belgian case before the Court of Cassation of 31 October 2023 (P.23.0998.N), when communications intercepted abroad and handed over to the Belgian authorities, including PCAP files containing a record of network traffic, were eventually decrypted.

EncroChat

An interesting example of circumventing E2EE is the EncroChat case. A judgment of the British Court of Appeal of 5 February 2021, A, B, D & C v Regina, [2021] EWCA Crim 128, describes how the French authorities used the EncroChat infrastructure to deploy a backdoor under the guise of an update. According to the findings in those proceedings:

- first, data already stored on the device was retrieved,
- then, new messages were collected,
- the content was copied from the devices in plain text: either before encryption at the sender's end or after decryption at the recipient's end.

German case

Meanwhile, in the German case involving an investigating judge at the Federal Court of Justice, on 9 July 2020 (2 BGs 468/20), the court heard a case in which the parents of a suspect had handed over their mobile phones to the police so that officers could secure messages from their daughter. On that occasion, access was also granted via WhatsApp Web, enabling to monitor, record and analyse all messages sent or received via WhatsApp, as well as previous messages from chats that were still stored on the messaging app on a computer at the Federal Criminal Police Office. This action was subsequently deemed unacceptable due to the lack of consent from the individuals concerned and the resulting breach of family ties.

Unequal Technical Capabilities and Incompatible Systems

Recommended Approach:

- Specify the requested data format in the EIO (e.g. ETSI LI HI2/HI3 or PCAP, or the executing authority's own format accompanied by its specification), as well as the required metadata, the encryption method and the method of access. Without this, the material may be delivered in a national format that cannot be read without specialised software.
- Check whether office computers will open the suggested links and file formats and communicate potential problems.
- If you are unable to open the data you have received, contact the executing authority immediately to arrange for the data to be transferred by alternative means. If you attempt to convert the data, retain the original version you received and document the steps you have taken.

Data Volatility and Different Retention Practices

Recommended Approach:

- Determine the actual availability of the data and the deadlines for its deletion with the relevant provider as early as possible.
- Do not wait until the full data disclosure request has been finalised if there is an appropriate means of securing the data urgently.
- Check whether Article 32 or the relevant procedure under the Budapest Convention applies, including assistance from the 24/7 contact point.
- Obtain confirmation of the scope of the preservation and its expiry date; appoint a person responsible for the subsequent request for disclosure.
- In the case of EPOC-PR, monitor the time limits set out in Article 11 of Regulation 2023/1543 — the preservation order itself does not yet mean that the data has been obtained.

iv. Handling and Transmission of Interception Materials

Language Barriers and Uncertainty About Translation Responsibilities

Recommended Approach:

- Before requesting a translation, check which language is accepted and provide the translator with explanations of technical terms.
- Agree with the other country on the scope of the transcription and translation, as well as responsibility for their completion and the associated costs.
- Ensure that each section of the transcription is linked to the recording and that any illegible or uncertain sections are marked.
- Distinguish between literally spoken words and interpretations of jargon or code. If the meaning is unclear, establish the basis for the interpretation and consider seeking a specialist's opinion.

Handling Classified Materials and Differing Confidentiality Arrangements

Recommended Approach:

- Before handing over the document, determine its classification, authorised recipients and the conditions governing access, copying and disclosure. Clarify in advance how the material will be made available to the court and the defence.
- Confirm with the person responsible for information security the acceptable transmission channel and storage location.
- If a single EIO covers both open and classified activities, consider a separate EIO relating to interception where disclosure of the document could jeopardise the operation.
- Establish in advance whether the executing State will inform the suspect of the EIO that has been issued and of the investigative measures being carried out (esp. when using alternative measures). The national legal framework and approach to the confidentiality of such measures vary from country to country. If, as the issuing

authority, you wish to ensure that the suspect does not become aware of the proceedings against them, it is worth checking in advance whether it will be possible to keep them confidential.

Preserving Authenticity, Integrity and Chain of Custody

Recommended Approach:

- Request in the EIO itself hash values (e.g. SHA-256) for each file and for the whole package, and all timestamps in UTC with the time source indicated. Without them, the integrity of the material may be impossible to confirm in court, and interception logs may not match the operator's logs.
- Upon receipt, draw up a list of files, sources, time ranges, metadata and documentation.
- Agree with the IT specialist on the method for calculating and comparing checksums. Store the records in a way that prevents them from being overwritten.
- Retain the material received and work on labelled copies; document any decryption, filtering, conversion and other operations.
- In the case of checksum discrepancies or suspected tampering, secure the versions and request an explanation of the cause before basing your findings on the material.

v. Evidentiary Use, Defence Rights and Judicial Scrutiny

Ensuring that Material Obtained Abroad Can Actually Be Used as Evidence

Recommended Approach:

- Identify in the EIO the specific formalities required under the issuing State's procedures and agree on them before executing the measure.
- Determine the source of the material: whether it relates to a procedural measure, an operational check or intelligence activities, and the associated restrictions.
- Once you have obtained the data, check that the material received complies with the scope of authorisation: the subject, the period, the type of data and the conditions of use.
- Obtain from the executing State all the material gathered, even that which may prove to be irrelevant to the proceedings or exculpatory for the accused. The defence's inability to effectively challenge the measure and the evidence may render it inadmissible.

