CEPS Paper in LIBERTY and SECURITY in Europe

JUD-IT Handbook

Marco Stefan

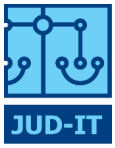
No. 2020-03, March 2020

Abstract

The JUD-IT Handbook provides a tool for judicial authorities, law enforcement actors, and defence lawyers to better navigate the complex legal and institutional framework governing cross-border cooperation for accessing and exchanging electronic information sought in the context of criminal proceedings. Based on the JUD-IT Project findings, the Handbook identifies ways in which existing instruments of criminal justice cooperation in the field of evidence gathering can be used in practice to request and obtain data held by service providers across borders. It does so through an overview of the main legal channels and actors to be involved in the issuing, validation, and execution of cross-border data requests within the EU and in transatlantic relations. The Handbook offers guidance that is of value for those concerned with ensuring that data are accessed, collected and exchanged across borders in full compliance with the fundamental right of individuals – including both suspects and accused persons as well data subjects – and admitted as evidence in criminal proceedings.

This Handbook has been prepared in the context of the JUD-IT (Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the author and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

Marco Stefan, PhD, is Research Fellow at CEPS Justice and Home Affairs Unit. The author would also like to express his gratitude to Sergio Carrera, Senior Research Fellow and Head of the CEPS Justice and Home Affairs Unit for his comments on earlier drafts of the Handbook. The authors would also like to thank Fabrizia Bemer, at the Prosecutor's Office of Court of Florence, and Laure Baudrihaye-Gérard, Senior Lawyer at Fair Trials Europe, who provided valuable inputs and comments on earlier drafts of the Handbook. A special acknowledgement goes to Ngo Chun Luk, PhD, for his work on the Handbook's infographics.



978-94-6138-765-3

Contents

List of abbreviations 4
1. Introduction 1
1.1 Why is the JUD-IT Handbook needed? 2
1.2 Who does the JUD-IT Handbook target? 3
1.3 Structure of the Handbook 3
2. The legal framework: how does it work? 5
2.1 Intra-EU cooperation: The European Investigation Order 8
2.1.1 Geographic and material scope 8
2.1.2 For which measures can EIOs be issued and executed? 9
2.1.3 Who can issue and execute EIOs entailing access to and collection of electronic information? 10
2.1.4 Issuing and execution of data requests under the EIO 12
2.1.5 At which stage of the proceeding can EIOs be issued/executed? 14
2.2 Mutual Legal Assistance 14
2.2.1 MLAs requests to Ireland 15
2.2.2 MLA requests to the US 18
3. Using the EIO for the purpose of accessing and exchanging data sought in criminal proceedings - Checklist for practitioners 24
3.1 Checklists for judicial practitioners 24
3.1.1 Practical use and relations with other instruments 24
3.1.2 Involving the competent judicial authority in the issuing state 24
3.1.3 Formulating 'quality requests' 25
3.1.4 Assessing legality, necessity and proportionality 27
3.1.5 Transnational coordination and direct judicial contacts 27
3.1.6 The execution of cross-border data requests under the EIO Directive 28
3.1.7 Urgent cases 29
3.2 Role and checklist for defence lawyers 30
3.2.1 Request the issuing of an MLA request or an EIO 30
3.2.2 Challenging the issuing of an MLA or EIO request 31
3.2.3 Challenging the execution of an MLA or EIO request 31
3.2.4 Challenging the probity or admissibility of the data obtained under the MLA or EIO procedure as evidence at trial 31
Annex I – Glossary 33

Annex II - EU data protection and criminal justice standards (Selected CJEU jurisprudence) .. 35
Annex III - Inventory 39
Annex IV - Methodological note 83

List of Boxes, Figures and Tables

Box 1. The principle of mutual recognition in criminal matters 8
Box 2. MLA vs direct access: the 'Microsoft Ireland' case 17
Box 3. US law and the probable cause 21
Box 4. Case Study: Apple's guidelines on emergency procedure 22

Figure 1. Criminal proceedings and cross-border data gathering: the available instruments 7
Figure 2. Issuing and executing EIOs: main steps and control points 13
Figure 3. MLA cooperation with Ireland 16
Figure 4. MLA cooperation with the US 20

List of abbreviations

AFSJ	Area of freedom, security and justice
CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Use of Overseas Data Act
CoE	Council of Europe
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EIO	European Investigation Order
EU	European Union
MLA	Mutual legal assistance
MLAT	Mutual legal assistance treaty
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union

1. Introduction

The exponential use of internet services for daily communications and activities has led investigating and prosecuting authorities (including both police and judicial actors)[1] to rely increasingly on the access to and collection of electronic information for the investigation and prosecution of crime. Different types of data[2] are currently sought after not only for the countering of 'cybercrime' (both target and content-related), but also for the investigation and prosecution of criminal offences in the 'offline world'.

If data stored by private service providers in different countries, or in the cloud, increasingly constitute valuable evidentiary sources, investigative measures targeting electronic information also raise several legal, procedural, and practical dilemmas that impose careful consideration.

The conditions and circumstances justifying law enforcement requests for data largely depend on national laws, which also identify the authorities competent for respectively issuing, validating, and executing such measures. National provisions regulating access to data for the purpose of investigating and prosecuting crime are linked to the notion of jurisdiction and its assertion over both individuals and companies holding the data sought. The concept of jurisdiction is connected to states' territory, but also with states' responsibility to investigate and prosecute crime while at the same time protecting the rights of citizens and individuals under their jurisdiction.

When it comes to access to data sought in criminal proceedings, the notion of jurisdiction therefore presents two distinct but closely intertwined ramifications:

- The first relates to criminal law and its enforcement in the context of criminal investigations and the prosecution of crime;
- The second pertains to fundamental rights law, which in the EU legal system guarantees both the right to privacy and data protection, and the rights of the defence/fair trial.

The transnational and cross-border nature of the internet is often a source of jurisdictional based practitioners seeking access to data in the context of criminal proceedings. A request for data that is lawful under the law of the issuing state, might not be considered so in the country where such measure has to be executed. Unilateral assertions of criminal jurisdiction in the field of data gathering can seriously harm trust in intra-EU and international relations, and expose individuals to risks of fundamental rights abuses.

At the international and EU levels, a number of instruments are available to investigating and prosecuting authorities, as well as to defence lawyers, seeking to cooperate among them in order to access and exchange obtain data across borders. Mutual Legal Assistance Treaties (MLATs) provide the possibility for judicial authorities to channel their requests for data through formal and centralised venues of international judicial cooperation. Regulating access

[1] See the glossary in this Handbook.
[2] Ibid.

to data in the fight against crime now also falls squarely under the sphere of EU competence, and specific norms developed at the Union's level currently apply depending on the specific purpose for which electronic information are sought. As far as collection of electronic information to be used as evidence in criminal proceedings is concerned, the European Investigation Order (EIO) allows participating member states to issue and execute cross-border evidence gathering measures based on the principle of mutual recognition of judicial decision.[3]

Both MLATs and the EIO rely on a model of judicial cooperation in cross-border evidence gathering which relies on the involvement of judicial authorities (including, depending on the specific case and stage of the proceeding, judges or prosecutors) in both the country of issuing *and* the country of execution of a request for data sought for criminal justice purposes. This 'mediated model' of judicial cooperation[4] is designed to allow investigating and prosecuting authorities to request, collect, and exchange electronic data, while at the same time preventing conflicts of laws and jurisdiction through the exercise of reciprocal oversight over cross-border enforcement of criminal justice decisions directed at gathering evidence across borders.

1.1 Why is the JUD-IT Handbook needed?

The JUD-IT Project research demonstrated that law enforcement actors, judicial authorities, and defence lawyers still struggle in mutually understanding the substantial and procedural conditions to be met in the EU and third countries in order to lawfully request, access and exchange electronic information held by private companies across borders or in the cloud. A major obstacle faced by practitioners is that they are often "lost in translation" due to the different constitutional traditions, legal terms and notions used across various countries.

And yet, compliance with the multi-layered set of national, international, and EU norms and standards regulating access to data in the context of criminal investigation is crucial to ensure that *electronic data* gathered across borders can be presented and admitted as *electronic evidence* before a court. Respect of EU criminal justice and fundamental rights standards is in particular required to all member states' investigating and prosecuting authorities, which, acting under the scope of EU law, seek to access data across borders (both within and outside the EU). These standards must also be respected by foreign authorities requesting electronic information (pertaining to EU citizens or not), or held by private companies operating under EU law. Furthermore, they are binding upon the service providers holding the data sought.[5]

The JUD-IT Handbook provides streamlined guidelines, explanations, comments and links to the legal provisions currently regulating access to data for criminal justice-related purposes. By

[3] See infra, Section 1.1.

[4] Carrera, C., González Fuster, G., Guild, E., Mitsilegas, V., (2015), 'Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights', CEPS Research Paper, https://www.ceps.eu/ceps-publications/access-electronic-data-third-country-law-enforcement-authorities-challenges-eu-rule-law/.

[5] Stefan, M., González Fuster, G. (2019),'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters: State of the art and latest developments in the EU and the US', JUD-IT State of the Art Report No. 1, https://www.ceps.eu/wp-content/uploads/2018/12/MSGGF_JudicialCooperationInCriminalMatters-2.pdf.

doing so, it addresses some knowledge gaps that hamper the full potentials and correct functioning of the instruments of judicial cooperation currently available within the EU and at the transatlantic level for the collection of data to be used in the context of criminal proceedings.

1.2 Who does the JUD-IT Handbook target?

The JUD-IT Handbook will be of help for judicial actors, legal practitioners, and law enforcement officials across the EU to navigate the existing legal and institutional framework in an easier way.

The Handbook outlines the main legal and administrative processes to be followed for the issuing and execution of investigative or prosecutorial measures directed at accessing, collecting, and exchanging data held by private companies across borders and sought in the context of criminal proceedings.

The categories of stakeholders that will benefit from the JUD-IT Handbook include EU member states' judges, prosecutors, and defence lawyers participating - in their respective capacity - in the issuing, validating and execution phases of cross-border requests for electronic information to be used as evidence in criminal matters.

1.3 Structure of the Handbook

The Handbook is comprised of two main sections. The first section provides textual and visual guidelines to the different EU law instruments available to EU member state investigating and prosecuting authorities, as well as to criminal defence lawyers for seeking and obtaining data across borders in the context of criminal proceedings. A number of text boxes are included throughout the first section of the Handbook to provide synthetic explanations of key legal concepts. The understanding of such legal concept is of central importance for the correct everyday use of existing instruments of judicial cooperation for cross-border evidence gathering in criminal matters.

The second section consists of checklists to help legal practitioners, including both investigating and prosecuting authorities,[6] and defence lawyers,[7] in the use of the existing EU judicial cooperation instruments – and most notably the EIO – to deal with the different legal, procedural and administrative challenges related to the issuing, validating, or execution of cross-border requests for data held by private companies and sough for criminal justice purposes.

[6] See Section 2.1 below.
[7] See Section 2.2 below.

The JUD-IT Handbook is complemented by three Annexes:

- A glossary with definitions of key actors and concepts pertaining to cross-border criminal investigations, and access to electronic information in such context (*Annex I*);
- A summary of selected case law of the Court of Justice of the European Union (CJEU) setting forth some of the fundamental rights standards to be taken into account in order for cross-border requests for electronic information sought in the context of criminal proceedings to be considered lawful under EU law (*Annex II*);
- An inventory providing a synthetic overview of relevant the national legal frameworks that EU countries covered by the JUD-IT Research have in place to regulate investigating and prosecuting authorities' requests for electronic information (*Annex III*);[8]
- A methodology section explaining the process followed to develop the Handbook (*Annex IV*).

[8] The results of the country-level research generated by the institutions involved in the JUD-IT national-level research is available – in the form of dedicated country briefs – on the JUD-IT Project website.

2. The legal framework: how does it work?

There are several different judicial cooperation instruments currently available for investigating and prosecuting authorities across the EU to request and obtain data sought in criminal proceedings.

The **European Investigation Order**,[9] the 2000 **Mutual Legal Assistance Convention**,[10] the 2013 **EU-US Agreement on Mutual Legal Assistance** (MLA),[11] and other bilateral MLATs in place with third countries such as the US are the most important judicial cooperation tools for mediated cross-border access to data held by private companies. All these instruments are based on the notion of judicial cooperation between competent authorities of the country of issuing and execution of a cross-border data request. Judicial cooperation and mediated access to data is at the heart of these EU and international cooperation instruments.

Besides the instruments mentioned above, the 2001 Council of Europe (CoE) Convention on Cybercrime (the so-called **Budapest Convention**) also provides a forum for cross-border cooperation in data gathering for law enforcement and criminal justice purposes. While largely espousing the mediated model of cooperation for cross-border data access, the Budapest Convention also foresees the possibility – under certain conditions and circumstances – for law enforcement authorities to address their requests for data (in the form of preservation and production orders) directly to service providers.[12]

In addition to the instruments mentioned above, other cross-border data-gathering tools (existing, or under discussion at the EU and international level) are designed in ways which provide (or would provide) the possibility for public authorities to request the data directly from private companies. These instruments propose an alternative model of cross-border data gathering which can be described of '**unmediated access**'. Instruments for unmediated access do not rely on the involvement of an authority mediating the submitted request in the country where the data-gathering measure is addressed and has to be executed.

This Handbook pays specific attention to the functioning of **existing EU law-based instruments of judicial cooperation for mediated access** to data and evidence gathering in criminal matters. These instruments currently encompass the European Investigation Order and the MLATs with the US. Given the practical relevance of cooperation with Ireland (which is not party to the EIO, nor signatory of the Budapest Convention) in the field of cross-border data gathering, attention is also paid to the functioning of MLA cooperation with this EU country.

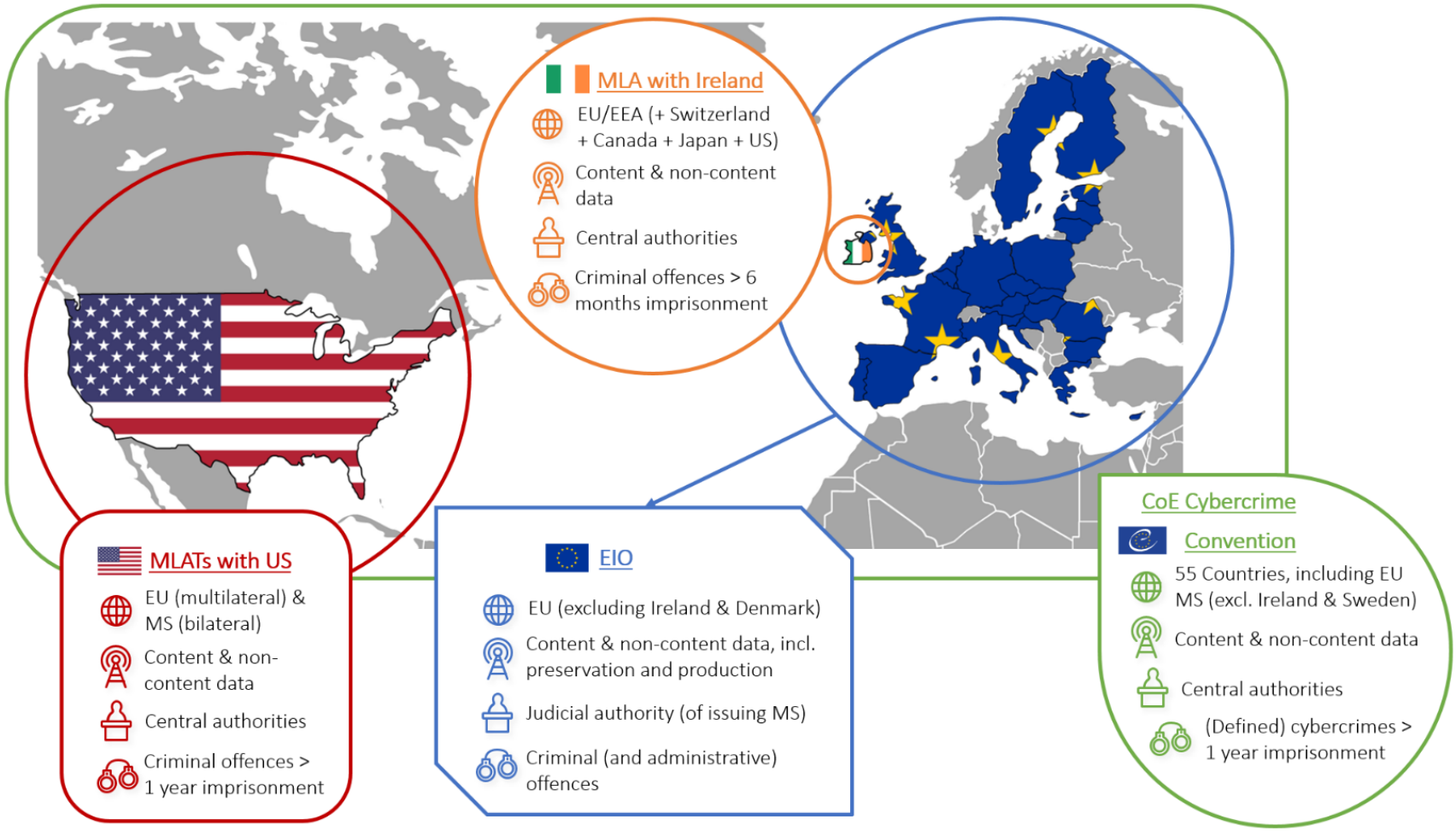
[9] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.
[10] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1 and its Protocol.
[11] Agreement of 25 June 2003 on mutual legal assistance between the European Union and the United States of America.
[12] See article 16, 17, 18 of the Budapest Convention.

Figure 1 below provides an **overview of the different legal instruments** currently in place to issue and execute cross-border measures entailing access to and collection of data held by private companies across borders, and the measures they cover. It also schematises their geographical scope of application, as well as the main categories of data that can be requested and accessed through them.

The existing EU instruments of judicial of judicial cooperation for cross-border gathering of evidence incorporate and must be interpreted and used in line with standing rule of law and fundamental right standards enshrined in EU primary and secondary law. Is important to recall that a number of **EU primary law safeguards apply across all areas of EU law**, including those referred to in Title V of Part Three of the Treaty on the Functioning of the European Union (TFEU) and relating to the AFSJ. The consistent application of such standards to all activities entailing access to and exchange of data in the fight against crime is required to prevent that these initiatives translate into arbitrary or unjustified interferences with individuals' rights.

Of special relevance in this context are the guarantees that the European Union Charter of Fundamental Rights (EU Charter) sets forth with regard to the right to respect for private life (Article 7) and data protection (Article 8). A synthetic overview of how such standards have been interpreted by the Court of Justice of the European Union (CJEU) in a selection of landmark cases is included in Annex 2.

Figure 1. Criminal proceedings and cross-border data gathering: the available instruments



Source: Authors' own elaboration.

2.1 Intra-EU cooperation: The European Investigation Order

2.1.1 Geographic and material scope

Within the EU, the EIO allows cross-border requests for data sought in different phases of a criminal proceeding to be issued and executed based on the principle of mutual recognition of judicial decisions.

Box 1. The principle of mutual recognition in criminal matters

The principle of mutual recognition

EU judicial cooperation in criminal matters is currently governed by the principle of mutual recognition. The principle of mutual recognition implies a high degree of automaticity in the execution of judicial decisions issued by competent member state judicial authorities, and in the frame of judicial procedures in which political authorities do not participate.

