Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D2.1 Initial Legislative compliance relating to law-enforcement powers and evidence requirements

Document Summary Information

Grant Agreement No	833276	**Acronym**	INSPECTr
Full Title	**Intelligence Network & Secure Platform for Evidence Correlation and Transfer**		
Start Date	01/09/2019	**Duration**	42 months
Project URL	https://inspectr-project.eu		
Deliverable	2.1		
Work Package	2		
Contractual due date	M21 31/05/2021	**Actual submission date**	
Nature	Report	**Dissemination Level**	PU
Lead Beneficiary	RUG		
Responsible Author	Melania Tudorica, Jeanne Mifsud Bonnici		
Contributions from	Melania Tudorica, Jeanne Mifsud Bonnici, Anna Marquez Daly,Joe Cannataci		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v1.0		90	Initial Deliverable Structure	Melania Tudorica
			Reviewed by	Anna Marquez Daly
			Reviewed by	Jeanne Mifsud Bonnici
			Reviewed by	Joshua Hughes
V2.0		99	Final Deliverable Structure	Melania Tudorica
			Reviewed by	Anna Marquez Daly
			Reviewed by	Jeanne Mifsud Bonnici
V3.0		100	Final version for submission	Melania Tudorica
V.3.1		100	Reviewed by	Joe Cannataci

Disclaimer

Copyright message

Table of Contents

Glossary of terms and abbreviations used

Abbreviation / Term	Description
ACPO	Association of Chief Police Officers
AFIS	Automated Fingerprint Identification System
CDPC	The European Committee on Crime Problems
Charter	Charter of Fundamentals Rights
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
CSIRTs	Common Security Incident Response Teams
Cybercrime Convention	The Council of Europe Convention on Cybercrime
DoA	Description of Action
EAW	European Arrest Warrant
ECHR	European Convention of Human Rights
EECC	EU Electronic Communications Code
eEDES	e-Evidence Digital Exchange System
EEG	Electronic Evidence Guide
EIO	European Investigation Order
EJN	European Judicial Network
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
Interpol	International Criminal Police Organisation
JITs	Joint Investigation Teams
LEA Directive	LEA Data Protection Directive
LEAs	Law Enforcement Agencies
LL	Living Labs
MLA	Mutual Legal Assistance
NCMEC	National Center for Missing and Exploited Children
NI-ICS	Number-Independent Interpersonal Communications Services
NIS Directive	The Directive on Security of Network and Information Systems

OLAF	European Anti-Fraud Office
PC-CY	Committee of Experts on Crime in Cyberspace
SERE	Standardization of Evidence Representation and Exchange
SIAs	Security Intelligence Agencies
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
USA	United States of America
WP	Work Package

List of legislation and documents

Full name and link to full text
Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099
Charter of Fundamental Rights of the European Union [2000] OJ C 364/01
Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security* COM (2015) 185 final
Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47
Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/3
Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 005
Convention on Cybercrime [2001] ETS No. 185
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 [2000] OJ C 197/1
Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63
Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1
Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1

Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 2.1, Strasbourg, France, 6 March 2020
Council of Europe, "Explanatory report to the Convention of Cybercrime" (ETS No 185)
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002]
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218
Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L131/1
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31
ENISA, *Cooperation between CSIRTs and Law enforcement: interaction with the Judiciary* [2018]
ENISA, *Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders* [2014]
ENISA, Identification and handling of electronic evidence – Handbook, document for teachers [2013] September 2013
European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030
Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final
Proposal for a Regulation of the European Parliament and of the Council 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 Commu
Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da
The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their c

Executive summary

This document reports on the research conducted by WP2 on the INSPECTr Reference Framework for Standardization of Evidence Representation and Exchange. This reference framework to be implemented in the INSPECTr platform will facilitate standard solutions for forensic investigations across LEAs within the EU. The objective of this report is to provide an initial legislative compliance relating to law-enforcement powers and evidence requirements considering that LEAs are bound by law in their activities.