Clarifying Subsequent Use In Other Proceedings and Onward Sharing

Recommended approach:

- Note that further use of material obtained through interception depends on the applicable national law, the conditions of the original authorisation and any relevant restrictions arising from cross-border cooperation. In particular, check whether those rules require the new offence to be included in the list of offences for which interception may be authorised
- Before using the material for another purpose or passing it on to another authority, check the conditions of transfer, confidentiality restrictions and the relevant regulations. If consent is required, obtain it before reusing the material. Where the obligation is unclear, contact the executing authority and request written confirmation of the permissible scope of use; agree whether a separate application will suffice or whether a further EIO is required.

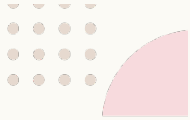
- Seek authorisation from the executing State whenever the data obtained includes personal data obtained from the other State and is to be transferred to a country outside the EU or to an international organisation.
- Eurojust and the EJN recommend making a separate request to the executing State before using the evidence for purposes other than those specified in the original EIO in any case.

Fundamental Rights Safeguards Issues

Interception is one of the most intrusive measures available to law enforcement agencies, and therefore the proportionality and necessity of the measure should be justified by referring to the specific circumstances, rather than merely to statutory categories. Interception-based measures should only be used where it is truly necessary, and there is no other way to obtain certain evidence. Providing adequate justification for proportionality and necessity was one of the challenges faced by the authorities ordering the interception, as identified in the INCEPT project.

Necessity and proportionality

FUNDAMENTAL RIGHTS SAFEGUARDS



Necessity

Why is it necessary to intercept communications in the first place? Can the specific information be reasonably obtained by a less intrusive means?

Proportionality

Do the gravity of the offence and the expected outcome justify the scope of the interception — the individuals concerned, the communication channels, the duration, and the intrusion into the privacy of others?

- For example, it cannot be considered that interception is necessary and proportionate if an existing recording is sufficient to establish certain facts, even if it is contained in the case file of proceedings in another country. Similarly, the use of interception covering too many different communication channels without a specific link between their use and the offence in question may be deemed disproportionate.

- In the ECtHR's case of Adomaitis v. Lithuania (14833/18), the use of interception was deemed necessary and proportionate, as the prison governor was suspected of accepting benefits in exchange for providing better conditions for specific inmates. The authorities demonstrated that their suspicions were well-founded and that the methods used to date had not been sufficient, partly due to the suspect's position.

- In the ECtHR's case of Lüdi v. Switzerland (12433/86), the use of interception was deemed necessary after the Swiss authorities received information from German officers regarding an individual seeking to finance the purchase of 5 kg of cocaine. The clarity of the information and the seriousness of the offence were deemed sufficient, even though the interception was intended to identify the transaction and seize the drugs. Nevertheless, it was held that, whilst the measure may have been necessary and proportionate, the standard of a fair trial had been breached.

- In the ECtHR's case of Karabeyoğlu v. Turkey (30083/10) it has been confirmed that the subsequent discontinuance of criminal proceedings does not in itself mean that the use of interception in the case was not necessary and proportionate.

- In the ECtHR's case of Dragojević v. Croatia (68955/11) it was, on the other hand, held that the absence of specific facts to justify that the use of an alternative measure would not be sufficient does not allow for the conclusion that the measure was necessary and proportionate. A similar finding was made in the case of Dudchenko v. Russia (37717/05), where there were insufficient facts to substantiate the suspicion.

VII. Changes Affecting International Cooperation in Matters of Telecommunications Interception in the Proposal to Amend the EIO Directive

The proposal to amend the EIO Directive (The Proposal for a Directive of the European Parliament and of the Council on the European Investigation Order in criminal matters and the European Order for Remote Participation (recast)) introduces several significant changes concerning cooperation in criminal matters, including cooperation on the interception of telecommunications. This sub-section provides an overview of the changes resulting from this proposal.

It is planned to include in the new Directive a broad definition of 'telecommunications', covering the content thereof and related data, transmitted via electronic communications networks or services as defined in the European Electronic Communications Code. There is an explicit reference to electronic communications law. The recitals, however, state that the mere transmission over a network of data collected by a device for the purpose of storage is not sufficient in itself to constitute the interception of telecommunications (recital 46). Separate definitions of 'investigating Member State' and 'notified Member State' are also to be introduced.