Cooperation among the judicial authorities of the issuing and executing member states should take place within a limited timeframe, under strict deadlines, and on the basis of a pro forma document that is usually annexed to the relevant framework decisions or directives. The principle of mutual recognition requires the authorities of the executing country to recognise decisions from other member state with a minimum of procedure and formality, and the grounds for non-recognition must be kept to the minimum required.

EU mutual recognition instruments (e.g. the EAW and the European Investigation Order) build on some underpinning principles – mutual trust at the forefront – that apply only to EU member states. Member states are required to trust that each other's criminal justice decisions – including cross-border measures directed at obtaining electronic information for the purpose of preventing, detecting, or combating crime – adhere to the values enshrined in Article 2 of the TEU, the EU Charter, and the safeguards found in secondary pieces of EU legislation. By demanding that each EU country consider all the others to be compliant with fundamental rights, mutual trust prevents, in principle, member states from taking unilateral action that runs counter to mutual recognition or that may compromise the primacy, unity, and effectiveness of EU law.

At the same time, the free movement of judgments should not be implemented to the detriment of respect for the rule of law and fundamental rights. Mutual recognition shall not have the effect of modifying the EU member states' obligation to ensure respect of the fundamental rights and core legal protections provided under EU law. The Court of Justice of the European Union (CJEU) has repeatedly stressed that whereas the execution of a member state order is deemed to constitute a manifest breach of a rule of law regarded as essential in the legal order of the other state in which enforcement is sought, or of a right recognised as being fundamental within that legal order, the refusal to recognise or enforce an order given in another member state is justified.

The duty to verify compliance with fundamental rights and the rule of law standards relies, in the first place, upon the authorities responsible for issuing or validating a decision to enforce criminal

jurisdiction across borders. Most notably, EU law entrusts the authorities of the issuing member state with the responsibility of assessing the legality, necessity and proportionality of a cross-border measure entailing access to data sought for criminal justice-related purposes.

Existing EU law instruments for mutual recognition of judicial decisions in criminal matters also foresee the involvement of competent authorities in the EU country where a criminal justice measure is to be executed. In particular, recent CJEU case law shows that the role of judicial oversight in the executing state is central to verifying the existence of those exceptional circumstances in the presence of which the principle of mutual recognition ceases to operate. Judicial scrutiny by the executing member state authorities remains especially crucial in a context where member state criminal justice systems perform differently under important judicial independence indicators. The lack of judicial independence and 'prosecutorial bias' in issuing countries entail the risks of quasi-automatic approval of all data requests from the prosecutors and constitute a danger not only for the fundamental rights of the persons concerned, but also for the independence of the judiciary and EU rule of law as a whole.

Among participating member states (**EU27, minus Ireland and Denmark**),[13] the EIO replaces previous instruments for criminal justice cooperation regulating the exchange of evidence through mutual legal assistance. When judicial authorities in an EU member state participating in the EIO aim at having an investigative measure entailing access to and collection of electronic information executed in another EU member state participating in the EIO, the judicial cooperation channels provided by EIO should be used.

For data requests issued in the context of intra-EU judicial proceedings, **the EIO should be preferred to 'direct cooperation' with service providers abroad**, given that, to date, this latter way of working remains voluntary. As far as cross-border measures targeting data held by service providers in another EU country, it should in fact be recalled that under the national legislation of all EU member states, providers of IT and telecommunication services are not allowed to respond to direct requests for data issued by foreign investigating and prosecuting authorities.

2.1.2 For which measures can EIOs be issued and executed?

Through the EIO, a wide range of cross-border investigative measures can be issued and executed, ranging from hearing of witnesses to interception of communication. One single EIO can foresee the execution of more than just one investigative measure.

While EIO legislation does not expressly mention "electronic evidence" as such, the inclusion of a reference to data in Article 13 of the Directive indicates that **different categories of electronic information can be collected and exchanged** across borders through this judicial cooperation instrument. EIOs can also cover the "collection of traffic and location data

[13] Under the Lisbon Treaty, Ireland and Denmark can opt into (or opt out from) any post-Lisbon legislative proposal in the field of criminal justice on a case-by-case basis.

associated with telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications".[14]

Investigative measures requiring data allowing for the identification of persons holding a **subscription to a specified phone number or IP** are always available under the EIO, and cannot be refused in the country where the order is addressed based on the objection that such measures are not available in that legal system.

EIOs can be issued and executed for the investigation and/or prosecution of several criminal or administrative offences. Under the EIO a **limited double criminality check** is maintained, but only for orders related to offences **falling outside the list of the 32 offences** for which double criminality has been abolished. These are offences which are **not punishable** by a custodial sentence or a detention order **for a maximum period of at least three years** in the issuing member state.[15] Such provisions ensure that double criminality grounds might only be raised by the competent authorities of the state of execution for certain categories of less serious offences.

The executing country might decide not to recognise EIOs relating to a criminal offence allegedly committed **outside the territory of the issuing state** and wholly or partially on the territory of the executing state, and the conduct in connection with which the **EIO is issued is not an offence in the executing state**.[16] EIOs might also not be recognised when the use of the investigative measure indicated in the EIO is restricted under the law of the executing state to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO.[17]

In some EU countries, access to and gathering of electronic information is only allowed in the context of criminal investigation or prosecution of '**serious crime**'. This concept, however, assumes different meanings in specific national legal systems, and currently it still lacks a definition under EU law.[18]

2.1.3 Who can issue and execute EIOs entailing access to and collection of electronic information?

As an EU instrument of mutual recognition of judicial decisions in criminal matters, the EIO requires the **systematic involvement of competent judicial authorities in the issuing and executing** member states.

Member state **national laws identify the judicial authorities responsible** for respectively requesting, validating, and executing investigative measures targeting electronic information.

[14] Recital 11 of the EIO Directive .
[15] Art. 11(1)(g) of the EIO Directive.
[16] Art. 11(1)(e) of the EIO Directive.
[17] Art. 11(1)(h) of the EIO Directive.
[18] Carrera, S. and Stefan, M. (2020), 'Access to Electronic Data for Criminal Investigations Purposes in the EU, JUD-It Project Report', pp. 14-18, https://www.ceps.eu/ceps-publications/access-to-electronic-data-for-criminal-investigations-purposes-in-the-eu/.

To assist in clarifying the interpretation of the scope of the EIO DIR, the European Judicial Network (EJN) Secretariat has published a document, Competent authorities, languages accepted, urgent matters and scope of the EIO Directive, which is available to practitioners on the EJN website. It includes a **complete and regularly updated list of competent judicial authorities** for the purpose of the issuing and execution of EIOs.

In each member state, the judicial authority responsible for issuing, validating, or executing an EIO concerning access to or gathering of electronic data, might vary depending on factors such as the:

- **Type of offence** for which a EIO is issued and has to be executed (in several countries, the authorities responsible for requesting and validating investigative measures directed at accessing or gathering data vary depending on the seriousness of the crime investigated/prosecuted);
- **Type of data sought** (e.g. content data; metadata including traffic and location data; subscriber information; IP addresses, etc.);
- **Investigative measure envisaged** (e.g. preservation of data; production of data; search and seizures of computer devices; measure intended as coercive or non-coercive in the legal system of EIO issuing or execution, etc.);
- **Categories of persons** affected (e.g. lawyers, journalists);
- **Stage of the proceeding** in which the EIO is to be issued and executed (pre-trial phase; trial phase).

The involvement of the right **oversight authorities in the issuing state** is necessary to ensure that EIOs are not used for the performance of investigative measures/gathering of evidence that are not available at the domestic level for an equivalent case. EIOs may in fact only be issued if the substantial and procedural conditions applying to the domestic investigation or trial are met.

The involvement of the right **oversight authorities in the execution state** allows for the 'domestication' of an EIO coming from another member state with a different constitutional tradition, and ensures that every order is executed in accordance with the procedures (and underlying constitutional safeguards) prescribed under the national system of execution.

While prosecutors might be entitled for issuing and/or executing EIOs, it is important to remember that **prior independent judicial validation by a judge or court** is often required for requests for different categories of data, including data such as subscriber's information, IP addresses, etc.

EIOs can also be issued at the **request of defence lawyers** at each stage of the proceeding. Art. 1(3) of the EIO directive provides that the issuing of the EIO may be requested by the suspect or accused person (or by a lawyer on his behalf) within the framework of applicable defence rights in conformity with national criminal procedure.

2.1.4 Issuing and execution of data requests under the EIO

The EIO system requires member states to cooperate in the field of cross-border evidence gathering based on **minimum formality and speed**, while at the same time imposing **compliance with a set of legal and procedural safeguards**.

In the issuing state, the competent judicial authorities for the adoption or validation of the investigative measures included in the EIO member state are required to verify the **legality**, **necessity** and **proportionality** of a cross-border decision entailing access to or gathering of electronic information.[19] Legality, necessity and proportionality must be assessed by a competent judicial authority in light of legal standards provided under EU criminal justice and data protection law, as well as by the law of the issuing state.

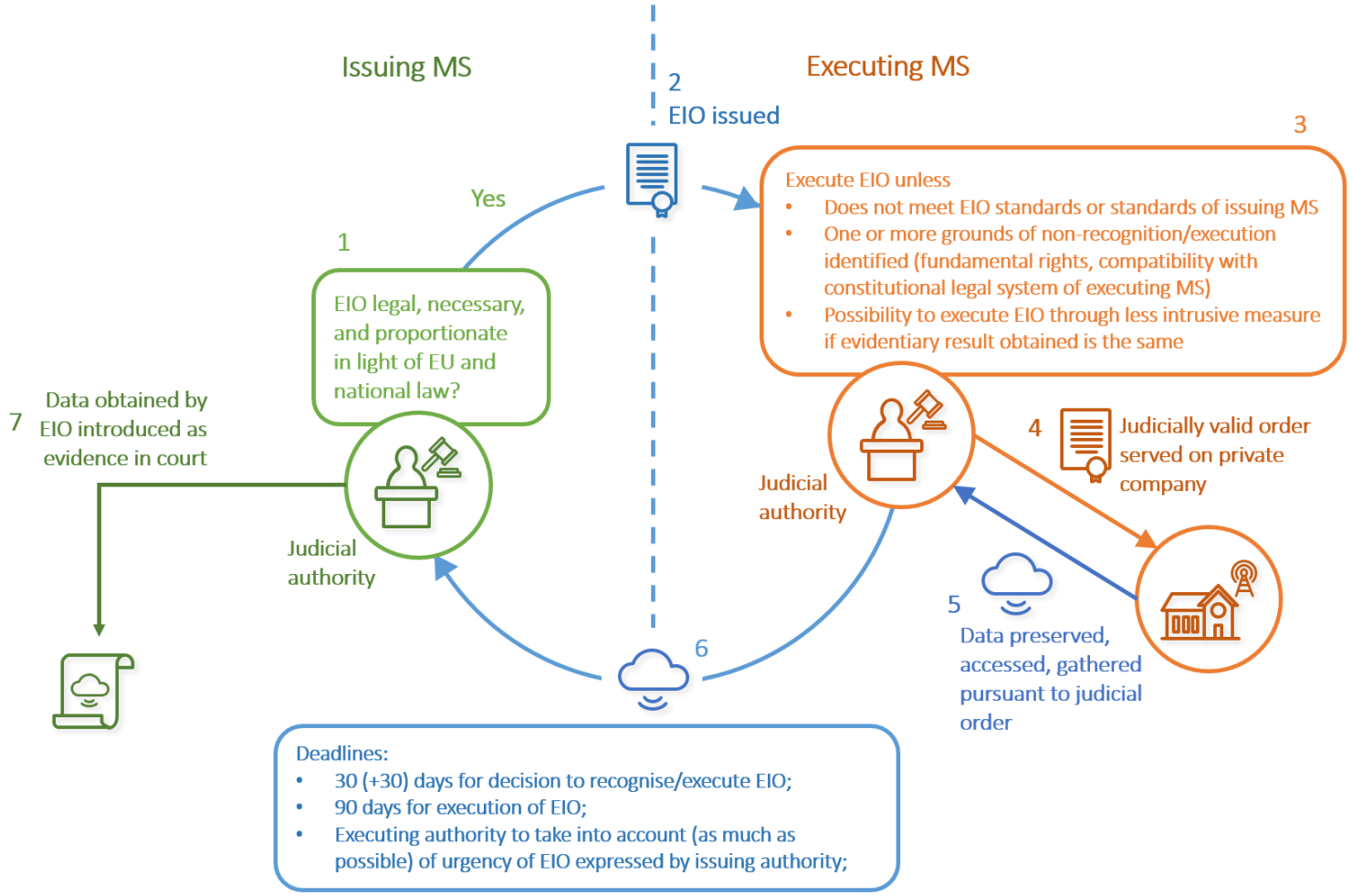
The executing authority needs to follow the formalities and procedures expressly indicated by the issuing authority, but only to the extent that these are not contrary to fundamental safeguards provided under their own legal system. Execution of an EIO is supposed to take place **in the same ways and under the same modalities (and related procedural safeguards)** as if the investigative measure concerned had been ordered by an authority of the executing state.

The competent authorities of the member state receiving an EIO have a maximum period of **30 days** to decide to recognise the request, and **90 days** to execute the request effectively. The Directive also allows for a shorter deadline when required by the *seriousness of the offence* or in other *particularly urgent circumstances*, and this should be taken into consideration to the greatest extent possible by the competent authorities of the EU country of execution when processing the order. Article 32(2) of the Directive provides for a **24-hour** deadline for provisional measures, such as the preservation of data.

Figure 2 below describes the main steps to be undertaken throughout the issuing and execution of an EIO entailing access to or gathering of electronic information.

[19] Art. 6(1)(a) of the EIO Directive.

Figure 2. Issuing and executing EIOs: main steps and control points



Source: Authors' own elaboration.

Article 11 of the EIO Directive contemplates a set of **limited non-recognition grounds**. Recognition or execution of an EIO may be refused in the executing state where, *inter alia*, the execution of the investigative measure indicated in the EIO would:

- **Breach immunities**, **privileges**, or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media;
- **Harm essential national security interests**, jeopardise sources of the information or involve the use of classified information relating to specific intelligence activities;
- **Be contrary to the principle of *ne bis in idem***;
- **Be incompatible with EU fundamental rights** (Article 6 TEU and the EU Charter);

Persons accused or suspected of crimes, third parties affected by the EIO, and addressees of the orders (including private companies) have the right **to seek remedies in the issuing member state**. The issuing state must ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measures indicated in the EIO. Remedies in the issuing state are without prejudice to the **guarantees of fundamental rights in the executing state**.

2.1.5 At which stage of the proceeding can EIOs be issued/executed?

The EIO applies to the gathering of evidence during both the **pre-trial** phase of a proceedings (e.g. the investigative phase), as well as also during the **trial phase**.

In some member states, the EIO can also apply to measures related to the **execution of a judgement** (e.g. during a financial investigation for the purpose of identifying assets after a final decision on confiscation has been adopted, or to gather evidence on the circumstances surrounding the execution of a sentence).

2.2 Mutual Legal Assistance

As far as cross-border demands for electronic information involving EU member states not part to the EIO Directive (i.e. Ireland or Denmark), or third countries (e.g. the US or Japan), EU Mutual Legal Assistance Treaties (MLATs) provide channels that can be used for requesting, gathering and exchanging data for criminal justice purposes.

With several major IT service providers established in their territories, **Ireland** and **the US** are the recipients of high volumes of data requests from EU countries' investigating and prosecuting authorities. The proper functioning of MLA cooperation depends, to a significant extent, on a good understanding of both:

- The roles played by the **different actors** involved in the MLA process, and;
- The **main legal requirements** that MLA requests issued by EU member states need to meet in order to be accepted by the competent authorities of these two receiving countries.

Addressing MLA requests through the right authorities and following standing rules can significantly enhance cooperation between EU investigating and prosecuting authorities issuing

MLA requests on the one hand, and the authorities responsible for receiving, assessing and executing the investigative measures indicated in the MLA requests.

2.2.1 MLAs requests to Ireland

When it comes to MLA cooperation with Ireland, it should be noted that considerations of whether to execute a cross-border request for electronic data sent to this EU member state are mainly undertaken by the **Ministry of Justice and Equality**.[20]

Ireland's Ministry of Justice and Equality is the main authority responsible for assessing the suitability for execution of incoming MLA request concerning evidence (also in digital form) sought for the purposes of criminal proceedings or a criminal investigation in the requesting state. The Ministry of Justice and Equality's assessment of the request is conducted based on the following requirements:

- The request concerns assistance in obtaining **specified evidential material**;
- There is **power to issue a warrant** for the search of a place in respect of an offence constituted by the conduct giving rise to the request;
- The evidence is sought for an offence **punishable both in Ireland and the requesting EU state by imprisonment for a maximum period of at least 6 months**; or the offence is a criminal offence in Ireland and an administrative offence in the requesting member state that could give rise to proceedings before a court having, in particular, jurisdiction in criminal matters;
- The **requested evidence will not be used for any purpose** other than for which it was requested;

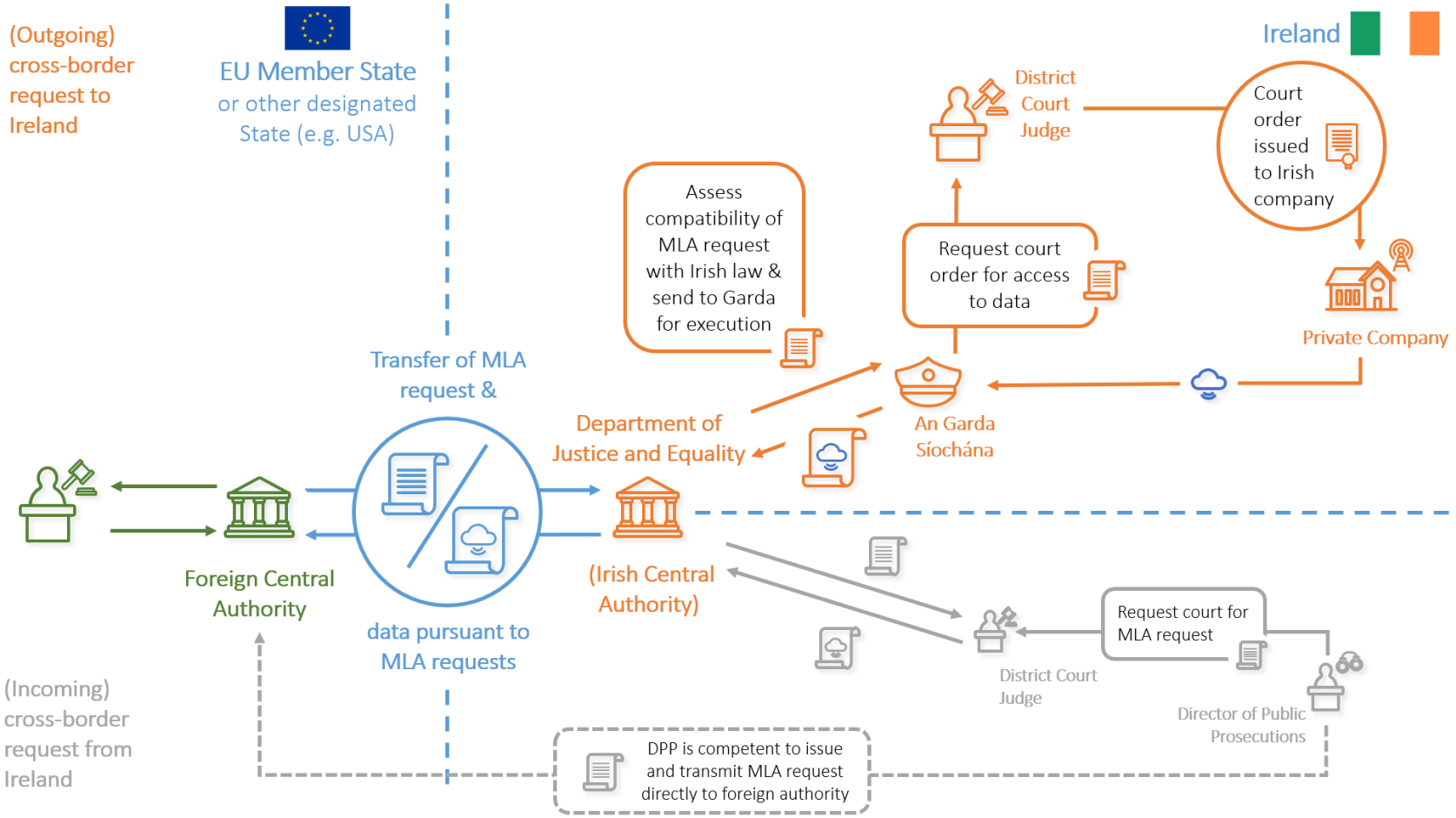
The MLA request will be refused if, *inter alia*, the Minister considers that providing assistance would be likely to prejudice the sovereignty, security or other essential interests of Ireland or be contrary to *ordre public*, or if there are reasonable grounds to believe that the request is of a discriminatory nature, providing assistance would lead to violation of a person's rights under the ECHR (including prohibition of torture), or (and for as long as) providing assistance would prejudice a criminal investigation or criminal proceedings in Ireland.