This Deliverable is devoted to understanding the legal requirements for law enforcement powers and evidence requirements, i.e. which legal instruments are applicable to investigations and to acquiring evidence, what powers (and restrictions) do law enforcement have to investigate in criminal procedures and share this with their colleagues across Europe, how do LEAs with each other and with other parties, which are the relevant data protection implications to be taken into account, etc. This is achieved by an analysis of the overarching European legislation and an analysis of the national legal frameworks of the countries where Living Labs (LLs) are taking place.

There is a lot of fragmentation in the legal framework as regards digital evidence. National, European and international laws and regulations, bilateral agreements and multilateral agreements all play a role in regulating the gathering, analysis and exchange of digital evidence. Criminal law is still very much based upon national laws and traditions, but also inspired by (implemented) international and European legal instruments. It is therefore not enough to look at the overarching international and European legal framework. National laws and traditions also need to be considered. Due to this fragmentation of applicable law, there is also fragmentation as regards actors involved and systems used for digital evidence. LEAs (national, local, regional), cybercrime units and specialised forces, CSIRTs, prosecution, the judiciary as well as private actors holding evidence and international and European organisations (Interpol, Europol, Eurojust, etc.) are all involved in one way or another in gathering, analysing and exchanging digital evidence and all use different legal frameworks and different systems to do so. In particular, when exchanging digital evidence across borders, it highly depends on the countries involved which legal instrument needs to be used for mutual assistance.

As regards the INSPECTr platform, two things need to be highlighted within the context of this legal analysis:

1. All countries have their own rules on access to databases, which includes access restrictions with strong authentication, determining who has access to which database and which files and with whom it may be shared under which circumstances. These rules include data protection consideration as reflected in the LEA Directive. Considering that the INSPECTr platform will be set up for investigative purposes, the platform needs to take into account these rules and restrictions to be able to guarantee a secure channel for inter-jurisdictional investigations;
2. Countries cooperate by way of MLA in cross-border criminal cases. This MLA and exchange of digital evidence can take place on the basis of various international and European legal instruments and bilateral and multilateral agreements depending on the countries involved. Currently, the leading legal instrument for this within the EU is the EIO, which will be digitised within the eEDES system operating on the e-CODEX platform. For countries who have opted out of the EIO Directive, such as Ireland, other instruments need to be relied upon for MLA requests. This includes the EU 2000 Convention and the Cybercrime Convention.

Although legal developments and systems of cooperation within the area have greatly improved over the years, in particular as regards speed and efficiency, the practical reality is that it can still be a time-consuming procedure. This is a challenge, in particular considering the volatile nature of digital evidence, which can be easily altered, moved or deleted. In spite of harmonisation, there are still differences in national enforcement legislation and approach. While there is increasingly more attention to setting common standards for gathering and exchange of digital evidence, some countries still apply traditional evidential rules to digital evidence and approaches vary.

Section 1 of this Deliverable sets the scene for this Deliverable and discusses the background and what will be discussed in this Deliverable (and what is omitted) and why.

In section 2, the relevant international and European legal framework as regards digital evidence is discussed. It provides an overview of the relevant legal instruments that are applicable to gathering, analysing and exchanging digital evidence. This processing of digital evidence needs to be done with regard for data protection. This is why section 3 discusses the relevant data protection legal framework.

Finally, section 4 aims to offer a picture of the laws and practices related to digital evidence in the countries where the LLs are taking place: Ireland, Estonia, France, Belgium, Latvia and Romania. This legal analysis of national laws is carried out on the basis of the answers provided in the questionnaires annexed to this deliverable.

1 Introduction

This document – "Initial legislative compliance relating to law-enforcement powers and evidence requirements" brings together the findings of work carried out in Task 2.1, Subtask 2.1.1 of Work Package 2 – INSPECTr Reference Framework for Standardization of Evidence Representation and Exchange (SERE) – as explained in the Description of Action (DoA) of the INSPECTr project (Grant agreement no 833276).

The main objective of Work Package (WP) 2 – INSPECTr Reference Framework – is to provide a reference framework to be implemented in the INSPECTr platform which will facilitate standard solutions for forensic investigations across Law Enforcement Agencies (LEAs) within the European Union (EU). Building such a framework cannot be done without regard for the law as LEAs are bound by law in their activities. As such, an important part of this reference framework is the analysis of the relevant legal status quo.