The provision concerning interception using technical assistance from another Member State includes the following amendments:

- The executing State is obliged to notify any discrepancy between the requested and the permissible duration of interception, as well as grounds for extension. If the issuing authority requests interception for a period longer than that authorised or permitted under the law of the executing State, the executing authority must immediately point out this obstacle.
- If the duration of the interception were to be extended, a new EIO would need to be issued.

However, further changes relate to interception without technical assistance, including, amongst other things:

- If a notification is forwarded to the wrong authority, that authority should respond within 24 hours by forwarding the notification to the competent authority and informing the investigative State accordingly.
- There is an obligation to provide additional information if it is necessary for the notified State to assess whether interception would be possible in a similar domestic case.
- A provision has been added allowing the deadline for a response from the notified State to be extended by a further 96 hours.
- It was pointed out that a failure to reply within the prescribed time limit should be taken to constitute a lack of objection.
- Continuing beyond the period specified in the notification requires a new notification.

The amended text of the Directive includes a provision that directly refers to the subsequent use and onward transfer of information or evidence and the use of previously exchanged information as evidence.

- Before using material for another purpose, authorities will need to check the restrictions communicated by the executing or notified State. Where such restrictions have been imposed under Article 21, prior consent will be required.
- Prior consent will also be required before transferring material covered by Article 21 to another Member State, a third country or an international organisation.
- Requests for consent for subsequent use or onward transfer will be made using Annex IV and will need to identify the material, the intended purpose and any proposed recipient.
- For previously exchanged police information or spontaneous judicial exchanges covered by Article 35, authorities will need to request consent using Annex VII where required by national law or the original transmission conditions.
- A decision will normally be required within 14 days, with a possible extension of up to 10 days. Postponement will also be possible where the relevant grounds persist.

- In an emergency under Article 21, immediate use or transfer will be permitted where an immediate and serious threat to public security prevents obtaining prior consent. The requested authority will need to be notified within 24 hours, with an explanation of the urgency.

- Consent will not remove the obligation to comply with national law, data protection requirements or applicable restrictions on use.

Other significant changes include:

- a clear obligation to specify the available remedies in Annex A;

- the strengthening of judicial review of EIOs and a specific section in Annex A to indicate whether such authorisation has been granted;

- a clear legal basis for requesting assistance from Eurojust and the EJN at every stage of the proceedings.

The amendment to the Directive also introduces another new measure which relates directly to the situation analysed in the INCEPT project, namely the situation in which a car fitted with a hidden microphone (‘technical recording device’) recording conversations inside the vehicle crosses a border. If the device has been lawfully installed in country A, and the car enters country B, and the continued use of the device does not require technical assistance from country B, the proposed Article 34 — notification to country B — will apply and it will not, in general, be considered interception of telecommunications.

To sum up, the proposed amendments partly address challenges identified as part of the INCEPT project, in particular regarding the use of evidence for other purposes, the definition of ‘interception of telecommunications’, the use of technical recording devices and the use of law enforcement information previously exchanged as evidence, and support some of the good practices set out in this manual.

VIII. Key Takeaways for Practice

For issuing authorities

1. Choose the appropriate procedure: new interception, transfer of existing material, or a notification under Article 31.
2. Confirm the addressee and identify a contact person before sending the documents.
3. Check the requirements of the other country. Clarify any doubts in advance with the competent authority, the EJN, or Eurojust.
4. Describe the purpose and scope of the request: what you need, from whom, from which number or account, for how long, and why other measures are insufficient.
5. Describe the subject matter of the proceedings in plain language, based on the facts.
6. Justify the urgency by referring to the dates and the needs of the case. Indicate what consequences a delay would have.
7. Agree on the implementation: technical capabilities, confidentiality, the method of transmitting results, and the file format that the recipient will actually be able to open.
8. Monitor receipt and deadlines. Follow up if there is no response; request an extension before the expiry of the investigation.

For executing authorities

1. Confirm receipt and identify the person in charge. If you are not the appropriate person, forward the document to the relevant authority and inform the sender.
2. Specify what is missing, rather than raising general objections. State what information or document you require and why.
3. Before refusing, discuss possible solutions to the problem: providing additional information, narrowing the scope, or applying an acceptable alternative measure.
4. Check the technical arrangements before starting. Agree with the contractors on the available tools, the support required, and how to hand over the material safely.
5. Report any obstacles immediately. State the reason for the delay, the proposed solution, and the expected deadline.
6. Provide the material with clear documentation: the scope and duration of the work, how it was obtained, and any conditions of use.
7. Before handing over the material, check for any protected material or material unrelated to the case, and apply the appropriate rulse for its separation and protection.





This deliverable was funded by the European Union under Grant Agreement 101192923. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.