If Ireland's Ministry of Justice and Equality considers that a request for mutual legal assistance/cross-border request for access to electronic data meets the above mentioned conditions, it shall direct the Ireland's Commissioner of the Garda Síochána to obtain such evidence for transmission.

Figure 3 below provides a visual guide to the main steps involved in the execution of MLA requests directed to and coming from Ireland.

[20] The Department (of Justice and Equality) determines internally which procedure to use in order to respond to an MLA request, with section 75 of the *Criminal Justice (Mutual Assistance) Act 2008* Act being the 'standard procedure'.

Figure 3. MLA cooperation with Ireland



Source: Authors' own elaboration.

Representatives of the Ministry of Justice and Equality heard during the JUD-IT Project noted that, according to their experience, service providers "generally cooperate with requests made under MLA procedures". Replies obtained through the JUD-IT questionnaire indicate that **channelling requests for data through MLA** processes, **domestication via local court orders** and/or **access via Irish law enforcement authorities** are the conditions under which investigating or prosecuting authorities from other jurisdictions can lawfully request and obtain access to electronic information from service providers under Irish law.

Box 2. MLA vs direct access: the 'Microsoft Ireland' case

The 'Microsoft Ireland' case

The jurisdictional, legal and practical challenges that come from direct (i.e. non-judicially mediated) requests for access to electronic information held by service providers in Ireland were made manifest in the long-running dispute underlying the case of *Microsoft Ireland v Department of Justice*.[21]

The case originated in Microsoft's refusal to execute a warrant received directly by US authorities, which requested Microsoft Ireland to disclose some data stored in the EU. This type of extraterritorial exercise of criminal jurisdiction is a longstanding practice of US LEAs, and the US Department of Justice argued that its warrant authority under the Stored Communication Act compelled US-based companies to turn over the requested data, regardless of where the latter were stored. Microsoft, by contrast, maintained that this authority did not extend to data located outside United States territory.[22] The company consequently challenged the US warrant's power to reach overseas data.[23]

The case, which had been pending appeal before the US Supreme Court, was ultimately dismissed. Meanwhile, policy and legislative efforts have been directed at the creation of new data-gathering tools for crime fighting across the Atlantic, but also within the EU. In the US, the signature of the Clarifying Lawful Use of Overseas Data (CLOUD) Act constituted a significant step in that direction.

After the authority of US federal courts to issue warrants for the search and seizure of data located outside the territory of the United States was challenged in the 'Microsoft Ireland' case, the US government introduced the CLOUD Act,[24] which the US legislator adopted with the intention to clarify that the SCA's scope of application extends to data stored abroad.

[21] Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp. 3. 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

[22] Stored Communications Act (SCA), codified at 18 U.S.C. Chapter 121 §§ 2701–2712. Under the SCA, US law enforcement actors are authorised to compel US providers to disclose information about a person, regardless of both the nationality of the data subject and the localisation of the data.

[23] A detailed account of the arguments defended by the parties and of the main legal and jurisdictional issues underlying the dispute if provided in Carrera, S. and others (2015), op. cit.

[24] Clarifying Lawful Overseas Use of Data (CLOUD Act), S. 2383, H.R. 4943.

Part I of Act 32 now formally grants US authorities the power, under US law, to order private companies to disclose the "content of a wire or electronic communication and any record of other information" about a person, regardless of either the nationality of the latter or the location of the data. Providers can also be ordered to preserve data in their possession for up to 180 days prior to the issuance of any compulsory process.

From an EU law perspective, a number of questions arise with regard to the CLOUD Act's fitness to provide a sound legal basis for the gathering and transfer of data in the context of cross-border criminal proceedings.[25]

The execution of EU member state authorities' **requests for data addressed directly to service providers in Ireland** are, instead, dependent on the assessment conducted on a case-by-case basis by the private company recipient of the request. JUD-IT research has showed that US cloud service providers with branches in Ireland usually respond to requests for data in the following ways:

- **Requests for content data** held by the company are automatically redirected by the company to its USA branch;
- **Requests for non-content data** might be executed upon Company's own assessment. In the performance of such assessment, some company follows a "3-pronged approach":
    - ✓ User is under the jurisdiction of issuing authority;
    - ✓ The request is based on the issuing authorities' own legal process;
    - ✓ Respect of international human rights standards.

Formal MLA instruments constitute therefore the only formal and therefore reliable tools of judicial cooperation available when it comes to the transmission, reception, validation and execution of requests for data originating from foreign (i.e. non-Irish) investigating and prosecuting authorities.

2.2.2 MLA requests to the US

Mutual Legal Assistance Treaties (MLATs) are the traditional channel of cooperation for cross-border gathering and exchange of electronic information between the EU and the US. The **EU-US MLA Agreement** complements existing bilateral treaties and amends some of their provisions, if they provide for "less effective avenues" of cooperation between EU member states and the US.[26]

Exchange of evidence under MLATs with the US relies on the **involvement of different authorities**, including the **political bodies and judicial actors** responsible for supervising and examining cross-border requests for evidence gathering against domestic standards.

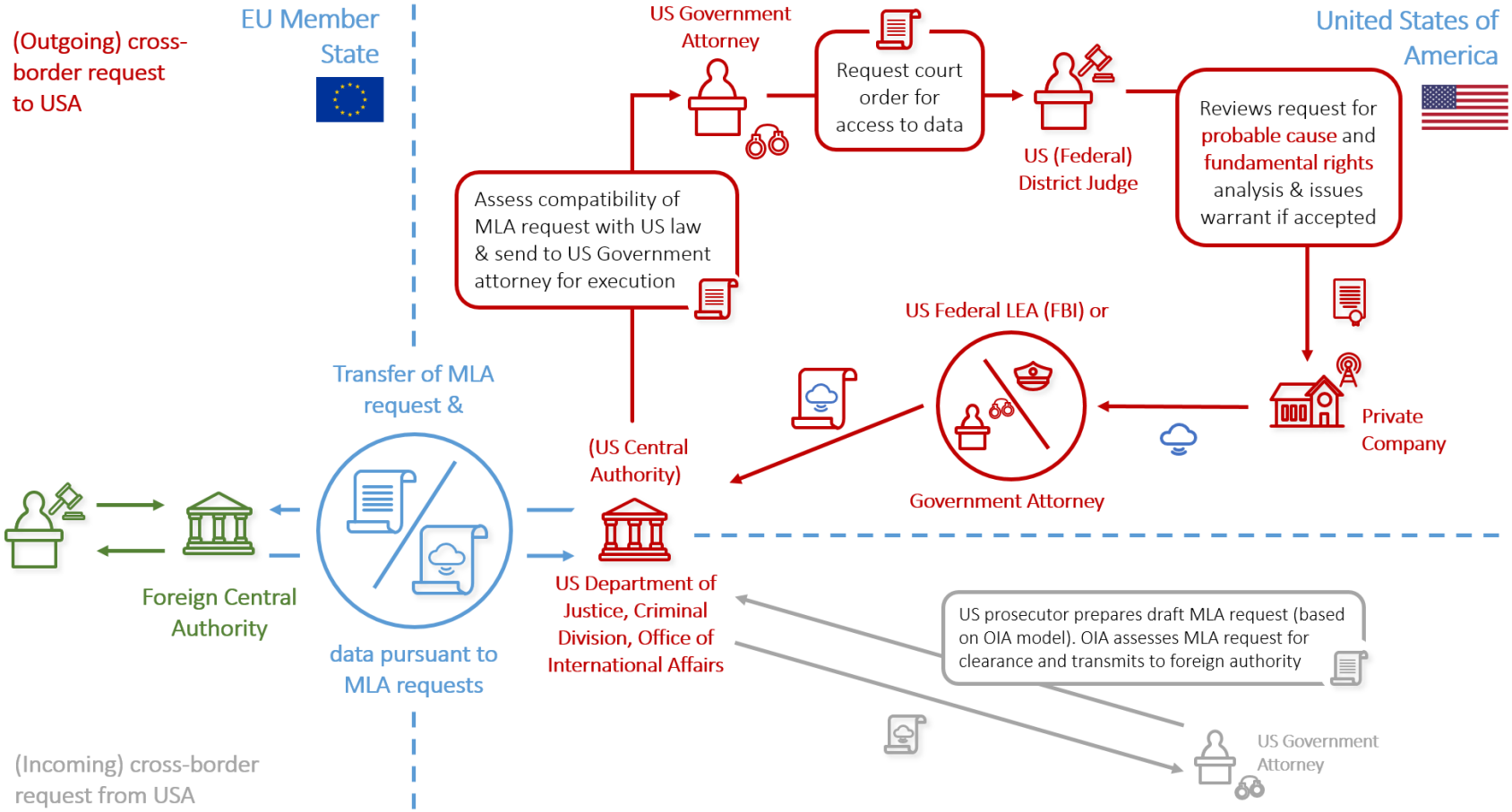
[25] Carrera and Stefan (2020), op. cit., and Stefan and González Fuster (2019), op. cit.
[26] See Article 3(2)(a) of the EU–US MLA Agreement.

MLA requests originating from a EU member state and directed to the US are first reviewed by the central authority of the requesting state. Once ready, the MLA request is sent to the **US Office of International Affairs of the Department of Justice** (OIA). The OIA analyses the request against US constitutional requirements and sends it to the US Attorney's Office established where the company holding the data is located. The **US Attorney**'s Office defends the request in front of a judge (and in presence of the **US Federal Bureau of Investigation – FBI**). If the **US judge grants the warrant**, the request is then sent to the private company.

When the company produces the data, the FBI first conducts a screening to verify that the they do not exceed the request, and then sends it on a CD-ROM to the OIA, which finally forwards it to the central authority (Ministry of Justice) of the requesting state, from where the data arrives to the judge/LEA who initiated the request. Some member states appointed **liaison magistrates** that are based in Washington and are responsible to review the MLATs issued by their country's authority before they are submitted to the central authority of the executing country.

Figure 4 below provides a visual guide to the main steps involved in the execution of MLA requests directed to and coming from the US.

Figure 4. MLA cooperation with the US



Source: Authors' own elaboration.

The **content of electronic communications** held by companies in the US might only be obtained by EU investigating authorities when a US federal judge has been satisfied of the existence of 'probable cause'. The US Stored Communications Act (SCA), which is contained in Title II of the Electronic Communication Privacy Act (ECPA), acts in fact as a blocking statute that limits the possibility for foreign governments to directly request content data held by IT companies in the US, by subjecting their possibility to access electronic information to the requirement of independent judicial validation in the US. This means that, even when an order meets the probable cause standard, service providers in the US are not currently allowed to respond to direct orders (or: 'requests') for content data from EU authorities. EU member state judges often do not take into due account US legal standards, and most notably the 'probable cause' one.

Box 3. US law and the probable cause

The 'probable clause' standard

EU law enforcement requests for access to data stored in the US are assessed against the probable cause standard under the Fourth Amendment. The Fourth Amendment limits the government's ability to conduct searches and seizures, and warrants can be issued only after independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to communications, covering a person's "papers and effects". Probable cause that a crime has been committed must be established by the law enforcement officer on the basis of "reasonably trustworthy information" that is sufficient to cause a reasonably prudent person to believe that an offence has been or is being committed or that evidence will be found in the place that is to be searched. Thus, in order to obtain the warrant necessary to access data in the US through the MLA procedure, EU authorities must prove that an offence has been or is being committed or that evidence will be found in the place that is to be searched.

For certain categories of information, the ECPA would require less than probable cause. For instance, the statute specifies that data or electronic communications that have been in storage for more than 180 days can be produced upon the issue of a subpoena or a court order, which occurs when a judge is persuaded of the existence of 'specific and articulable facts' enabling the assumption that the requested data are relevant to an ongoing criminal investigation. Still, federal appellate courts have progressively extended application of the probable cause requirement to these requests. In the *United States v Warshak* case (2010), the Sixth Circuit broadened the interpretation of the Fourth Amendment's guarantees expanding the probable cause standard to include communication that has been in storage for more than 180 days. In *Riley v California* (2014), the Supreme Court stated that "the police generally may not, without a warrant, search digital information on a mobile phone seized from an individual who has been arrested". In the *Carpenter v United States* case (2018), the Supreme Court ruled that in order to

obtain mobile phone tracking information (metadata/non-content), law enforcement authorities needed a warrant.[27]

Companies falling under US jurisdiction can instead provide **non-content data to foreign authorities on a voluntary basis**. JUD-IT research has found no evidence that direct or unmediated requests for content data directly addressed to US service providers (i.e. without going through MLATs channels) are more successful then MLA requests for the same type of data.[28]

In relation to '**emergency requests**', US law allows US service providers to respond to these requests following the policies and standards set out by the service providers themselves and irrespective of the 'probable cause' standards being present. The usual process is that EU member state law enforcement authorities liaise with the US authorities who, in turn, facilitate the voluntary provision by service providers of the required material pursuant to US law. According to the Commission, this arrangement can work very well and, in the most exceptionally serious and urgent cases, the US has assisted in the obtaining of evidence in under 24 hours.[29]

At the same time, there is currently no streamlined procedure to follow in the issuing and execution of an emergency request. Some US companies developed internal guidelines to deal with these type of demands originating from non-US, including EU member state, authorities.

Box 4. Case Study: Apple's guidelines on emergency procedure

Emergency procedure for access to data held by US companies: "the Apple example"

Apple considers as an emergency request those that relate to circumstances involving imminent and serious threats to:

1) the life/safety of individual(s);

2) the security of a state;

3) the security of critical infrastructure/installation(s).

If the requesting government or law enforcement officer provides satisfactory confirmation that their request relates to emergency circumstance(s) involving one or more of the above criteria, Apple will examine such a request on an emergency basis. In order to make an emergency request to Apple, the requesting government or law enforcement officer should complete the Emergency Government & Law Enforcement Information Request form and

[27] See Department of Justice, Principles of Federal Prosecution, https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution#9-27.200.

[28] González Fuster, G. and Vázquez Maymir, S. (2020), 'Cross-border Access to E-Evidence: Framing the Evidence', JUD-It Policy Brief. Available at: https://www.ceps.eu/ceps-publications/cross-border-access-to-e-evidence/.

[29] European Commission (2018), "Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings", SWD/2018/118 final – 2018/0108 (COD), 17 April, p. 84-85.

transmit it directly from their official government or law enforcement email address to the mailbox: exigent@apple.com with the words "Emergency Request" in the subject line.

In the event that Apple produces customer data in response to an Emergency Government & Law Enforcement Information Request, a named supervisor for the government or law enforcement agent who submitted the Emergency Government & Law Enforcement Information Request may be contacted and asked to confirm to Apple that the emergency request was legitimate. The government or law enforcement agent who submits the Emergency Government & Law Enforcement Information Request should provide the supervisor's contact information in the request.[30]

[30] See https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf.

3. Using the EIO for the purpose of accessing and exchanging data sought in criminal proceedings - Checklist for practitioners

3.1 Checklists for judicial practitioners

A first thing to check is the exact instrument to be used in order to channel and execute cross-border requests for data. In cases where requests fall within the scope of application of EU law, and the EU has exercised competence through the adoption of secondary legislation (EIO) or international agreements (MLTAs), EU instruments (and corresponding standards) should be given preference.

Among participating member states, **the EIO replaces previous instruments for criminal justice cooperation**. The EIO should be used when judicial authorities in an EU member state participating in the EIO aim at having an investigative measure entailing access to and collection of electronic information executed in another EU member state participating in the EIO.

For data requests issued in the context of intra-EU judicial proceedings, the EIO should be preferred to 'direct cooperation' with service providers abroad, given that this latter way of working remains voluntary to date. As far as cross-border measures targeting data held by service providers in another EU country, it should in fact be recalled that under the national legislation of all EU member states, providers of IT and telecommunication services are not allowed to respond to direct requests for data issued by foreign investigating and prosecuting authorities.

3.1.1 Practical use and relations with other instruments

The EIO can only be used in cases in which the requests for electronic data have **evidence-related implications**. These cases exclude requests for data presenting a mere procedural objective (e.g. service and sending of procedural documents). In these cases, a MLA request, and not an EIO, should be issued.

The EIO and the MLA request work in parallel. EIO use does not have to be restricted to measures covered by the Directive, but should nevertheless be **avoided where it causes too much administrative burden** (e.g. translation, etc.) on the competent authorities in the issuing and executing state. Notifications, for instance, are out of the scope of the EIO and must be not asked for through it: they have to be asked for instead through the usual channel of the MLA requests.

3.1.2 Involving the competent judicial authority in the issuing state

The EIO Directive has 'judicialised' the issuing phase by requiring that EIOs be issued by a **judge,** a **court**, an **investigating judge** or a **public prosecutor** competent in the case concerned (judicial authority as issuing authority). The judicialisation requirement can be also satisfied by ensuring that an EIO is validated by one of these authorities (judicial authority as validating authority).[31]

[31] See Article 2(c) EIO Directive.

When in accordance with national law of the issuing country the gathering of evidence is ordered by an authority different from a court, judge or prosecutor, **the EIO shall be validated** by one of these judicial authorities, which remain responsible for examining the Order's conformity with the conditions for issuing an EIO.[32]

The involvement of competent judicial authorities in the issuing state is important as **non-judicial authorities identified by some member states** as 'competent for issuing EIOs' are not always recognised as such by all EU countries. For instance, Italy's criminal procedural law does not allow UK barristers' associations to be considered as judicial authorities. In practice, an EIO written by a UK barristers' association might be considered a valid measure (and consequently executed) by Italian authorities, provided that it is validated by a UK court. The European Judicial Network (EJN)'s dedicated page on the EIO includes a useful link to identify 'competent authorities' for the purpose of issuing and executing EIOs.