Task 2.1 is therefore devoted to understanding the legal requirements for law enforcement powers and evidence requirements, i.e. which legal instruments are applicable to forensic investigations and to acquiring evidence, what powers (and restrictions) do law enforcement have to investigate in criminal procedures and share this with their colleagues across Europe, how do LEAs interact and how do LEAs interact with other agencies such as Security Intelligence Agencies (SIAs), how do they interact with Common Security Incident Response Teams (CSIRTs) and third party data owners, which are the relevant data protection implications to be taken into account, etc. This is achieved through a wide collection of relevant documentation and available information, including by way of a questionnaire in order to identify the existing national legal frameworks.

Subtask 2.1.1 and the resulting deliverable (D)2.1 (this document) deals primarily with the status quo analysis and is aimed at providing a comparative overview of legislation and practises in EU Member States. This was done in two steps:

1. Analysis of relevant overarching European legislation;
2. Analysis of national legal frameworks of the countries where Living Labs (LL) are taking place within the framework of the INSPECTr project.

This analysis was carried out by conducting a desktop research of various studies, legal instruments, policy documents, literature, etc. and by asking the LEAs partners within the INSPECTr project to answer the questionnaire[1] developed to understand their national legal frameworks. The results of this deliverable will feed into the reference framework of WP2 and, more specifically, into task 3.4.1.a and the EU legislation management tool which will consist of a database containing the relevant legislation and practices.

Following the work done in this deliverable, the legal developments within this field will be closely monitored throughout the lifetime of the INSPECTr project. As such, the legal status quo will be monitored and updated continuously, including monitoring of developments regarding the European Commissions' proposal for a European production and preservation order for electronic evidence in criminal matters[2] and ongoing negotiations regarding the United States (US) Cloud Act. This will result in a final legislative compliance document at the end of the INSPECTr project (D2.2).

1.1 Mapping INSPECTr Outputs

The purpose of this section is to map INSPECTr Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

[1] Appendix 1 Questionnaire for the collection of information WP2 – INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange – Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements.

[2] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final.

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions

INSPECTr GA Component Title	INSPECTr GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D2.1 Initial Legislative compliance relating to law-enforcement powers and evidence requirements	*Initial Legislative compliance relating to law-enforcement powers and evidence requirements. Consolidated survey of EU laws on evidence deriving from digital data and legal requirements concerning privacy and data protection highlighting legal influence factors and constraints. Initial Version Including Legislation Frameworks for LEAs and CSIRTs. Review of Regulatory developments in EU and USA. Legal issues of LLs.*	*All components addressed throughout this Deliverable where relevant. Legal issues of LLs have not been reported.*	*Legal analysis of relevant legislation addressed from a national and European perspective. Legal analysis of national laws is based on the answers provided by the LEAs partner in the INSPECTr project.*
TASKS			
T2.1 Understanding, assessing and meeting legislative compliance relating to law-enforcement powers and evidence requirements. ST2.1.1 Survey of EU laws of digital evidence and legal requirements concerning privacy and data	*Legislation framework for LEA and Agencies interactions. Review of per Living Lab laws at national level affecting interaction between LEA and Security Intelligence Agencies. Align results to the EU related frameworks.* *a. Legislation framework for CSIRTs and third-party data owner's interactions. Survey on legal considerations affecting data exchange with CSIRTs and other third-party data owners.*	*All components addressed throughout this Deliverable where relevant.*	*Legal analysis of relevant legislation addressed from a national and European perspective. Legal analysis of national laws is based on the answers provided by the LEAs partner in the INSPECTr project.*

protection. Consolidated survey of EU laws on evidence on digital data and legal requirements concerning privacy and data protection (reference and EVIDENCE/e-CODEX) highlighting legal influence factors and constraints that need to be considered.	*b. Field survey on legal considerations affecting data management and information exchange of authorities like LEA with network operators and identification of practices affecting 'unregulated' cyber investigation such as for example "observation on the internet, "infiltration on social media", rules for digital search and seizure.*		

1.2 Scope

With most of our lives organised online and by using the latest technologies we rely on information and communications technology and use it in our daily lives to interact with our friends, families, colleagues, even with the government, we use it to share and store information, conduct our business, etc. The systems keep our economies running. As a consequence, we leave digital traces everywhere. The amount of data is massive and some of this data can potentially help law enforcement to predict, detect and manage crimes. Therefore, the INSPECTr project aims to develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to facilitate this process by using forensic tools. The platform will allow an investigator to visualise and bookmark important evidential material, and export it to an investigative report by using various knowledge discovery techniques. This will allow for cross-correlation analysis with existing case data and improve knowledge discovery within a case, between separate cases and between inter-jurisdictional investigations. The gathering, analysis, prioritisation and sharing of data across jurisdictions for criminal investigations is regulated by law. The platform therefore, needs to be in line with relevant legislation, including fundamental rights.

Due to the very nature of data, modern technologies and growing globalisation, digital evidential material may be located or stored anywhere in the world. Because of this increased cross-border dimension due to technology and globalisation, sharing information and evidence across borders has become extremely relevant. To be able to do this, countries cooperate by way of Mutual Legal Assistance (MLA). MLA allows authorities in one country to request evidence from other countries. This helps the requesting country in criminal investigations or proceedings where there is a cross-border dimension. This cross-border nature of crime is especially the case in cybercrime cases, as cybercrime is a global problem that does not stop at our countries' borders, but also increasingly in crimes in general, such as data that is stored online, in cloud storage, for example.

In investigating criminal matters, enforcement authorities need a variety of powers to gather, preserve and exchange evidence. Cyber-specific powers, include for example search and seizure of stored computer data, real-time collection of traffic data and interception of content data, as evidence may come in the form of computer files, logs, transmissions, metadata, computer data, etc. There is a large variety of free and commercial digital

forensic tools available. The INSPECTr platform intends to reduce complexity by offering one platform with extended options for multi-level and cross-border collaboration, for reactive and preventative policing which, in turn, will facilitate the detection and prediction of cybercrime operations as well as crime trends.

1.3 Setting the scene

Task 2.1.1 focuses on law and practices in the EU Member States as regards digital evidence, including privacy and data protection considerations. In understanding this legal framework, it is first important to understand who the actors involved in this field are. On a national level the actors involved in gathering digital evidence include LEAs, such as police forces on local, regional and national level, cybercrime units and specialised forces, CSIRTs, prosecution and the judiciary. With technological developments and globalisation causing an increase in cross-border cases, various legal instruments are used for cross-border mutual assistance. As it can be a complicated affair to reach out to foreign authorities, several legal instruments require Member States to set up national contact points, such as the Cybercrime Convention's 24/7 Network. These national contact points vary per country and can be, for example, seated within the Ministry of Foreign Affairs. Judicial and police cooperation often takes place via these national contact points and via international and European agencies and bodies who assist Member States in preventing, detecting, investigating and prosecuting cross-border crimes. These agencies and bodies, including Interpol[3], Europol[4], Eurojust[5], and ENISA[6], assist in international cooperation, gathering and exchange of digital evidence and have their own regulations for these processes. Apart from informal requests between LEAs, digital evidence is often shared via the secure channels of these agencies and bodies, such as Europol's Secure Information Exchange Network Application (SIENA), the Camden Asset Recovery Inter-agency Network (CARIN) for more informal requests, the Schengen Information System (SIS) and via the e-CODEX platform which will operate the e-Evidence Digital Exchange System (eEDES) for European Investigation Orders (EIOs) and the INSPECTr platform which will be used for ongoing investigations. SIS and eEDES will be explained in more detail in sections 2.1.1 and 2.1.3.