Judicial **validation of data-gathering** measures adopted by non-judicial issuing actors (e.g. police) can be crucial for the sake of EIO recognition/execution. In the absence of a judicial validation, EIOs might not be recognised or executed pursuant to the rule according to which an EIO cannot be executed in line with the procedures/modalities indicated by the issuing member state when they run counter the fundamental principle of the country of execution.

Issuing authorities should **not use the EIO to bypass judicial checks** by authorities different from the one issuing the request or investigating the case, when their involvement is foreseen in equivalent domestic procedures. If a validation of a data-gathering measure by a judicial authority (different from the one investigating or prosecuting the case) is required by the law of the issuing state for a domestic measure equivalent to the one included in the EIO, the issuing authority shall seek it and obtain it, and not presume that this requirement will be fulfilled in the country of execution.

Judicial scrutiny over police requests for data shall be effective, and not limited to a form of automatic/default validation.

3.1.3 Formulating 'quality requests'

Including the right information in the EIO Form (Annex A) is particularly important to ensure smooth cooperation. Issuing authorities should make sure to specify:

- What are the facts under investigation and the measure of technological investigation required (production or preservation of data);
- Who is the suspect or accused person and other individuals potentially affected;
- Why the data requested is needed for the investigation/prosecution of the crime that is the object of the proceeding, and what is expected to be found through the execution of the measures;

[32] Art. 2 (c) (ii) of the EIO Directive.

- What is the time limit within which the data should preserved/produced.

The **issuing authority** should **make clear if the data-gathering measure contained in the EIO is established in the trial or pre-trial phase,** because, depending on these circumstances, the executing authority could be different. Specifying whether an EIO has been issued in the pre-trial or trial phase is also particularly important for determining if the conditions justifying the secrecy of an investigative measure subsist.

During the pre-trial phase, **secrecy** might be justified, and its maintenance might be necessary until investigations are completed. In the trial phase **notification** is instead particularly important to ensure the rights and prerogatives not only of the suspected or accused person, but also of third parties. In the EIO Directive, it is not clearly mentioned whether in the **pre-trial phase** the suspected person or his/her lawyer can have a copy of the EIO and, in the affirmative, which part of it. Should there be no reason to justify secrecy of the measure requested through the EIO, the defence shall be put in the position to know that the data of a suspect are implicated in an EIO procedure. The inclusion of the judicial decision/decree accompanying the EIO is useful to execute the requested measures properly, having regard to guaranteeing fundamental rights.

To facilitate cooperation, it is important that **translations are of good quality** so as to make requests more understandable and clear. Where available, issuing authorities should make use of certified interpreters**. Translation costs** are borne by the issuing state.

Clear information shall also be included to motivate **the necessity to maintain the secrecy of an EIO** entailing access to and preservation of electronic information. Restrictions of an individuals' rights to be informed should be limited to situations where secrecy is strictly necessary and proportionate to protect sensitive law enforcement information or to avoid jeopardising ongoing investigations.

Exemptions to **the right to be informed** (which is crucial for the exercise of other criminal justice and data protection rights, including the right to fair trials, fair processing of the data, and effective remedies before a tribunal) should be not be formulated in a way that unduly prevents the exercise of these rights in practice, even if limited or performed by a trusted third party.

The EIO should include provisions on the protection of the defendant's fundamental rights, and an **indication of what remedies are available** in the issuing state. It should indicate which is the competent authority to receive appeals against the order. JUD-IT research has shown that, in practice, it is not easy for the defence to clearly establish if it is the issuing or the executing state.

3.1.4 Assessing legality, necessity and proportionality

The judicial authorities **in the issuing member state** are those responsible for verifying the **legality, necessity, and proportionality** of a cross-border decision.[33] Such assessments must be conducted by the competent judicial authorities of the issuing country against their own domestic legal standards, as well as in light of relevant EU primary and secondary law.

The issuing of **EIOs for minor offences** should be carefully evaluated to establish whether the cross-border data gathering measure is proportional for obtaining the information/evidence needed, also in consideration of the fact that an EIO might be refused based on the absence of double criminality (for offences falling outside the list of crimes for which double criminality is abolished, and which are not punished with custodial sentences of 3 years minimum).

The competent judicial authorities **in the executing country** also have a role in the assessment of necessity and proportionality. When "the executing authority has reason to believe that the conditions referred to in paragraph 1 [the issuing of the EIO is necessary and proportionate] have not been met, it may consult the issuing authority on the importance of executing the EIO. After that consultation the issuing authority may decide to withdraw the EIO". The executing country may **refuse the recognition/execution** of an EIO via written motivation (Decree of Non-Acceptance).

Cases involving costs that are "deemed to be exceptionally high" in relation to the investigative goal pursued can be resolved through a dedicated consultation mechanism.[34]

3.1.5 Transnational coordination and direct judicial contacts

EIOs can be **transmitted directly from the issuing authority to the executing authority** (without prejudice to the designation of central authorities).[35] For the identification of the competent executing authority and the relevant contact details, the EJN Atlas can be consulted. If **an EIO is sent to the incorrect authority** in the executing state, instead of being returned, it should be forwarded to the correct executing authority.[36]

Direct contact and **communication between the requesting** and **executing judicial authority** is crucial. Regardless of who is the receiving/executing authority, coordination between authorities in the issuing and executing state is to be ensured. Communication is particularly important in instances where, according to national laws of the country of execution, the authority receiving an EIO cannot execute the measure.

Depending on the nature, complexity and urgency of the case, different channels are used to speed up the transmission of EIOs and ensure authenticity. These include Eurojust, the EJN contact points and liaison magistrates. The **positive role and contributions ensured by the**

[33] See Article 6 EIO Directive.
[34] See Article 21(2) EIO Directive
[35] See Article 7 EIO Directive.
[36] See Article 7(6) EIO Directive.

European Judicial Network (EJN) and Eurojust have been highlighted as clear examples of facilitating efficient cooperation by providing contact points and information and communication platforms, liaising between relevant authorities, and providing training activities and materials.

EIOs can be submitted via the **Eurojust secure connection** (for those member states that are connected). In such cases, however, communication is only possible between a national authority and Eurojust (and not between national authorities) and the **EJN secure telecommunication connection**.[37] The secure connection is not, however, suitable for direct contact between the competent authorities.

3.1.6 The execution of cross-border data requests under the EIO Directive

For the EIO to be executed, a judicial decision in both the issuing *and* the executing state is necessary.

The **judicial authority in the executing state** shall recognise an EIO "without any further formality required" and ensure its execution. The decision on the recognition or execution of the EIO shall be taken and the execution of the measure shall be carried out "with the same celerity and priority as for a national case". The following mandatory deadlines shall be observed:

- 30 days + 30 days for taking the decision on recognition or execution;
- 90 days for undertaking the measure (after the decision on recognition or execution);
- 24 hours from receipt of the EIO measures, if possible, in case of emergency.[38]

When the validation of an EIO is required, some member states are willing, in urgent cases, to take some initial measures to secure evidence before the validated EIO has even been received. In those cases, an email is required, with a brief written summary of the facts. Furthermore, some member states will accept an email confirmation from the competent validating authority when the validating authority is not available to sign the EIO.[39]

Non-recognition grounds are listed exhaustively in the EIO Directive While the **EIO Directive does not allow for an extensive study of the file in the executing state**, some checks must still be made.[40]

While judicial decisions are presumed to comply with certain fundamental rights and rule of law standards, they must be reviewable.

The executing authority must comply with the formalities and procedures expressly indicated by the issuing authority, but only to the extent that these are not contrary to the fundamental principles of law of the executing state. Execution of another EU country's EIO is in fact

[37] See Article 9 of the EJN Decision, and Article 7(4) EIO Directive.
[38] See Article 32 of the EIO Directive.
[39] See EUROJUST/EJN, Joint Note on the Practical Application of the EIO.
[40] See Article 10(3) and Article 11 EIO Directive.

supposed to take place in the same ways and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing state.

The executing authorities are supposed to perform a **fundamental rights assessment** to establish whether the execution of an EIO would unduly undermine fundamental rights protected under EU law. Competent authorities in the executing states are also responsible for **ensuring that EIOs are not used for trivial offences**, and can go back to the issuing authority to check: "Are you sure about this"?

As a general rule the EIO requires the execution of a **non-coercive measure**. The executing authority shall not analyse if a non-coercive measure should be substituted by a less intrusive measure. As a general rule, the EIO establishes that recognition or execution orders requiring data allowing for the identification of persons holding a subscription of a specified phone number or IP address cannot be refused based on the objection that such measures are not available in the state of execution. Such a measure should exist in all member states. However, this does not mean that it shall be recognised automatically, nor that the general grounds for refusal do not apply.

Cost-related considerations cannot be used as grounds for non-recognition.

3.1.7 Urgent cases

Some member states accept EIOs issued in English (instead of their own national language), for urgent cases. A complete list of member states that allow the exceptional derogation of translation requirements in urgent cases is available at the following link (under the "urgent matters" heading).

Requests for data channelled through EIOs should not be labelled as "urgent" simply because authorities in the issuing member state would like to accelerate the case. Urgent requests for the execution of an EIO should be motivated by the issuing authority through the inclusion of information capable of proving **the seriousness of the offence** or the existence of other **particularly urgent circumstances.**

Precise information that can help in proving or substantiating 'urgency' include:

- Information related to the **risk of data loss**, and
- Existence of a clear and **imminent threat** against specific people.

Such information should be given thorough consideration and taken as much as possible into account by the competent authorities of the EU country of execution when processing the order. If an urgent request for data is made through an EIO, and the latter foresees the execution of several measures, coordination with other requests and measures is necessary.

As far as 'emergency requests' directed toward the US are concerned, the usual process applies: EU member state law enforcement authorities liaise with the US authorities who, in turn, facilitate the voluntary provision by service providers of the required material pursuant to US law.

3.2 Role and checklist for defence lawyers

While cross-border judicial cooperation mechanisms have been traditionally designed to increase the capacity of law enforcement authorities to obtain evidence to prosecute alleged crimes, the **EIO directive is the only instrument that expressly takes the interests of the defence into account**. This section, which builds on the results of the JUD-IT Practitioners workshop organised by Fair Trials in the context of the JUD-IT Project,[41] focuses on the role of defence lawyers in MLA and EIO procedures.

Lawyers can play an active role in respect of both (i) the request to issue an MLA or EIO request; (ii) challenges to the issuing of an MLA request or an EIO; and (iii) challenges to the execution of an MLA or EIO. Moreover, lawyers can seek to challenge the reliance on the electronic data obtained pursuant to an MLA request or an EIO as evidence against the accused person (see (iv) below).

3.2.1 Request the issuing of an MLA request or an EIO

When lawyers become aware that an investigation is ongoing in respect of their client, they should **consider whether it is necessary to ensure that exculpatory electronic evidence** is obtained, which the client cannot secure by him or herself. In practice, given the volatile nature of electronic data, by the time the defence finally obtains disclosure of the case file, exculpatory electronic data may already have been deleted.

The EIO enables lawyers to seek access to the electronic data before it is deleted. This can be a key part of the defence strategy. A suspected or accused person, or by a lawyer acting on his behalf, may request the issuing of an EIO within the framework of applicable defence rights in conformity with national criminal procedure.[42] The **EIO directive does not specify the process and instead leaves it up to the national criminal procedure of the issuing state**. In the absence of a specified procedure in national law, lawyers can rely directly on the EIO directive to apply for an EIO in the competent court of the issuing state.

The traditional MLA system does not recognise the possibility for defence practitioners to request cross-border electronic data. Instead, national law will determine to what extent the defence may apply to the authorities to request international cooperation. However, informally, **the defence can ask the competent national authorities to send a letter of request to have investigations carried out in another state** even where they do not have a legal right to this. The defence will need to demonstrate in detail how the data requested is relevant to the case, that it is necessary and proportionate in order to conduct the defence, as well as specify what data needs to be obtained, where the data is stored and who holds it.

[41] Fair Trials Europe (2019), 'Policy Brief: The impact on the procedural rights of defendants of cross-border access to data through judicial cooperation in criminal matters', Available at https://fairtrials.org/sites/default/files/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf.

[42] Article 1(3) of the EIO Directive.

3.2.2 Challenging the issuing of an MLA or EIO request

Defence lawyers can also challenge the lawfulness of an MLA request or EIO when it is issued, where they are aware of such a request by law enforcement authorities. In particular, **the EIO requires law enforcement authorities to seek judicial authorisation**, and for the competent judicial authority to conduct a proportionality and necessity assessment against the fundamental rights of the defendant before issuing an EIO. Provided the defence is notified that law enforcement authorities are seeking to make a cross-border request for data, lawyers can take this **opportunity to challenge the proportionality and necessity** of an EIO.

Even if law enforcement authorities have the legal power to gather electronic data, because of the impact this has on the right to private and family life, Article 8 ECHR requires that these powers should only be used when it is proportionate to do so. One practical aspect of the principle of proportionality is the requirement that there is a sound basis to justify the request for electronic data. A vague and unsubstantiated suspicion that a person may have committed a criminal offence should not be enough.

3.2.3 Challenging the execution of an MLA or EIO request

In traditional judicial cooperation mechanisms, the involvement of a judicial authority in the state that is asked to gather the evidence may provide an additional check on the legality of the evidence gathering, and an **opportunity for lawyers to submit evidence that the request should not be executed**.

The EIO is the first instrument to include a risk to fundamental rights as legitimate grounds to refuse the execution of an EIO. Therefore, an EIO may be refused in the executing state where "there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter".[43] In this respect, please refer to Annex II for some guidance on risks to fundamental rights that arise in the context of electronic data.

3.2.4 Challenging the probity or admissibility of the data obtained under the MLA or EIO procedure as evidence at trial

Once cross-border data has been obtained by the issuing state, the prosecution may seek to rely upon it as evidence against an accused person. Defence lawyers may have an **opportunity to challenge the probity or admissibility of the evidence on which the prosecution is seeking to rely**, for instance, on the grounds that the data contains legally privileged information.

Lawyer may face difficulties in this respect. For instance, it may be difficult to obtain information on how that evidence was gathered and to understand whether this was done in violation of local law or in a way which undermines its reliability. **Lawyers can actively seek disclosure of the electronic data and how it was obtained**. In this respect, the EU Directive on the right to information in criminal proceedings[44] enshrines the right to access all material

[43] Articles 1(4), 6(1) (a), and 11 (1) (d) and (f) of the EIO Directive.
[44] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.

evidence in possession of the competent authorities in due time to allow the exercise of the rights of the defence (Article 7).

Reviewing electronic data is a time-consuming and onerous task, especially when the defence has limited resources and a client is in detention and cannot assist with the review of the data, creating a risk that potentially relevant data is overlooked. These challenges can be exacerbated by the quantity of electronic data defence lawyers are given. In this respect, it may be possible to apply for legal aid and/or for lawyers to obtain specialist technical support or training.

Annex I – Glossary

The definitions of the categories of public authorities and data provided in the glossary below are intended solely for the purposes of this Handbook. They do not coincide with definitions of more general concepts developed in EU law, e.g. independent judicial authority, or issuing judicial authority in EU Criminal Justice Law.

Public authorities	
Judges	Judicial authorities who are independent from the executive branch and who exercise judicial oversight functions in the pre-trial phase, as well as independent judicial actors responsible for admitting and/or evaluating evidence in the trial phase. This definition does not encompass administrative authorities such as ministries or police authorities, which are "within the province of the executive".
Prosecutors	Judicial or administrative authorities with the competence to order the gathering of information as part of a criminal investigation, and who are responsible for coordinating criminal investigations and/or representing the prosecution in a criminal trial.
Law enforcement authorities (LEAs)	Governmental police authorities involved in criminal investigations; depending on the specific national framework of reference, this category might also include specialised law enforcement agencies (customs, anti-fraud, etc.). LEAs do not include intelligence or security services. In some member states, where prosecutors do not qualify as an independent judicial authority and may even be considered part of the executive, LEAs could also include prosecutors.
Central authorities	Representatives of the executive branch dealing with the issuing of cross-border requests and/or responsible for the processing (e.g. transmission or translation) of incoming foreign requests for access to data for criminal proceedings. This category includes liaison magistrates/prosecutors who are seconded abroad (e.g. to the foreign ministry by the justice ministry) and responsible for facilitating and advising on matters concerning mutual legal assistance in relation to the investigation and prosecution of transnational and cross-border crime.

Electronic information		
Content data	The content exchanged by means of electronic communications services, such as text, voice, images and sound.[45] While content data include both stored and intercept (i.e. data from real-time interception of telecommunications) electronic communications content, the Commission has stressed that intercept data are out of the scope of the proposal. However, discussions within the Council suggest that the scope of the proposed regulation could be expanded to also cover this type of data (live interception).[46]	
Non-content data	Metadata	Data processed in an electronic communications network for the purpose of transmitting, distributing or exchanging electronic communications content. Metadata encompasses data used to trace and identify the source and destination of a communication; data on the location of the device generated in the context of providing electronic communications services; and the date, time, duration and type of communication.[47] Metadata also includes, for instance, data relative to the connection, traffic or location of the communication.[48]
	Subscriber data	Information that allows the identification of a subscriber to a service. Examples are the subscriber's name, address and telephone number.[49]
	Access logs	Information that records the time and date an individual accessed a service, and the IP address from which the service was accessed.[50]
	Transaction logs	Information that identifies products or services an individual has obtained from a provider or a third party (e.g. a purchase of cloud storage space).[51]

[45] Article 4(3)(b) of the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (European Commission, 2017c).

[46] See Council of the European Union (2018b), p. 3.

[47] Ibid., Article 4(3)(c).

[48] See European Commission (2018a), p. 43.

[49] Ibid.

[50] Ibid.

[51] Ibid.

Annex II - EU data protection and criminal justice standards (Selected CJEU jurisprudence)

Key standards stemming from the Court rulings for checking legality on *Data Retention and Third Country Transfer of Data*	
Retention of telecommunication data (*Tele2*)	The member states may not impose a general obligation to retain data on providers of electronic communications services. • EU law precludes a general and indiscriminate retention of traffic data and location data, but it is open to member states to make provision, as a preventive measure, for targeted retention of that data solely for the purpose of fighting serious crime, provided that such retention is, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention, limited to what is strictly necessary. Access by national authorities to the retained data must be subject to conditions, including prior review by an independent authority and the data being retained within the EU. • The Court noted that the national legislation "provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions".[52] • The Court considers it important that national law safeguards professional secrecy[53] and criticised the fact that national law was "not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[54]
Retention of PNR data (*Opinion 1/15*)	• The CJEU differentiates between different stages of retention and use of PNR data: (i) retention and use before arrival; (ii) retention and use during passengers' stay; (iii) retention and use after a passengers' departure.

[52] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 97.
[53] Ibid., para. 104-105.
[54] Ibid., para. 106.