Secondly, in understanding the legal framework as regards digital evidence, it is important to be aware of the fact that there is a lot of fragmentation in this area of law. National, European and international laws and regulations, bilateral agreements, multilateral agreements – they all play a role in regulating the collection, analysis and prioritisation and (cross-border) exchange of digital evidence. This makes writing about this area of law – and making sure that the INSPECTr platform takes into account all the relevant legislation – a complex endeavour. Even more so as the law is not generally black and white, but has a lot of grey areas which are open for interpretation. In describing the legal framework as regards digital evidence relevant for the INSPECTr project, there is not simply one legal framework which needs to be taken into account – all countries and all levels need to be considered. Not having a comprehensive international or European legal framework relating to (digital) evidence means that parties involved rely mostly on national laws and traditions when it comes to the collection, analysis and prioritisation of digital evidence. The added complexity is that national laws and traditions are never exactly the same. According to the United Nations (UN) Study on Cybercrime, evidence rules vary considerably

[3] World's largest international police organisation under international law, global coordinating body, aiding in mutual assistance, also provides targeted training, expert investigative support, relevant data and secure communications channels and facilitates international police cooperation.

[4] The European Police Office (Europol) assists Member States in their fight against serious international crime and terrorism. It also includes the Europol European cybercrime centre (EC3) specialised in cybercrimes.

[5] Eurojust assists Member States when dealing with cross border criminal matters by stimulating and improving cooperation and coordination of investigations and prosecutions between Member States, for example by facilitating the execution of international MLAs and extradition requests.

[6] The European Network and Information Security Agency (ENISA) is the EU's centre of expertise for the purpose of ensuring a high and effective level of network and information security within the EU which assists the EU and the Member States and cooperates with the private sector.

even amongst countries with similar legal traditions.[7] Furthermore, these national criminal laws and traditions have existed for a long time, long before technologies came into existence which could produce electronic data and be used as digital evidence in criminal procedures. While legislation has evolved over time and some countries have adapted their laws to include technological developments, this may not always be the case. Some countries may still rely on traditional laws and apply them to digital evidence as well. For example, search and seizure has long been one of the instruments to acquire evidence. However, search and seizure in the physical world regulated by traditional laws requires a different approach from search and seizure in the digital world. The legal provision providing LEAs with the power to search and seize may however be used for both traditional and digital search and seizure. This is only one example of how national laws and regulations can vary. Not only are there differences in legislation and approach, things such as language barriers and cultural differences also challenge cross-border cooperation and exchange of digital evidence. To understand these differences in national legislation and approach and as such be able to integrate this into the INSPECTr platform, this Deliverable analyses the national laws of the countries where LL are taking place by looking at the answers provided by the LEA partners in the INSPECTr project as annexed to this Deliverable. It should be noted that if INSPECTr will be operational, all national legal frameworks of participating countries will need to be taken into account.

While there are differences among countries, there are also similarities. What all countries have in common for example is that legislation requires a clear scope of application of powers and sufficient legal authority for action.[8] LEAs and SIAs need certain powers to be able to investigate. What countries may also have in common is that they can be party to international and European treaties, conventions, regulations, etc. which will provide them with a common basis upon which to act. These instruments and documents may inspire national laws and practices or may even be implemented into national law. As such, there are a number of international and European legal instruments relating to digital evidence. As the INSPECTr project focusses mainly on a European solution and the countries involved in a LL are all EU Member States, this deliverable focuses mainly on EU and Council of Europe legal instruments applicable to digital evidence. These instruments will be discussed in section 2 of this deliverable. Bilateral and multilateral agreements will only be discussed insofar as the countries who are taking part in a LL explicitly mentioned these agreements in their answers to the questionnaire.[9] Section 3 will discuss legal requirements concerning privacy and data protection and section 4 will discuss the national legal frameworks of the countries where a LL is taking place.

[7] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 158.
[8] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 122, 123.
[9] Appendix 2 Questionnaires with answers from partners.

2 European legal framework on digital evidence

In this section, the relevant overarching European legal framework concerning digital evidence will be discussed. This overarching legal framework not only consists of EU legislation, but also of the legal framework of the Council of Europe.