	• Retention and use before arrival: viewing the PNR system as one that "facilitates security checks and border control checks", the Court found that the retention of data up to the departure from Canada is proportionate in relation to all air passengers; • Retention and use during passengers' stay: the use of passenger data must be based on new circumstances justifying the use, in particular "substantive and procedural conditions governing that use in order […] to protect that data against the risk of abuse"; here, the Court requires objective evidence that PNR data must constitute an effective contribution to the combating of terrorism or other serious crimes and highlights the need for prior judicial approval or approval of an independent administrative body; • Retention and use during passengers' stay: retention and use of PNR data after a passengers' departure was deemed to not fulfil the purpose of entry and exit checks at the border anymore; here, the Court opined that such retention of data is disproportionate; only in specific cases, where "objective evidence is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada, it seems permissible to store their PNR data beyond their stay in Canada".[55]
Security of retained data and localisation of data (*Tele 2*)	• The Court stressed, first, that national legislation should provide for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period. The Court did not follow the suggestion by the Advocate General that a member state could reasonably go further and require that the data be stored within the national territory, especially in the absence of coordination of national authorities within the European Union.[56]
Data transfers in the law enforcement domain and adequacy of third countries	• Art. 34 of Directive 2016/680 introduces the 'adequacy' standard in relation to the law enforcement domain. Transfer of personal data from the EU to a third country is possible for third countries that are deemed adequate. In this context, existing bilateral agreements between an EU member state and third countries are to remain unaffected until amended (Art. 61). Adequacy decisions currently in place do not cover data exchanges in the law enforcement sector.[57]

[55] Opinion 1/15 of 26 July 2017, para. 207.
[56] Opinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 Tele 2 and Watson, para. 241.
[57] European Commission, 'Adequacy decisions', https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Key standards stemming from the Court rulings for checking legality on *Independent justice and effective judicial control in mutual recognition in criminal justice*	
Prior review of judicial body or independent administrative body	• Prior review of the conditions of access to private electronic data is indispensable, both in cases regarding PNR data and telecommunications data; access to this data is conditional on the authorisation of a judicial body or independent administrative body. • According to the Court in Digital Rights Ireland, access must be reviewed "by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions".[58] • In Tele 2, the Court the Court stressed the need to ensure review of compliance by an independent supervisory authority, as required under Article 8(3) of the Charter. This constitutes, in accordance with the Court's settled case law, an "essential element" of the right to protection of personal data and makes it possible for persons whose personal data was retained to complain to the national supervisory authority seeking the protection of their data.59
Access to that data by the authorities (*Tele 2*)	• Applying the *principle of proportionality* to the area of prevention, investigation, detection and prosecution of criminal offences, the Court reiterated that only the objective of fighting serious crime is capable of justifying access to the retained data. • Applying the *principle of necessity*, the Court found that a general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary. In this respect, the Court cited the ECtHR ruling in *Zakharov v Russia*,[60] where the ECtHR underlined the need for there to be a "reasonable suspicion" against the persons concerned. • In order to ensure that the above conditions are fully respected, the Court required that access to retained data should be subject to a *prior review carried out either by a court or by an independent administrative body* on the basis of a reasoned request by the investigating authorities. The Court specifically referred to the ruling of the ECtHR

[58] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Ireland*, para. 62.
[59] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 122-123.
[60] ECtHR, Roman Zakharov v Russia (application no. 47143/06), 4 December 2015, para. 260.

	in *Szabó and Vissy v Hungary*[61] that "in this field, control by an independent body, normally a judge with special expertise, should be the rule", except in cases of urgency.
Right to legal remedy of individuals under investigation (*Tele 2*)	• The Court stressed that the legislation should provide that the competent national authorities should notify the persons affected "as soon as this is no longer liable to jeopardise the investigations being undertaken by those authorities". Such notification is necessary to enable these persons to exercise their right to a legal remedy.[62]

[61] ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14), 12 January 2016, para. 80.
[62] Joined Cases C-203/15 and C-698/15 *Tele 2 and Watson*, para. 121.

Annex III - Inventory

AUSTRIA

Legal Framework		
Legal framework	*Primary sources*	• **Basic Law on the General Rights of Nationals**[63] o Article 9, para 1: "The rights of the home are inviolable." o Article 10: "The privacy of letters may not be infringed and the seizure of letters may, except in case of a legal detention or domiciliary visit, take place only in times of war or by reason of a judicial warrant in conformity with existent laws." o Article 10a: "[1] Telecommunications secrecy may not be infringed. [2] Exceptions to the provisions of the foregoing paragraph are admissible only by reason of a judicial warrant in conformity with existent laws." • **Personal Liberty Act**[64] o Article 1, para 2: "No one may be arrested or detained on grounds other than those named in this Federal constitutional law or in a manner other than in accordance with the procedure prescribed by law." o Article 2, para 1, explicitly provides for instances in which persons may be deprived of their liberty.
	Secondary sources	• **Criminal Code**[65] o Articles 118–120 provide for crimes aiming at the protection of persons' private sphere. Those who infringe the secrecy of correspondence (Article 118), a computer system (Article 118a), or telecommunication secrecy (Article 119), as well as abusively intercept data (Article 119a) or apply sound recording or listening devices (Article 120), will be punished accordingly.

[63] *Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder*, RGBl. Nr. 142/1867.
[64] *Bundesverfassungsgesetz vom 29. November 1988 über den Schutz der persönlichen Freiheit*, BGBl. Nr. 684/1988.
[65] *Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB)*, BGBl. Nr. 60/1974.

		○ Article 126c criminalises the creation and the making available of any computer programme or access code whereby it is possible to commit crimes linked to computer secrecy (out of the foregoing, those stipulated in Articles 118a–119). • Code of Criminal Procedure[66] ○ Article 47a: appointment and legal status of the legal protection representative (Rechtsschutzbeauftragte). ○ Article 76a, para 1: communication service providers' obligation to provide master data related to subscribers. ○ Article 135: conditions of seizure of letters, providing information on communication, localisation of technical devices, data storage, and monitoring of messages. ○ Article 147, para 1, point 5: the legal protection representative is responsible for the examination and control of the order, approval, authorisation, and execution of the monitoring of communication, localisation of technical devices, providing information on traffic data, access data, and location data, and temporary data storage. • Other relevant legislation • Security Police Act[67] • Data Protection Act[68] • Telecommunication Act[69] • Police State Security Act[70] • Decree on Interception[71] • Decree on Interception Costs[72] • Decree on the Assessment of Investment Costs[73]

[66] *Strafprozeßordnung*, BGBl. Nr. 631/1975.
[67] *Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG),* BGBl. Nr. 566/1991.
[68] *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)*, BGBl. I Nr. 165/1999.
[69] *Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003),* BGBl. I Nr. 70/2003
[70] *Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG)*, BGBl. I Nr. 5/2016.
[71] *Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung – ÜVO)*, BGBl. II Nr. 418/2001.
[72] *Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Anbieter für die Mitwirkung an der Auskunft über Daten einer Nachrichtenübermittlung, der Auskunft über Vorratsdaten und der Überwachung von Nachrichten (Überwachungskostenverordnung – ÜKVO)*, BGBl. II Nr. 322/2004.
[73] *Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über den Ersatz der Investitionskosten der Anbieter für die Bereitstellung der Einrichtungen, die zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten erforderlich sind (Investitionskostenersatzverordnung – IKEV)*, BGBl. II Nr. 107/2012.

BELGIUM

<table>
<tr><th colspan="3">Legal Framework</th></tr>
<tr><td rowspan="2">Legal framework</td><td>Constitutional provisions</td><td>Belgian Constitution
Articles 12, 13 and 14 of Belgian Constitution (in relation to the rights to the rights to freedom and fair trial)
Article 15 (inviolability of the home), Article 22 (private and family life), and Article 29 (confidentiality of communications) of Belgian Constitution.</td></tr>
<tr><td>Other provisions</td><td>Belgian Code of Criminal Procedure
Articles 46bis, 88bis, 90ter and 90quater of the Belgian Code of Criminal Procedure.
Other relevant legislation
Article 13 of the Loi du 9 décembre 2004 sur la transmission policière internationale de données à caractère personnel et d'informations à finalité judiciaire, l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'instruction criminelle.
Loi relative à la décision d'enquête européenne en matière pénale, of 22 May 2017.</td></tr>
<tr><td>Case law</td><td colspan="2">Cass. 4 January 1994, Arresten van het Hof van Cassatie 1994, n° 1.
Hof van Cassatie van België (Court of Cassation of Belgium), Nr. P.13.2082.N. of 1 December 2015.
Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016.</td></tr>
</table>

BULGARIA

Legal Framework		
Legal framework	*Primary sources*	**Bulgarian Constitution** • Articles 30-34 of the Constitution of Bulgaria contain provisions on the rights to privacy, freedom and confidentiality of correspondence, as well as the right to a fair trial and the exceptional conditions under which they may be infringed upon.
	Secondary sources	**Bulgarian Criminal Code** o Article 171 (1) A person who contrary to the law: 1. […] 2. […] 3. becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee, shall be punished by imprisonment for up to one year or by a fine from BGN one hundred to three hundred. (2) If the act was perpetrated by an official who availed himself of his official position, the punishment shall by imprisonment for up to two years, and the court may also rule deprivation of the right under Article 37 (1), sub-paragraph 6. (3) A person who, by use of special technical means, unlawfully obtains information not addressed to him, communicated over the telephone, telegraph, computer network or another telecommunication means, shall be punished by imprisonment for up to two years. […] o Article 171a (1) A person who unlawfully acquires, stores, discloses or disseminates data as those collected, processed, kept or used as per the Electronic Communications Act, shall be punished by imprisonment up to three years or probation. […] o Article 319a - Cybercrime

		(1) Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine from up to BGN 3,000. (2) […] (3) […] (4) Where acts under paragraphs 1 - 3 have been committed with regard to information that qualifies as a state secret or to another information protected by the law, the punishment shall be imprisonment from one to three years, unless severer punishment has been envisaged. (5) Where grave consequences have occurred as a result of the acts under Paragraph 4, punishment shall be of one to eight years. If law enforcement activities are conducted "according to law", and not "contrary to law", "unlawfully" or "without permission, where such is required", these provisions are not applicable. Bulgarian Code of Criminal Procedure (CCP) o Articles 159-163 contain provisions on searches and seizures; e-data is explicitly mentioned as a potential 'target' of such investigative measures. o Articles 172-177 contain provisions on Special Investigation Means, including interception of communications. o Articles 193 et seq. contain provisions on pre-trial investigations and the authorities in charge thereof. o The admissibility of e-data as evidence may be challenged according to general provisions regarding the admissibility of evidence during the pre-trial phase, court proceedings in the first instance, on appeal (articles 359-360 CPC) or during the cassation procedure [article 348(1) CCP]. o Articles 471 et seq. contain provisions on MLAT-based letters rogatory, which still apply to non-EIO international judicial cooperation requests. A centralised model is followed. Other relevant legislation • European Investigative Order Act (State Gazette, No. 16/20.02.2018) • Electronic Communications Act (Stage Gazette No. 41/22.05.2007, repeatedly amended ever since) • Special Intelligence Means Act (State Gazette No. 95/21.10.1997, repeatedly amended ever since)

GERMANY

Legal Framework		
Legal framework	*Primary sources*	**Basic Law for the Federal Republic of Germany** ○ Article 1, para 3, stipulates that "[t]he […] basic rights [as provided for in the Basic Law] shall bind the legislature, the executive and the judiciary as directly applicable law." ○ Article 2, para 1: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." ○ Article 10: "(1) The privacy of correspondence, posts and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."
	Secondary sources	• **Criminal Code**[74] ○ Article 201 protects the privacy of the spoken word by, inter alia, criminalising the "unlawful […] overhear[ing] with an eavesdropping device the privately spoken words of another not intended for his attention". ○ Article 202a penalises if one "unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection". ○ Article 202b provides that [w]hosoever unlawfully intercepts data […] not intended for him, for himself or another, by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to [phishing]". ○ Article 202c penalises acts preparatory to data espionage (Article 202a) and phishing (Article 202b). ○ Article 206 sanctions the "unlawful […] disclos[ure] to another person facts which are subject to the postal or telecommunications secret and which became known to [the perpetrator] as the owner or employee of an enterprise in the business of providing postal or telecommunications services". • **Code of Criminal Procedure**[75] ○ Articles 94–98: provisions on seizure, out of which, Articles 97–98 relate to those which may not, or may with restrictions, be subject to seizure.

[74] *Strafgesetzbuch*, BGBl. I S. 3322.
[75] *Strafprozeßordnung*, BGBl. I S. 1074, 1319.

		○ Article 100a enumerates the conditions of when "[t]elecommunications may be intercepted and recorded also without the knowledge of the persons concerned" (Article 100a, para 1). ○ Article 100b: authorities are allowed to have access to information on mobile devices before it is encrypted. Such measure must be applied by the public prosecution office and ordered by a court. ○ Articles 100c and 100f provide the opportunity of secret interception and recording of "private speech on private premises" (Article 100c) and words spoken in a "non-public context outside private premises" (Article 100f). ○ Article 100g: the public prosecutor's office and, in relation to tax offences, the tax authority are empowered to acquire certain traffic data related to customer communications, as well as to request the disclosure and, if necessary, the seizure of stored communications. ○ Articles 102–110 contain the rules and methods for conducting searches. According to Article 105, "[s]earches may be ordered only by the judge and, in exigent circumstances, also by the public prosecution office and the officials assisting it". **Other relevant legislation** • Federal Police Act[76] • Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications (Article 10 Act)[77] • Customs Investigations Services Act[78] • Telecommunication Act[79] • Act on the Federal Intelligence Service[80] • Federal Criminal Police Office Act[81] • Telecommunications Interception Ordinance[82] • Technical Directive[83]
Case law	• Judgement of 21 February 1964, BGHSt 19 325 • Judgement of 31 January 1973, BVerfG 2 BvR 454/71 • Judgement of 18 April 1980, BGH 2 StR 731/79 • Judgement of 14 July 1999, 100, BVerfG	• Judgement of 16 March 2005, 113, BVerfGE • Judgement of 4 April 2006, 115, BVerfGE • Judgement of 22 June 2017, 13 B 238/17

[76] *Gesetz über die Bundespolizei*, BGBl. I S. 2978, 2979.
[77] *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, BGBl. I S. 1254, 2298; 2007 I S. 154. Also referred to as: *Artikel 10-Gesetz*.
[78] *Gesetz über das Zollkriminalamt und die Zollfahndungsämter*, BGBl. I S. 3202.
[79] *Telekommunikationsgesetz*, BGBl. I S. 1190.
[80] *Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes*, BGBl. I 2016 S. 3346.
[81] *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*, BGBl. I S. 1354.
[82] *Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation*, BGBl. I S. 2316.
[83] *Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften*.

FRANCE

Legal Framework		
Legal framework	*Primary sources*	**French Constitution** • France's 1958 Constitution does not include specific provisions related to personal data protection or privacy guarantees. • Article 55 French Constitution imposes - par ricochet - the protection to the rights of privacy and data protection, as recognised respectively under the EU Charter of Fundamental rights (and EU law more in general), as well as under the European Convention on Human Rights.
	Secondary sources	• Criminal Code o Article 368 criminalises "listening, recording, or transmitting by means of any device whatever words pronounced in a private place by a person without that person's consent" if "done with intent to infringe on the intimacy of another's private life." No explicit exception for law enforcement activities. • French Code of Criminal Procedure o Art. 10: provides a functional definition of persons accused in criminal proceedings i.e. all "persons against whom there exist grave and concordant indications of guilt". o Art. 56-1/56-5: access to and gathering of data concerning certain categories of places and/or individuals such as lawyers, doctors, journalists and media outlets (e.g. direct involvement of judicial authorities and express *ex ante* consent of the data subject required). o Art. 57-1: establishes conditions for access to data through *perquisitions* and *requisitions* (i.e. search and seizures) directed at investigating facts related to *crimes* and *délits flagrants.* o Art. 57-1, para 3: collection of data located outside the national territory might occur at the hand of the *officier de police judiciaire* (OPJ) subject to the conditions for request and access provided for in the applicable international engagement. o Art. 60-1: information (including data from a computer system, or data processing of personal data). The addressee of such request must make the requested information available, and refusal to comply with the measure results in a pecuniary sanction.

		○ Art. 60-2 para 2: preservation order for content data under retained for a period not exceeding one year (prior authorisation from the judge of freedoms and detention required, see also Art. 77-1). ○ Article 76 para 2: searches and seizures of computer data by OPJ in the context of an *enquête préliminaire* (only possible upon prior authorisation by the public prosecutor). ○ Article 76 para 4: production and preservation of data ordered without the consent of the person concerned (only when necessary for the investigation concerns a *crime* or *délit* punishable by imprisonment for a term of three years; express request the public prosecutor to be validated by the judge of freedoms and detention of the court of first instance). ○ Article 97: gathering or preservation of electronic information in the context of the *information judiciaire* (computer data which is "necessary for the manifestation of the truth", is seized and placed in the hand of the judicial authorities responsible for the instruction of case). ○ Art. 694-15: EIO replaces the corresponding provisions of previously adopted mutual legal assistance treaties. ○ Article 694-20: EIOs originating from France must emanate directly by a judicial authority. ○ Art. 694-23: The competent French judicial authorities forward the measure they issue directly to the competent authority designated by the executing state. The Ministry of Justice, acting as central authority for EIO, may also assist in the transfer of the orders and supports issuing authorities with any other difficulty they face. ○ Article 694-29: All orders (including those requiring gathering or preservation of data) transmitted to and received by French authorities must be issued or validated by a judicial authority. ○ Article 694-30: The executing French authorities are respectively, the *Procureur de la République* or the *juge d'instruction* of the *tribunal de grande instance* territorially competent for its execution. If an EIO concerns the execution of investigative measures for which - under French criminal procedural law - a prior authorisation by an independent judge (e.g. "the judge of the freedoms and detention") is required, its recognition and execution will occur at the hand of the investigating judge. ○ Article 694-31: Grounds for non-recognising or executing an EIO to be raised by the judicial authority competent for recognition include *inter alia* privilege and immunity; *ne bis in idem*; fundamental rights; requests targeting classified information; absence of dual criminality for non-serious crime.

		○ Art. 694-33: Incoming EIOs directed at obtaining information related to the identification of subscribers with a specific phone number or persons with a specific IP address cannot lead to non-recognition or non-execution decisions by French executing authorities. ○ Art. 694-34: The French Minister of Justice may decide that an EIO from another EU country is not given recognition or execution when it considers it detrimental to fundamental national security interests, or if it finds that the EIO poses risks to a source of information; or if the order envisages the collection of classified information). ○ Article D. 32-2-1: Ministry of Justice (Office for International Mutual Assistance in Criminal Matters) might provide technical or legal assistance in cases where any difficulties are encountered by the national judicial authority or the foreign authority. Other relevant legislation • Loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers • Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale • Loi 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions • Loi 2015-912 du 24 juillet 2015 relative au renseignement • Loi 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.
Case law	French Constitutional Court, Decision no. 2016-536 QPC, 19 February 2016 French Constitutional Court, Decision no. 2005-532 QPC, 19 January 2006. European Court Human Rights (ECtHR), Medvedyev et al v France, Judgment of 29 March 2010 (Grand Chamber, Application No 3394/03).	

GREECE

Legal Framework		
Legal framework	*Primary sources*	**Greek Constitution** • Article 9bis ("9A") of the Greek Constitution (as introduced by virtue of the 2001 Constitutional Amendment) provides for an individual right to the protection of personal data in the following words: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law". The said provision prescribes a (negative) right, which aims at confining the state (and other public entities) in its use of the personal data of its citizens. Concomitants of this right are the rights to deny (or consent to) the collection and processing of one's personal data, as well as the right to be informed of any processing of data. The reference "especially to electronic means" connotes that other means of collection or processing are also restricted under the Constitution. • Article 19 of the Greek Constitution (as amended by virtue of the 2001 Constitutional Amendment) establishes (i) the absolute inviolability of all forms of communication, and (ii) a (presumably absolute) prohibition of the use of evidence acquired in breach thereof in the following words: "1. Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law. 2. Matters relating to the constitution, the operation and the functions of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law. 3. Use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited". • Other pertinent (albeit indirectly) provisions of the Greek Constitution: Article 5A (introduced by virtue of the 2001 amendment), which establishes the right to information; Article 9, providing that "every person's home is a sanctuary"; and Article 28, establishing a hierarchy between international law and domestic legislation.

	Secondary sources	• Criminal Code o Article 370bis ("370A") of the Greek Criminal Code criminally proscribes: (a) surveillance, recording, etc. of any form of distance communication or the mere tapping of any telephone device absent the consent of everyone participating in the communication [sec. 1]; (b) surveillance, recording, etc. of any other form of private communication and/or any private act(s) absent the consent of everyone participating or involved therein [sec. 2]; (c) the use of any recorded material(s) by any person [sec. 3]. The provision also introduces aggravated circumstances, e.g. for certain classes of offenders such as private investigators [sec. 4]. o Articles 370ter ("370B"), 370quater ("370Γ"), 370quinquies ("370Δ"), and 370sexies ("370E") of the Greek Criminal Code (as recently amended and/or introduced) criminally proscribe various forms of unauthorised access to information systems or e-data. Although there is no significant body of case law concerning the said provisions, their presence is expected to become more "visible" in the immediate future. o Article 371 of the Greek Criminal Code criminally proscribes breach of various forms of professional confidentiality (e.g. attorney-client confidentiality). Under paragraph 4 of the said provision, the proscribed act is justified if carried out to avoid conflict with vital interests (public or private). * Following the enactment of the new Criminal Code [Statute No. 4619/2019, in force since 1 July 2019], all the above offences (even in their aggravated forms) are now proscribed as misdemeanours (they were proscribed as felonies under the former Criminal Code). ** Although the said provisions themselves do not provide for an explicit exception covering law enforcement activities, such forms of surveillance/interception shall be justified based on a combination of Article 20 of the Criminal Code and the pertinent procedural provisions explicitly delimiting the authorities' prerogatives in investigating various forms of crime (see infra). • Code of Criminal Procedure o Article 177 section 2 provides that unlawfully obtained evidence shall not be used in criminal proceedings. Evidence obtained in breach of the provisions protecting privacy/e-data is a paradigmatic case of unlawfully obtained evidence in the above sense.

		○ Article 178 section 2 introduces the explicit obligation of judicial and prosecutorial authorities to seek and take into account all types of evidence, including exculpatory evidence, throughout criminal proceedings. ○ Article 212 introduces an exclusionary rule concerning witness testimony which would be in breach of confidentiality (under the new Code of Criminal Procedure, explicit reference is made to article 371 of the Criminal Code). ○ Article 254 applies to specific violent offences (including organised crime and terrorism), allowing for measures such as interception of e-data, real-time surveillance, lifting of confidentiality, and various forms of processing personal data. ○ Article 255 applies to corruption offences and also provides for similar measures. Again, competence lies with the Pre-Trial Chamber or the Prosecutor in cases of extreme urgency. ○ Article 265 introduces (for the first time as of July 2019) explicit provisions concerning the confiscation of digital data. ○ Article 362 concerns the admission of documents (including e-documents) to trial. ○ Article 458 regulates the filing of requests of evidence in the context of judicial assistance. The said provision applies alongside any applicable bilateral or multilateral treaty in force. ○ Article 459 regulates the reception of requests of evidence in the context of judicial assistance. The said provision applies alongside any applicable bilateral or multilateral treaty in force. Other pertinent legislation • Statute No. 4624/2019 (the new Greek Statute concerning personal data, replacing Statute No. 2472/1997). • Statute No. 4579/2018 transposing Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. • Statute No. 4489/2017 transposing the EIO Directive. • Statute No. 4070/2012 concerning the regulation of telecommunications.

		• Statute No. 3917/2011 concerning retention of data. • Statute No. 3783/2009 concerning the identification of the users of telecommunications services. • Statute No. 3471/2006 entitled "Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997". • Statute No. 3251/2004 transposing the Framework-Decision concerning the European Arrest Warrant. • Statute No. 2472/1997 entitled "Protection of Individuals with regard to the Processing of Personal Data" has largely been replaced by the new Statute No. 4624/2019. • Statute No. 2225/1994 (as consecutively amended by virtue of Statute Nos. 3340/2005, 3606/2007, 3658/2008, 4267/2014, 4411/2016, and 4481/2017) provides for the legal requirements to lift confidentiality for the purpose of national security or criminal justice. The said Statute has remained in force even after the enactment of the new Code of Criminal Procedure. • Statute No. 2068/1992, ratifying the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).
Case law (indicatively)	Decision No. 31/2018 by the Pre-Trial Chamber of Heleia. Decision No. 16/2016 by the Court of Appeals Pre-Trial Chamber of Athens. Decision No. 27/2011 by the Pre-Trial Chamber of Katerini. Areios Pagos [Supreme Court for civil and criminal cases] Decision No. 924/2009. Opinion No. 19/2005 by the District Prosecutor of Thessaloniki. Opinion No. 14/2004 by the District Prosecutor of Thessaloniki.	

HUNGARY

Legal Framework		
Legal framework	*Primary sources*	**Fundamental Law of Hungary** • According to Article VI, para 1, "[e]veryone shall have the right to respect for his or her private and family life, home, communications, and reputation […]". • Article VI, para 3, recognises the persons' right to protection of their personal data. • Article VI, para 4, stipulates that an independent authority created by means of a cardinal law is competent in supervising the protection of these personal data.
	Secondary sources	• **Act C of 2012 on the Criminal Code** o Article 224 (infringement of the confidentiality of correspondence) criminalises a) "[the] destruct[ion of] a sealed consignment containing communication which belongs to another person, or [the] open[ing] or [the] attain[ment] of such consignment for the purpose of gaining knowledge of the contents thereof, or [its] convey[ance] to unauthorised person for this purpose", and b) "[the] capture […] [of] a correspondence forwarded by means of electronic communication networks, including information systems, to another person". o Article 307 (unauthorised covert information-gathering or illegal use of covert means) provides that it is against the law a) "covertly [to] gather […] information without authorisation, for which the authorisation of a judge or the minister for justice is required, or [to] use […] any covert means for which a court order is required, or [to] exceed […] the scope of such authorisation", and b) "unlawfully [to] order […] or [to] authorise […] covert information-gathering operation for which the authorisation of a judge or the minister for justice is required, and […] [to] use […] covert means for which a court order is required".

		• Act XC of 2017 on the Code of Criminal Procedure o Article 100: the defendant and the counsel for the defendant have the right of access to the documents of the procedure after the questioning of the defendant. o Article 205, para 1: electronic data can serve as evidence. o Article 214: general rules concerning the application of covert means for collecting data. o Article 215: forms of covert means neither subject to judicial approval nor to that of the public prosecutor (e.g. application of a secretly cooperating person; gathering information related to the crime without disclosing the real objective of the procedure). o Articles 216–230: forms of covert means subject to the approval of the public prosecutor (e.g. observation of financial transactions; observation with the approval of the person concerned; use of covert investigator). o Articles 231–232: forms of covert means subject to judicial approval (secret surveillance of an information system; secret research; secret observation of a place; secret knowledge of a consignment; interception). o Article 252, para 2: the outcome of covert data collection may be used for prosecuting another crime provided that the conditions of applying covert means are applicable to this latter crime, too. o Article 302, para 1: search may extend to information systems and data carriers. o Articles 308–323: detailed rules of seizure. a) Article 308: seizure has to ensure that the piece of evidence at issue is secured so that the criminal procedure can be conducted efficiently. b) Article 309: seizure can be ordered by the court, the prosecutor or the investigation authority. It is always the court that orders the seizure of the evidence kept in a notary's office or law firm, and of that related to the activities of notaries or attorneys. c) Article 310: letters and other consignments between the defendant and the counsel for the defendant, and the notes of the counsel for the defendant pertaining to the case cannot be seized.

		d) Articles 315–316: special rules related to the seizure and the preservation of electronic data. The obligation to preserve evidence limits the rights of the owner, the controller, and the processor over the electronic data. o Article 470: the suspect and the counsel for the defendant must have access to all pieces of evidence referred to in the motion for arrest. • Other relevant legislation • Act CXXV of 1995 on the National Security Services • Act LIV of 2002 on International Cooperation Between Law Enforcement Agencies • Act C of 2003 on Electronic Communications • Act CLXXX of 2012 on Cooperation in Criminal Matters between Member States of the European Union • Government Decree No. 180/2004. (V. 26.) on the Rules of Cooperation between Electronic Communications Service Providers and Authorities Authorised for Secret Data Collection • Government Decree No. 100/2018. (VI. 8.) on the Detailed Rules of the Investigation and the Preparatory Procedures
Case law	• Hungarian Constitutional Court, Decision No. 3271/2012. (X. 4.) AB • Hungarian National Authority for Data Protection and Freedom of Information, Opinion No. NAIH-1410-4/2014/J, 24 June 2014 • Hungarian Constitutional Court, Decision No. 3082/2015. (V. 8.) AB	

IRELAND

Legal Framework		
Legal framework	*Primary sources*	**Constitution of Ireland** • Article 40.3.1°, which requires the State to "guarantee in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen" • Article 40.3.2°, specifying that the State shall "in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name and property rights of every citizen" • Article 40.5, which protects the inviolability of dwelling • Article 40.6.1°.i, mandating the State to guarantee "liberty for the exercise of" a number of rights "subject to public order and morality", including the right of citizens to express freely their convictions and opinions".
	Secondary sources	• **Communications (Retention of Data) Act 2011** o Section 1: "Serious offence" is defined in the 2011 Act as "an offence punishable by imprisonment for a term of 5 years or more". The (criminal) offences referred to in Schedule 1 to the 2011 Act are deemed to be serious offences, notwithstanding the corresponding term of imprisonment for such offences. o Section 3: obliges service providers to retain data specified in Schedule 2 for one (internet data) or two years (for telephony data). o Section 3(3): Retention must be effectuated such that the retained data "may be disclosed without undue delay" upon request. o Section 4(1)(a)-(c): Service providers are required to ensure the quality and security of retained data. o Section 4(1)(d): Service providers are required to ensure the destruction of retained data within one month after the relevant retention period. o Section 4(2): the security of data retained under the 2011 Act by service providers is supervised by the Data Protection Commission. o Section 5: specifies the four situations in which retained data may be accessed, namely:

		a) at the request and with consent of the data subject, b) in order to comply with a "disclosure request", c) upon a court order, or d) as may be authorised by the Data Protection Commissioner. Within the context of (cross-border) access for criminal investigative and prosecutory purposes, the situations under (b) and (c) above are relevant. o Section 6(1): A disclosure request may not be made by a member of the Garda Síochána below the rank of chief superintendent. o Section 6(1)(a)-(c)A disclosure request may only be made for the purpose of (a) prevention, detection, investigation, or prosecution of serious (criminal) offences; (b) safeguarding of state security; or (c) the saving of human life. o Section 6(4) and (5): permits disclosure requests to be made orally "in cases of exceptional urgency"; oral disclosure requests must furthermore be confirmed in writing within two working day. o Section 10(2) and (3): Empowers the Complaints Referee84 to receive requests from data subjects to investigate whether a disclosure request pertaining to his/her data was in conformity with the provisions of section 6 of the 2011 Act. o Section 10(4) and (7): The Complaints Referee shall notify the data subject of its finding and, if it finds that LEAs acted in contravention of section 6 of the 2011 Act in the issuance of a disclosure request, report its conclusion to the Irish President. o Section 10(5): Upon concluding that section 6 had been contravened, the Complaints Referee is entitled to apply one or both of the following remedies as it sees fit: (a) issue a direction for the LEA to destroy the relevant data, and (b) recommend that compensation be paid to the data subject. o Section 10(8): The decision of the Complaints Referee is final. o Section 12: Designates judges who are tasked with monitoring the operation of the provisions of the 2011 Act and ensuring that LEAs comply with its provisions.

[84] The Complaints Referee refers to the Complaints Referee established pursuant to section 9(2)(a) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*. This Referee shall be nominated by the Irish President, and shall be a judge of the Circuit Court or the District Court or a practicing barrister or solicitor with at least 10 years' standing (see *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, section 9(2)(b)).

		○ Section 12(1)(c): the designated judge reports to the Irish President (Taoiseach), who in turn reports to the Irish Parliament. • Data Protection Act 2018 ○ Section 60(1)(a) and (3)(a)(ii): contains a provision restricting data protection standards in the interest of criminal investigation and prosecution, even for what are considered 'minor offences'. • Criminal Justice (Mutual Assistance) Act 2008 ○ Section 73(1): A judge at a sitting of any (Irish) court to whom it appears that evidence, for the purpose of criminal proceedings have been instituted or a criminal investigation is taking place, may be obtained "at a place in a designated state",85 may make a (letter of) request for assistance. In order for a judge to issue such "letters of request", it must appear to him or her that criminal proceedings have been instituted or a criminal investigation is taking place, and that evidence for the purpose of such proceedings or investigation may be obtained at a place in a designated state. ○ Section 73(2): An application for such assistance may be made by the Director of Public Prosecutions (DPP) or by the individual charged (i.e. the accused) in criminal proceedings that have been instituted. ○ Section 73(3): The "letter of request", issued by the Irish judge, shall be sent to the Minister for Justice and Equality (as the Irish Central Authority) for transmission to the authorities of the relevant designated state; the provision permits the Director of Public Prosecutions to issue and transmit an MLA request directly to the appropriate authorities of a designated state in exceptional ("urgent") cases, the cross-border request may also be sent directly to the relevant foreign authorities. ○ Section 73(5)(a)-(d): Requests issued by Irish authorities shall be issued in writing or by any means capable of producing a written record under conditions allowing the requested (Member) state to establish authenticity, and shall include the following: A statement that the evidence is required for the purpose of criminal proceedings or a criminal investigation; Information relating to the nature and location of the evidence concerned; A brief description of the conduct constituting the offence concerned; and Any

[85] According to section 2 of the *Criminal Justice (Mutual Assistance) Act 2008*, a "designated state" includes all EU Member States, as well as any other States designated under section 4 of the Act.

		other available information that may assist the appropriate authority in complying with the letter of request. o Section 73(6): Evidence obtained through a cross-border request in accordance with section 73 of the 2008 Act may not be used for any other purpose than for which it was sought. o Section 75: The Minister for Justice and Equality, upon receipt of a mutual legal assistance request pursuant to the appropriate MLAT, will determine whether the MLA request is suitable for execution. The requirements for such a MLA request include: The request concerns assistance in obtaining specified evidential material or evidential material of a specified description;[86] The evidence is sought for the purposes of criminal proceedings or a criminal investigation in the requesting State;[87] There is power under any enactment to issue a warrant for the search of a place in respect of an offence constituted by the conduct giving rise to the request;[88] The offence for which evidence is sought is punishable in both Ireland and the EU Member State (including Iceland, Norway and Switzerland)[89] by imprisonment for a maximum period of at least 6 months,[90] or punishable in both Ireland and a non-EU designated State;[91] or the offence is a criminal offence in Ireland and an administrative offence in the requesting Member State which could give rise proceedings before a court having, in particular, jurisdiction in criminal matters.[92] The requesting authority must provide assurances that the evidence so provided would not be used for any purpose other than for which it was requested, and that such evidence will be returned when no longer required for said purpose;[93] The request will be refused if, inter alia, in the Minister considers that providing assistance would be likely to prejudice the sovereignty, security or other essential interests of Ireland or be contrary to ordre public,[94] there are reasonable grounds to believe that the request is of a discriminatory nature,[95] providing assistance would lead to violation of a person's

[86] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[87] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[88] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[89] See *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(19).
[90] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(2)(a).
[91] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(3).
[92] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(2)(b).
[93] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(6).
[94] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(a).
[95] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(b)(i).

		rights under the ECHR (including prohibition of torture),[96] or (and for as long as) providing assistance would prejudice a criminal investigation or criminal proceedings in Ireland.[97] ○ Section 75(5): If the Minister considers that a request for mutual legal assistance/cross-border request for access to electronic data meets the (abovementioned) conditions under the 2008 Act and relevant MLAT, the Minister shall direct the (Commissioner of the) Garda Síochána to obtain such evidence for transmission. ○ Section 75(8A): If the Garda Síochána is already in possession of the requested evidence, it is passed on by the Commissioner of the Garda to the requesting authority without delay. ○ Section 75(8): If the Garda Síochána is not in possession of the requested evidence a member of the Garda Síochána (not below the rank of inspector) shall apply to the judge of a relevant District Court for a production order. Evidence obtained by the Garda pursuant to a court order will be transmitted by the Commissioner of the Garda to the requesting authority without delay. ○ Section 75(14): A District Court judge may, at any sitting, vary or discharge a production order issued under section 75. • Criminal Evidence Act 1992 ○ Section 1: defines "document" as including "a reproduction in permanent legible form, by a computer or other means (including enlarging) of information in non-legible form".
Case law	• Court of Justice of the European Union (CJEU) Joined Cases C-293/12 and C-594/12 Digital Rights Ireland, Judgment of 8 April 2014, and Joined Cases C-203/15 and C-698/15 Tele2 Sverige and Tom Watson, Judgment of 21 December 2016. • European Court of Human Rights (ECHR) Graham Dwyer v Commissioner of a Garda Síochána and others [2018] IEHC 685. • Irish Supreme Court in People (Attorney General) v O'Brien People (Attorney General) v O'Brien [1965] IR 142. • Irish Supreme Court in DPP v JC Director of Public Prosecutions v JC [2015] IESC 31.	

[96] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(b)(ii)(II).
[97] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(d).

ITALY

Legal Framework		
Legal framework	*Primary sources*	Italian Constitution • Articles 14 and 15 of the Italian Constitution come into play with reference to privacy concerns in relation to cross-border access to electronic information.
	Secondary sources	Criminal Code o Article 491 bis defines the "electronic document" as "electronic support containing data or information having value as evidence". It thus clearly still conceives evidence as something material. o Article 1(1)(p) Legislative Decree 82/2005 (Codice dell'Amministrazione Digitale) updated such definition, focusing on the digital "representation" of acts, facts and data legally relevant (Art. 491 bis CC) o Law 48/2008 equally acknowledges a distinction between electronic evidence and their digital support. Code of Criminal Procedure (CCP) • Articles 723-729 regulate traditional mutual legal assistance tools o Article 723–726 ter CCP explicitly covers cases in which national authorities are requested to collect or transfer evidence to another country o Article 727–729 CCP covers cases in which national authorities requested another country to collect or transfer evidence. • Law 48/2008 (implementing the Cybercrime Convention) amended the Code of Criminal Procedure introducing provisions on the use of new technologies: o Article 254 bis CCP, dealing with the acquisition of data from ICT providers. o Article 615 quinquies, 635 bis CC; Article 244(2), 247(1)(bis), 254, 352(1)(bis), 354(2) of the Italian CCP have been amended to regulate cases in which electronic evidence are involved. o Article 247(1)(bis) provides for "the gathering of data, information, computer programs or any trace of an offence" that "one may find in a computer system". o Article 723 CCP: the Ministry of Justice has to exercise a political scrutiny of all requests coming from a foreign country with reference to state sovereignty, security and the fundamental interests of the state, respect of the law and public order, safeguard of the defendant against any discrimination, etc. o Article 724 CCP: The file then proceeds to the judicial authority, scrutinising the admissibility of the request and its execution. The public prosecutor receives documents from the Ministry and sends its requests to the Court of Appeal where the investigation must take place

		• Legislative Decree 52/2017 implemented the **Convention on mutual assistance in criminal matters** between EU Member States: crucial role to judicial authorities, whereas the Ministry of Justice only intervenes in specific cases. By virtue of Art. 8, the competent authority to receive and handle requests is the public prosecutor of the district court where acts have to be executed. In order to simplify the procedure, there is no involvement of the Court of Appeal, that intervenes instead for mutual assistance cases (Art. 724 CCP) o Article 8(2): the Judge for Preliminary Investigations is instead competent for receiving and handling requests when foreign authorities require the involvement of an independent judicial authority ("sitting judge") or because the domestic legal order so requires (e.g. in the case of interception of communications). o (Art. 8(4) and (5)): the execution of the requests must comply with formalities indicated by the foreign authority to safeguard the possibility to use the information requested at trial. o Article 19 relates to the need for Italy to help in interceptions taking place in the requesting State or a Third State, which is still party of the Convention. o Should the interception take place in Italy, the prosecutor must obtain the authorisation of the Judge for the Preliminary Investigations (Art. 20). The interception must refer to an offence which would allow interceptions under Italian law. o Should there be urgent matters, the public prosecutor can proceed autonomously and ask for validation from the Judge for Preliminary Investigations within 48 hours (Art. 20(1) which corresponds to Art. 267(2) CCP). o Article 22 then provides for cases where interceptions are ordered for by the Italian authority, which require the assistance of a foreign authority. In such cases the request is sent by the public prosecutor. Should the interception take place abroad, the Italian authority must send a copy of the interception warrant to the foreign authority, which can stop the interceptions at any time. • Legislative Decree 108/2017 puts into effect Directive 2014/41/UE on the European Investigation Order. Legislative Decree 52/2017 continues to be applicable at least for Member States not bound by the 2014 EIO Directive, and countries which do not belong to the EU but have signed the 2000 Brussels Convention, such as Norway and Iceland. o Articles 43 and 44 identify the public prosecutor as the competent authority to send an EIO requests, bypassing the fact that Art. 267 CCP requires the authorisation of the Judge for the Preliminary Investigations (GIP) for interceptions to take place in Italy.

		○ Art. 9(1) and (3) highlights that the EIO request must be refused should there be no prerequisites requested by Italian law. ○ In order to guarantee a coordination, if the investigation concerns organised crime or terrorism offences (Art. 51(3)(bis) e (quater) CCP), the Antimafia National Directorate must be informed. ○ Article 5 of the Legislative Decree specifies cases when the judge must be involved, because of a request of the foreign authority or because the Italian legislation provides so (e.g. for the compulsory collection of biological samples ex Art. 359 bis CCP). • By virtue of Art. 7 of the legislative decree, the executing authority in Italy can operate a proportionality test. The Italian authority could also decide to choose a less invasive investigative tool in the name of proportionality, thus better safeguarding individual rights, while preserving the efficiency of international cooperation. Such choice becomes mandatory should the act required not exist under Italian law or should Italian law not provide the use of such investigative tool with reference to the offence under investigation (Art. 10 legislative decree). • Article 189 CCP: If evidence not regulated by law is requested, the judge may introduce it if it is deemed suitable to determine the facts and does not compromise the moral freedom of the person. After hearing the parties on the methods for gathering evidence, the judge shall order the admission of evidence. • Law 48/2008 provides for the main objectives for law enforcement authorities, in line with international best practices.
Case law	• Cass., I, 18 ottobre 2001 in MLA cases, even when the request has been sent directly to a public prosecutor by a foreign authority (because the mutual legal agreement in question provides so), the Court of Appeal is still competent for the execution of the request. • Cass pen, sez. V, sentenza 16/01/2018 n° 1822 on the use at trial of WhatApp messages and SMS stored in a seized cell phone. • Cass. Sez. Unite, Sentenza no. 15208 of 25 February 2010. The *Corte di Cassazione* decided that evidence gathered abroad are inadmissible only if gathered in contrast with provision of public order or good morals, which are not necessarily identifiable simply with defence rights. • Cass. Sez. 6, Sentenza no. 44488 of 1 December 2010 and Cass. Sez. 6, Sentenza no. 43534 of 24 April 2012. Evidence cannot be gathered in contrast with the fundamental principles of the Italian legal system, including defence rights. • Cass. Sez. II, Sentenza no. 44673 of 12 November 2008. Documents spontaneously produced by foreign judicial authorities and sent to the Italian authorities have been considered admissible as evidence at trial.	

LUXEMBOURG

Legal Framework		
Legal framework	*Primary sources*	**Luxembourg Constitution** • Art. 28: Secrecy of all communications; the law shall determine which responsible agents may violate this principle with regard to letters, and shall determine the protection to be given to the secrecy of telegrams.
	Secondary sources	• **Luxembourg Criminal Code** o Art. 458 enshrines as a criminal offence punishable by imprisonment of 8 days to 6 months and a fine of 500 to 5000 EUR any doctor, surgeon, health officer, pharmacist, midwife or any other person holding, by state or by profession, secrets confided to them, except when called upon by justice to reveal them. This provision expressly applies to telecommunications operators / service providers when called upon to cooperate in criminal justice context by virtue of Art. 48-27 of the Code of Criminal Procedure (cited below). • **Luxembourg Code of Criminal Procedure** o Art. 7-2 establishes that "any offence of which an act characterising one of its constitutive elements has been committed in the Grand Duchy of Luxembourg shall be considered to have been committed on the territory of the Grand Duchy". o Arts 5 – 7-4: several provisions providing for extraterritorial jurisdiction where offence is committed abroad but the perpetrator is either a Luxembourg national or resident or a foreign citizen present on Luxembourg territory. o Art. 24-1: with respect to all misdemeanours (*délits*), the public prosecutor may request that the investigating judge order a search of private premises, the hearing of a witness or an "expertise" without opening a judicial inquiry (*instruction préparatoire*)." However, beyond misdemeanours, the public prosecutor's power to do so is limited to certain *infractions* (use of forged documents; theft with aggravating circumstances or with violence). Furthermore, since 2014, and in this case only for those *infractions* just stated and misdemeanours carrying a correctional penalty of at least one year, the public prosecutor may also take the *mini-instruction* route to have an investigating judge order the "tracking and localisation" of telecommunications (Arts. 24-1(1) & 67-1). o Art. 33(1): public prosecutor may order that a search be carried out – at any time of day or night – of the residence of persons who appear to have participated in the commission of a criminal offence or

		(widening the scope of the provision) to possess *pièces, données ou objets* relating to the criminal acts in question. o Art. 48-25: rapid preservation of data; introduced in 2014 implementing Budapest Convention. o Art. 48-27: mandatory provision of subscriber data by telecommunications operators/service providers on pain of sanction (*inter alia* fine of 1,250 to 125,000 EUR) when requested by investigating judge, public prosecutor or (in urgent cases) the judicial police – who must provide reasoned, written decision within 24 hours to state prosecutor or investigating judge. Art. 458 Criminal Code also applies (see above). o Art. 49: in Luxembourgish law, unless otherwise stated a judicial inquiry is mandatory for crimes; it is optional for misdemeanours (*délits*). o Art. 51: The investigating judge may perform, in conformity with the law, any *acte d'information* which s/he deems to be useful to discovering the truth. S/he gathers and verifies, with equal care, the facts and circumstances tending to inculpate or exculpate (*à charge ou à décharge*) the *inculpé*. o Art. 65: Searches may be carried out in any place where objects may be found which could be useful for the discovery of the truth. o Art. 66(1): The investigating judge's powers of seizure cover any object, document, effects, data stored, processed or transmitted in an automated data processing or transmission system…. o …. as well as, via Art. 31(3): effects which have been used to commit a crime or which were destined to be used as such and those which have formed the object of the crime, as well as everything which appears to have been the product of the crime, as well as in general, all that appears useful to the discovery of the truth or the use of which would be of such as nature as to harm the good workings of the *instruction* and all that is liable to confiscation or restitution. o Art. 66(3): Seizure of data can be done either by taking possession of the device ("*support physique*") or by making a copy of the data made in the presence of the persons attending the search. If a copy is made, the investigating judge may order the definitive erasure of the data on the device, where the device is located in Luxembourg and is not "in the hands of justice", where possession or use of the data is illegal or dangerous for the security of persons or goods. o Art. 126: possibilities to challenge before *chambre du conseil* a request for *grande entraide* issued by investigating judge.

		○ Art. 48-2: possibilities to challenge before *chambre du conseil* a request for *petite entraide* emanating from public prosecutor. **Other relevant legislation** • Loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale, as amended. • Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques. • Loi du 27 février 2011 sur les réseaux et les services de communications électroniques. • Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques. • Loi du 27 juin 2018 adaptant la procédure pénale aux besoins liés à la menace terroriste et portant modification 1) du Code de procédure pénale, 2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 3) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques. • Loi du 1er août 2018 portant 1° transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale ; 2° modification du Code de procédure pénale ; 3° modification de la loi modifiée du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale.
Case law	Judgment of the *Cour d'appel,* 11th March 2008 Judgment of the *Cour de cassation du Grand-Duché de Luxembourg,* N° 14/2014 *pénal*, 13th March 2014	

The NETHERLANDS

Legal Framework		
Legal framework	*Primary sources*	**Dutch Constitution** • Art. 10: right to privacy. • Art. 11: right to inviolability of his person. • Art. 12: right to the inviolability of one's home; prior identification and notice of purpose shall be required to enter a home; a written report of the entry shall be issued to the occupant as soon as possible. If the entry was made in the interests of state security or criminal proceedings, the issue of the report may be postponed under rules to be laid down by Act of Parliament. A report need not be issued in cases, to be determined by Act of Parliament, where such issue would never be in the interests of state security. • Art. 13: The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament. • Art. 93 and 94: the Netherlands is a monist country; provisions of treaties and of resolutions by international institutions which may be binding on all persons by virtue of their contents shall become binding after they have been published.
	Secondary sources	• **Code of Criminal Procedure** (*Wetboek van Strafordering*) o Art. 5.4., Book 5: provisions on the European Investigative Order (EIO). o Art. 125n: a public prosecutor may request from a communication service to identify and provide traffic data for specific users. If the request concerns a person who can claim protection as a source, the public prosecutor requires authorisation by an investigative judge. o Art. 126na: investigating officers may request user/subscriber data from a communication service. Written report is required. o Art. 126nb: seizing of communications equipment by order of a public prosecutor for a maximum of one week. Written report is required.

		○ Art. 126nba: bugging/infiltration of a technical device of system ordered by the public prosecutor and authorised by an investigative judge for serious crimes and more intrusive measures for serious crimes that carry a prison sentence of 8 years or more. Written report is required. ○ Art. 126nc: investigative officers may request identifying data in relation to a crime person who is reasonably eligible for it and who processes data other than for personal use, provide certain stored or recorded identifying data of a person. Identifying data is: a) name, address, place of residence and postal address; b) date of birth and gender; c) administrative characteristics; d) in the case of a legal person, instead of the information referred to under a) and b): name, address, postal address, legal form and location. The request cannot relate to personal data regarding a person's religion or belief, race, political affiliation, health, sexual life or membership of a trade union. A written report must be drawn up. ○ Art. 126nd: a public prosecutor may request data in relation to a serious crime from those who can reasonably be suspected of having access to certain stored or recorded data, demand this data. The public prosecutor's request is conditional upon authorisation by an investigative judge where the data concerned relates to personal data concerning a person's religion or belief, race, political affiliation, health, sexual life or membership of a trade union (sensitive data). In any case, the public prosecutor must draw up a written report. ○ Art. 126nf: the investigative officer may request data in relation to a serious crime from a person who can reasonably be suspected of having access to images made with cameras for the protection of goods, buildings or persons. Such requests cannot be addressed to the suspect. In case the data includes sensitive personal data, i.e. data relating to a person's religion or belief, race, political affiliation, health, sexual life or membership of a trade union, such a request can only be made by a public prosecutor and is conditional upon authorisation of an investigative judge. ○ Art. 126ng: fall back measure for public prosecutors to request other data from communication service providers than those covered by Articles 126n and 126na. ○ Art. 126nh: a public prosecutor may request the encryption of data by a person who can reasonably be believed that he has knowledge of the method of encrypting the data referred to in these articles, orders that he will cooperate in decrypting the data by reversing the encryption, or making this knowledge available. This order cannot be given to a suspect, only to a third party.

		○ Art. 126ni: a public prosecutor can request the freezing of data for a maximum period of 90 days (with the possible of extending it once) for data held by those who can reasonably be suspected of having access to certain data stored in an automated system at the time of the request and data which can reasonably be assumed to be particularly susceptible to loss or alteration. In case this request is aimed at communications service providers, the provider is obliged to provide as soon as possible the information required to identify the other providers whose services have been used in the communication. A written report must be drawn up. ○ Art. 339: the judge admits evidence based on the principle of 'intimate conviction' and provided that it was collected using legal means. In addition, only certain forms of evidence are admitted (i.e. may be cited as proof in the judgement), which includes: own conviction or opinion of the judge; declarations of the suspect; declarations of a witness; declarations of an expert; and 'written documents'. ○ Art. 344: Evidence obtained from abroad, including the e-data files, protocols and transcripts issued by foreign authorities, are considered a 'written document'. Such documents, as long as they originate from/are certified by the competent (foreign) authorities and are composed in accordance with the legally prescribed format, are directly admissible in the Dutch proceedings. Other relevant legislation • Wet Bijzondere Opsporingsbevoegdheden, Wet BOB • Telecommunicatie Wet • Wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten met het oog op het moderniseren van de regeling van internationale samenwerking in strafzaken (Herziening regeling internationale samenwerking in strafzaken) • Wet tot wijziging van het Wetboek van Strafvordering ter implementatie van de Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie Richtlijn Europees onderzoeksbevel)

		• Aanwijzing Opsporingsbevoegdheden • Besluit tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 31 mei 2017 tot wijziging van het Wetboek van Strafvordering ter implementatie van de Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie Richtlijn Europees onderzoeksbevel)
Case law	Dutch Supreme Court HR, 25 February 2003, NJ 2003, n. 571 Dutch Supreme Court HR 14 September 1987, NJ 1988. N. 301	

SPAIN

Legal Framework		
Legal framework	*Primary sources*	**Spanish Constitution** • Article 18, Section: protects the rights to privacy, including in the context of criminal investigations. • Art. 18, Section 3: strictly requires prior judicial authorisation for acts or decisions interfering with the right to secrecy of communications.
	Secondary sources	• **Criminal Code** o Article 33.2. of the Criminal Code: classifies criminal penalties based on their nature and duration. Penalties are classified as serious, less serious and light. Serious penalties are those corresponding to a term of imprisonment of more than five years. • **Spanish Code of Criminal Procedure** o Article 579.1: introduces two criteria for determining the degree of seriousness that an offence must present in order to justify the retention, access and communication of personal data for law enforcement and criminal justice purposes. The first is a substantive criterion relating to serious criminal offences, including, in particular, offences committed in the context of a criminal organisation and terrorism offences. The second is a formal normative criterion, which sets a lower threshold of three years' imprisonment. o Article 588 bis (a): sets out general 'guiding principles' - and in particular the principles of speciality, suitability, exceptionality, necessity and proportionality – that must be complied with by the authorities issuing and/or implementing measures of technological inquiry. o Article 588 bis (b) para 2: requests for data made by police or prosecutors must often undergo prior scrutiny by a competent judicial authority. Their request for judicial validation shall contain the description of the facts, the object of the inquiry, indicate the identity of the person under investigation or of any other person affected by the measure (provided that such data are known), justify the necessity and utility of the requested data for the purpose of investigating the crime at hand, and specify scope and implementation modalities of the investigative measures for which authorisation is sought. o Article 588 bis (c): Upon reception of a police or prosecutor's request, the investigating judge – having heard the prosecutor – has 24 hours to decide whether to authorise or refuse its execution.

		○ Article 588 bis (g): The judicial police is under the obligation to report the results of the data-gathering measure to the investigating judge, and also the way in which it was carried out. ○ Article 588 ter (a): circumscribes the interception of electronic (and telephone) communication involving the investigated individual (either as transmitter or receiver) to serious offences, or offences committed through software tools or any other information or communication technology or communication service (cybercrime). ○ Article 588 ter (b), para 1 and 2: requires prior authorisation by a court for interception of electronic (and telephone) communication involving the investigated individual (either as transmitter or receiver) when the investigative measure entails access to the content of such information. The same requirement applies to the interception of traffic data, and data associated with the communication process or generated regardless of the establishment of a specific communication between the suspect and third parties. Special rules apply when the interception request affects third parties. ○ Article 588 ter (d) specific (additional) information must be included in police requests for judicial authorisation when the latter are directed at obtaining an authorisation for the interception of electronic communication. ○ Article 588 ter (e): imposes a duty to cooperate upon "all the providers of telecommunications services, of access to a telecommunications or services network of the information society, as well as any person that contributes in any way to facilitate the communications". ○ Article 588 ter (j): A prior judicial validation must be obtained when investigative measures are directed at obtaining data contained in the automated files of service providers. Such an authorisation must be obtained *ex ante* for measures targeting retained data, and data related to the communication process. ○ Article 588 ter (k): Requires judicial validation by the investigating judge for requests concerning information sought in relation to the ownership of a phone number or of any other communication, or the telephone number or the identifying data associated with the means of communication. Judicial validation is required when such information is not recorded, and the police and prosecutor need it for the identification and location of the terminal, connection device, or, for the identification of the suspect behind an IP address used to commit a crime, a request for access must be authorised. ○ Article 588 ter (l): IMEI and ISMI codes can also be tracked by the police without any judicial intervention. In case of emergency, the judicial police or the prosecutor may also search storage devices without judicial authorisation.

		o Article 588 ter (m): Subscriber data and, more generally, the data allowing the identification of the owner of a communication means (e.g. subscriber information, email addresses) can be requested by the public prosecutor or the judicial police directly from the service providers. o Article 588 sexies (a): When seeking access to electronic data repositories seized during traditional (i.e. house/physical) searches, the police or prosecutors must present an 'individual justification' specifying the grounds legitimating the access to the information contained in these devices to the investigating judge responsible for validating the request. o Article 588 sexies (c), para 3: In cases of emergency, the judicial police or the prosecutor may search storage devices without judicial authorisation. They must, however, immediately inform the magistrate about these emergency searches, the way in which they were conducted, and the results obtained. The competent magistrate may then confirm or revoke the measure. o Article 588 Octies: Preservation can be ordered for a maximum period of ninety days, which may be extended once, until the transfer is authorised. o Article 773 para 2: Opening of a criminal case. The trial preparation requires prior investigation and records of the commission of the offence and the circumstances including its perpetrator. The police investigation will be conducted in a preliminary stage, aimed at providing relevant and sufficient information to enable the public prosecutor to launch a formal prosecution. The latter is only opened when the investigating judge considers that there is sufficient evidence to open a formal investigative stage and/or pre-trial investigation. Under Spanish law, the investigative stage and/or pre-trial investigation is still conducted by a judge, generally the investigating judge. Other relevant legislation • Ley 25/2007 on the retention of data relating to electronic communications and to public communication networks) of 18 October 2007 o Article 3: Extends the prior judicial validation requirement to requests concerning different categories of retained data, including most notably traffic data, location data, as well as data necessary to identify subscribers or registered users o Article 5 para 2: Introduces an obligation for private companies to communicate retained data to authorised Spanish law enforcement authorities.

		• Ley Orgánica 13/2015 reforming the Code of Criminal Procedure for the strengthening of procedural guarantees and the regulation of he means of technological investigations. • Ley 23/2014, of 20 November on mutual recognition of criminal justice decisions within the EU. • Ley 3/2018, of 11 June, modifying Ley 23/2014, of 20 November on mutual recognition of criminal justice decisions within the EU for regulating the European Investigation Order. • Ley 59/2003.
Case law	*Constitutional Court* STC 62/1982 (Doctrine reiterated in: SSTC 181/1995; 49/1996; 54/1996; 123/1997; 49/1999; 166/1999; 171/1999; 236/1999; 126/2000; 14/2001; 202/2001; 82/2002; 167/2002; 184/2003; 205/2005; 259/2005; 104/2006; 239/2006) STC 70/2002 STC 123/2002 STC 26/2006 STC 173/2011 *Supreme Court* SSTS, 24 February 2015 SSTS no 16/2014 SSTS, 17 April 2013 SSTS, 20 May and 18 November 2008, and of 28 January 2009 STS Decision no. 737/2009 SSTS, 9 and 28 of May 2008 SSTC n. 161/1990 SSTC n. 150/1987	

SWEDEN

Legal Framework		
Legal framework	*Primary sources*	**Swedish Constitution** • The constitutional provisions on fundamental rights and freedoms contained in the **Freedom of the Press Act (*tryckfrihetsförordningen, TF*)** and the **Fundamental Law on Freedom of Expression (*yttrandefrihetsgrundlagen, YGL*)** are exclusive. Among other things, this means that it is exhaustively stated what opinions in the constitutionally protected media are allowed and who is responsible, under criminal liability, for possible violations.[98] Only the Chancellor of Justice may initiate a preliminary investigation for crimes as referred to in the Freedom of the Press Act and the Fundamental Law on Freedom of Expression. Only the Chancellor of Justice may decide on coercive measures for such crimes and there are special procedural provisions in these cases. If a question arises about the execution of an investigation order based on an offence covered by the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, consultations shall be held with the Chancellor of Justice. • In principle, the Directive and the implementing legislation cover all types of evidence gathering, including interrogation, seizure, body inspection, temporary transfer of detainees and secret coercive measures. These measures constitute such restrictions on the fundamental rights and freedoms that according to **Chapter 2 of the Swedish Instrument of Government,** [99] can only be regulated by law. • According to **Chapter 10, Section 13 of the Instrument of Government**, Swedish Prosecutors are obliged to notify the Head of the Ministry of Foreign Affairs when matters that are relevant to the relationship with another state arise. This may be applicable in cases where another state issues an EIO received by Sweden, as well as when Sweden issues an investigation order to another member state. The Legal Department shall be informed in these situations, and notifies the Ministry of Foreign Affairs.
	Secondary sources	• In general, the most relevant rules regulating what measures the Law Enforcement Authorities can take while investigating crimes can be found in **Chapter 23 (Preliminary Investigation), Chapter 27 (Seizure,**

[98] See Prop. 2016/17: 218 p. 139, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 66.
[99] *Regeringsformen (1974:152).*

		Secret Wire-tapping, etc.) and Chapter 28 (Search of Premises, Body Search and Body Examination) of the Swedish Code of Judicial Procedure.[100] • Some basic principles govern how a Swedish preliminary investigation should be conducted. Chapter 23, Section 4 of the Code of Judicial Procedure stipulates that a preliminary investigation shall be conducted objectively. In addition, it is stated that it should be conducted so that no person is unnecessarily exposed to suspicion, or put to unnecessary cost or inconvenience, the so-called principle of consideration (*hänsynsprincipen*). Four general principles apply primarily to the use of coercive measures against individuals: the principles of legality, purpose, need and proportionality (*legalitets- ändamåls-, behovs- och proportionalitetsprinciperna*). These principles guide the prosecutor's assessment of which measures should be subject to a Swedish investigation order.[101] • What may be considered necessary and proportionate is assessed in the individual case. In addition to the proportionality test under national law, issuing an investigation order shall be weighed against another member state's provision of staff and other resources to assist a Swedish prosecutor or court.[102] The offences to which the investigation order refers should be taken into account in this assessment, even if the penalty thresholds for the execution of the measure under Swedish law are met.[103] An executive authority may, if there is reason to assume that any of the conditions are not met, consult the issuing authority on the importance of executing the investigation order (Article 6(3) EIO Directive). After consultation, the issuing authority may withdraw the investigation order. • The rules of the Code of Judicial Procedure for information to the person entitled to appeal a final decision is applicable to the District Court's decision (Chapter 30, Section 10, second paragraph and Section 11). The possibility of appeal is open even when a decision on an action has been taken in connection with a foreign investigation order. • According to Chapter 23, Section 18, first paragraph of the Code of Judicial Procedure, the suspect and his or her defence counsel have the right to state the inquiry they consider desirable and otherwise state whatever they deem necessary. At the request of the suspect or his or her counsel, in accordance with the

[100] *Rättegångsbalken (1942:740).*
[101] Prop. 2016/17: 218 p. 93, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 20.
[102] See Prop. 2016/17: 218 p. 94f, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 20.
[103] Prop. 2016/17: 218 p. 94, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 20.

		second paragraph, interrogation or other investigation shall take place, if this may be considered to be of importance to the investigation. If such a request is refused, the reasons for this shall be stated. • Chapter 23, Section 19 of the Code of Judicial Procedure states that, if investigators do not approve such a request for investigation, the person concerned may report this to the court, who shall examine the notification as soon as possible. • Based on Chapter 45, Section 10 of the Code of Judicial Procedure the accused may also invoke evidence meaning that the court needs to issue an investigation order. No special provision has been introduced that an investigation order may be issued at the request of a suspect, accused or his or her defence counsel. • The decisions of the Court in these matters are decisions in the trial (see Chapter 30, Section 1, Code of Judicial Procedure) and may not be appealed separately, cf. Chapter 49, Section 3, unless there is a question under Chapter 49, Section 5 of the Code of Judicial Procedure (see especially point 6). • Chapter 4, Section 1 of the EIO Act states that there are only a few actions in an investigation order that may be appealed. A prosecutor should therefore, in connection with the notification pursuant to Chapter 23, Section 19 Code of Judicial Procedure expresses his or her views on the conditions for issuing an investigation order. • In Sweden witnesses are only interviewed under oath before courts of law during a trial (unless they are exempted because of a close relationship with any party). During a preliminary investigation, when witnesses are questioned by the police, they are informed about the importance of speaking the truth, but are not required to take an oath and it is therefore not illegal to lie. In Sweden, almost any evidence is allowed before the courts, and it is for the court to evaluate the evidence. Swedish prosecutors try to adapt to foreign formalities, but sometimes it is not possible since it challenges fundamental principles in Swedish law. • The investigation order for the taking of evidence shall be conducted in accordance with the law of the executing country. This means that consideration should be given to, as a special procedure, the request that defendants and plaintiffs not be heard under oath or equivalent assurance, as this would contravene basic legal principles in Swedish law. • If there is reason to assume that a witness to be heard at the foreign court is related to a party, the court should also state that the witness must be informed that he or she is not required to file a testimony (Chapter 36, Provisions 3 and 10 Code of Judicial Procedure).

		• The court should ask that the relatives of the defendant do not take an oath as there is a ban on this in **Chapter 36, Section 13 of the Code of Judicial Procedure**. • Provisions concerning the conditions for issuing an investigation order can be found in **Chapter 1, section 4, point 6 and Chapter 2, sections 1, 3 of the EIO Act**. • According to **Chapter 2, Section 5 of the EIO Act**, before issuing an investigation order, the prosecutor needs to apply for the court's examination of the prerequisites regarding secret camera surveillance and secret interception. • However, according to **Chapter 2, Section 5, second paragraph of the EIO Act,** pending a court trial, the prosecutor may issue an investigation order for secret camera surveillance under the conditions set out in **Chapter 27, Section 21 of the Code of Judicial Procedure.** (The provision does not apply to secret interception.) The prosecutor shall report to the court that such an investigation order has been issued without delay. **Other relevant legislation** • International Legal Assistance in Criminal Matters Act (2000:562) (*LIRB Act*).[104] • Chapter 2, Section 11 of the LIRB Act. • Act on Joint Investigation Teams for Criminal Investigations (2003:1174).[105] • Act (2017:1000) on a European Investigation Order (EIO Act).[106] • Chapter 3, Section 15 of the EIO Act: A request for a particular procedure to apply when a requested measure in an investigation order is executed must be met, unless such formalities and procedure are contrary to the fundamental principles of the Swedish legal order (**cf. Article 9(2) of the EIO Directive**).

[104] *Lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB)* (Government Bill 1999/2000:61; Government Bill 2004/05:144). See also The International Legal Assistance in Criminal Matters Ordinance (2000:704). The agreements that the International Legal Assistance in Criminal Matters Act (2000:562) refers to are listed in the Notification (2005:1207) concerning agreements referred to in the International Legal Assistance in Criminal Matters Act (2000:562).
[105] *Lag (2003:1174) om vissa former för internationellt samarbete i brottsutredningar*) (Government Bill 2003/04:4; Government Bill 2004/05:144); The Ordinance on Joint Investigation Teams for Criminal Investigations (2003:1174). Framework decision of 13 June 2002 on joint investigation teams (2002/465/RIF).
[106] *Lag (2017:1000) om en europeisk utredningsorder.*

		• **EIO Ordinance (2017:1019):**[107] **Article 16(2)(c) of the EIO Directive** provides for an obligation for the executing authority to inform the issuing authority if it has been decided in individual cases that the specific formalities and procedures requested cannot be complied with. The notification obligation has been introduced in **Chapter 3, Section 8, point 3 of the Ordinance**. In **Chapter 2, Section 11 of the LIRB Act** there is a corresponding provision with similar wording as regards legal assistance in criminal matters. • There are a number of international legal instruments that enable cooperation, such as legal assistance, EIO (since December 1, 2017), Nordic and European arrest warrant and extradition. • The **International Legal Assistance in Criminal Matters Act (*LIRB Act*)** mainly consists of cooperation between prosecutors and courts. International police and customs collaboration is regulated by other laws. The *LIRB Act* does not cover extradition, surrender or the service of documents for which special legislation exists. Cooperation with international tribunals and the International Criminal Court is also regulated by other laws. Likewise, investigation measures during the police investigation and investigation work are not covered by the EIO. Neither acts in the area of enforcement of judgments fall within its scope. • **The EIO Act,**[108] **and a new EIO Ordinance,**[109] entered into force on 1 December 2017.[110] At the same time, amendments were made to **the *LIRB Act*** and other acts,[111] along with certain consequential amendments to ordinances. **The EIO Act and the EIO Ordinance** replace the corresponding provisions of the *LIRB Act*, **Act (2005:500) on the recognition and enforcement of the Freezing Decree**, and **Act (2003:1174) on certain forms of international cooperation in criminal investigations**. • It is the issuing prosecutor or court that will send the investigation order to the competent authority (**Chapter 2, Section 7 of the EIO Act)**. • **The EU-convention from 2000 on mutual legal assistance (MLA) in criminal matters** direct communication is assumed, as a main rule. • **Chapter 1 Section 7 of the *LIRB Act*** states that a Swedish prosecutor may apply for legal assistance abroad to the extent permitted by the other state. As long as the requested state allows, prosecutors may apply

[107] *Förordning (2017:1019) om en europeisk utredningsorder.*
[108] *Lag (2017:1000) om en europeisk utredningsorder.*
[109] *Förordning (2017:1019) om en europeisk utredningsorder.*
[110] Govt Bill 2016/17:218 *Nya regler om bevisinhämtning inom EU* SFS: 2017:1000–1021.
[111] Mainly, *lagen (2000:562) om internationell rättslig hjälp i brottmål; lagen (2005:500 om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut (frysningslagen);* and, *lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar*.

		for actions other than those mentioned in the ***LIRB Act***, and it is the requested state that decides on the investigation measure based on its regulatory system. Hence, a Swedish prosecutor can apply for legal assistance with a measure that is possible in the other state, even if such a measure is not directly apparent from *LIRB's* provisions or even available under Swedish law. The ***LIRB Act*** differs significantly from the system provided for in the EIO Act. • The decision to issue a cross-border request for access to e-data is taken by the judicial authority that issues the request/order, which in Sweden is the prosecutor. This is a general rule, regardless if the request is for e-data or other types of evidence. The investigative measures that may be taken are listed in **Chapter 1, Section 4 of the EIO Act**. **Paragraph 12** of the section states that other measures that do not involve the use of force (*tvångsmedel*) or other means of coercive measures (*tvångsåtgärd*) may be taken. • The competent court to grant permission is set out in **Chapter 19 Code of Judicial Procedure** (see its section 12). • A Swedish court has jurisdiction to issue an investigation order for the following measures: Taking of evidence at a foreign or Swedish court; Interrogation through audio and video transmission or by audio transmission in connection with proceedings; and, transfer of a detained person to or from Sweden in connection with proceedings. • The Swedish prosecutor's jurisdiction to issue an investigation order is more general (**cf. Chapter 2, Section 1, and Chapter 1, Section 4 of the EIO Act**). It covers all measures available during an ongoing preliminary investigation if the evidence had been available in Sweden. Exceptions apply to the taking of evidence at a foreign court during preliminary investigations and evidence in Sweden according to the Code of Judicial Procedure, at the request of the prosecutor. In these cases, the court decides. In addition, if the preliminary investigation needs to be resumed during the main proceedings, the prosecutor is responsible for issuing a Swedish investigation order. • According to **Chapter 2, Section 3 of the EIO Act**, an investigation order may be issued if the conditions that apply to conduct the investigation action during a Swedish investigation or trial in criminal proceedings and according to this law are met. A Swedish prosecutor may issue an investigation order for such investigation measures that could have been taken in Sweden under equivalent conditions if the evidence had been available in Sweden. This means a Swedish prosecutor, for example if he or she wishes to request interrogation during the preliminary investigation, must make sure that the conditions set forth in the provisions of **Chapter 23, Code of Judicial Procedure**, and the **Preliminary Investigation Proclamation**

		(1947:948) (*Förundersökningskungörelsen, FUK*) for the measure are met. Sometimes several alternative measures are possible. The least intrusive should then be chosen in accordance with the principle of proportionality. • Chapter 2, Section 4 of the EIO Act states that an investigation order may be issued only if, taking into account the detriment for the individual and the time and costs that may be incurred, it appears necessary and proportionate to the nature and severity of the crime, and other circumstances. • Accordingly, in Chapter 2, Section 3 and 4 of the EIO Act, the conditions for issuing an investigation order are stated. However, with regard to the transfer of detainees there is no such investigation measure in Swedish law. Chapter 2, Section 12 of the EIO Act therefore states the special conditions for issuing an investigation order for this purpose. • Under the *LIRB Act*, Sweden can as a main rule provide assistance even if Sweden does not have an agreement on legal assistance in criminal matters with the other state, i.e. no demand for reciprocity (mutual assistance) is made. However, a number of countries require an agreement to be able to collaborate with Sweden.[112] • Chapter 4 Section 1 of the EIO Act states that there are only a few actions in an investigation order that may be appealed. From Article 14 of the EIO Directive follows *inter alia* that the remedies available under national law can be applied to investigative measures specified in the investigation order. The substantive reasons for issuing an investigation order may only be considered in proceedings brought in the issuing State. The issuing authority and executive authority are obliged to notify each other of the remedies used against the issue, recognition or enforcement of an investigation order. The deadlines should be the same as in domestic cases and they should be applied so that stakeholders are guaranteed an actual opportunity to use remedies available. • An investigation measure referred to in a Swedish investigation order may not be appealed otherwise than stipulated in the Act (see Chapter 4, Section 1 of the EIO Act). • A declaration of enforceability must neither be appealed otherwise than specified in the Act (see Chapter 4, Section 2 of the Act). A measure in a Swedish declaration of enforceability can only be appealed or tried by a court in the following cases: Examination of execution of seizures in accordance with Chapter 3, Section 32 of the EIO Act; Blocking and access bans, etc. in accordance with Chapter 27, Section 15 Code of Judicial

[112] Issues relating to judicial cooperation in criminal matters are also included in some multilateral conventions or bilateral agreements to which Sweden has acceded.

		Procedure, see **Chapter 3, Section 33 of the EIO Act**; All cases when investigative action, such as in a Swedish preliminary investigation or criminal trial, can only be taken after the court's trial; Interim measures shall be notified and tested by the court and may therefore be appealed, **cf. Chapter 4, Section 2 of the EIO Act**, which refers to **Chapter 3. Section 9 of the EIO Act**, which in turn is supplemented by **Chapter 3, Section 10 of the EIO Act**.
Case law	As from the beginning of 2018, there is a new case type for EIOs available. By 7 November 2018, there were in total eight cases received by the District Courts so far in 2018, and of those, four had been disposed of.[113]	

[113] Statistics collected by the Swedish National Courts Administration: Two cases concerning EIO from Gothenburg District Court, one case from Norrtälje District Court, and one case from Skarborg District Court, (B 3189-18 presentation of evidence in Court).

Annex IV - Methodological note

The Centre for European Policy Studies (CEPS) is an independent policy research institute based in Brussels. Its mission is to produce sound analytical research leading to constructive solutions to challenges facing Europe today.

The JUD-IT Handbook is based on the research findings generated throughout the JUD-IT Project (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, which received financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The information included in the Handbook was collected through legal research, primary and secondary data collection including semi-structured interviews with national and EU criminal justice policy makers, law enforcement officials and judicial practitioners, defence lawyers and civil society actors working on issues related to cross-border evidence gathering in criminal matters.

Expert discussions held during the three meetings of the JUD-IT Task Force also served to foster exchange of views and complement the evidence basis used to develop the Handbook. The JUD-IT Task Force ran between October 2018 and February 2019. It provided a forum for closed-door expert discussions encompassing three separate meetings held at the CEPS premises in Brussels. The Task Force made it possible to foster multidisciplinary debate on the challenges faced by judicial actors, law enforcement authorities, defence lawyers, and providers of internet and telecommunication services dealing with cross-border requests for data sought for criminal justice purposes. Civil society actors, legal scholars and experts in criminal and data protection law were also actively involved in the Task Force debate.

The Handbook also incorporates the main outcomes of the JUD-IT Practitioners Workshop organised in Brussels in the month of July 2017 by Fair Trials Europe. Results of the comparative research performed by the JUD-IT Academic Partners[114] in 13 different EU member states[115] has furthermore been leveraged to foster a better understanding of the roles of key stakeholders involved in the criminal justice process, and of the challenges they face when dealing with cross-border requests for data in the context of criminal proceedings.

Ngo Chun Luk helped in the development of the Handbook, in particular by designing the infographics included in section I. The author would like to thank the rapporteurs and the experts and officials who kindly agreed to be interviewed in the context of this research. A special mention and acknowledgement should go to the valuable inputs and comments provided by the following experts: Fabrizia Bemer, at the Prosecutor's Office of Court of Florence, and Laure Baudrihaye-Gérard, Senior Lawyer at Fair Trials Europe.

[114] Aristoteles University of Thessaloniki, Centre for European Policy Studies, Central European University, European University Institute, University of Luxembourg, Maastricht University, Uppsala University, Vrije Universiteit Brussel.

[115] AT, BE, BU, DE, EI, EL, ES, FR, HU, IT, LU, NL, SW.

ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy, Resources and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)