As regards the EU legal framework, it is important to note that the EU cannot adopt general EU criminal law. However, with the entry into force of the Lisbon Treaty[10] and the creation of an Area of Freedom, Security and Justice, back in 2009, the EU can add important value to existing national criminal laws within the limits of its competence. This means that there are a number of EU legal instruments which may be directly or indirectly relevant to digital evidence. This Area of Freedom, Security and Justice introduced a supranational regime for EU criminal law in Title V of the Treaty on the Functioning of the European Union[11] (TFEU). The aim of this Area of Freedom, Security and Justice is to ensure a high level of security through measures to prevent and combat crime, through police and judicial coordination and cooperation, through mutual recognition of judgements in criminal matters and if necessary through harmonisation of criminal laws.[12] Criminal law and police cooperation is further elaborated upon in Chapters 4 (judicial cooperation in criminal matters) and 5 (police cooperation) of Title V TFEU. While this is certainly progress, nuance needs to be made as regards the practical realities, considering that judicial and police cooperation are on stringent terms with sovereignty regarding national security as national security is the sole responsibility of each Member State.[13] This means that some subjects can be difficult to agree upon at EU level. Apart from this difficulty there are certain Member States who have made reservations on the rules regarding the Area of Freedom, Security and Justice. Ireland, for example, can opt out of any of the instruments and Denmark is only bound by virtue of its commitments under the Schengen Convention.[14] With this critical note, police and justice bodies across Europe do tend to work together in preventing and solving cross-border crimes. One of the ways to achieve this kind of cooperation is through harmonisation of laws, in particular when it comes to a number of serious crimes, such as terrorism, organised crime and cybercrime, but also as regards the admissibility of evidence between Member States.[15] The latter is based upon the principle of mutual recognition of for example judgements and judicial decisions, meaning that evidence collected lawfully in one Member State should be recognised by and admissible in another Member State.[16] Harmonisation is achieved by adopting Directives and other measures to the extent necessary to facilitate judicial and police cooperation within the EU. As such, the EU has adopted a number of Directives and other measures with regard to criminal law. The measures relevant to digital evidence will be discussed in this section below.

When describing the European legal framework as regards digital evidence, the Council of Europe legal instruments cannot be taken out of the equation. The Council of Europe instruments and documents are very important considering the number of Members, which includes all Member States of the EU. In particular with regard to cybercrime the Council of Europe provided a binding international treaty that provides an effective framework for the adoption of national legislation and a basis for international cooperation in this field.[17] The

[10] Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/01.

[11] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

[12] Article 67 (3) TFEU.

[13] See Article 4 (2) of the Treaty on the European Union (TEU): Consolidated version of the Treaty on European Union [2012] OJ C 326/13.

[14] Chalmers, D., Davies, G., Monti, G., *European Union Law*, Cambridge: University Press, 2010, p. 582.

[15] See Article 83 (1) TFEU.

[16] See Article 82 (1) TFEU.

[17] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 9, 15; See also Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218, Recital 15.

importance of the Council of Europe legal framework is emphasised and reiterated by several EU legislation and policy documents, which mention that the Council of Europe's instruments are the legal framework of reference for combating cybercrime and that the EU legislation and policies build on those of the Council of Europe. The Council of Europe Convention on Cybercrime[18] (Cybercrime Convention) remains the main (and only) international treaty which defines the procedural provisions for investigating and pursuing cybercrime. Considering that the treatment of digital evidence is the same regardless of whether a cybercrime or a traditional crime took place, the Cybercrime Convention applies when collecting, analysing and exchanging digital evidence. Apart from the Cybercrime Convention, the Council of Europe Convention on Mutual Assistance in Criminal Matters[19], and its 1978 Protocol[20] is also relevant within the context of digital evidence.[21]

This section will first discuss the relevant EU legal instruments, followed by the Council of Europe legal instruments.

2.1 European Union

Section 2.1 discusses the EU legal instruments which may be directly or indirectly relevant to digital evidence.

2.1.1 EIO Directive

Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN
Status	In force
Focusses on	Cross-border investigation
Relevance	Cross-border gathering and transmission of evidence
Additional comments	Does not apply in Ireland and Denmark[22]

In order to address the fragmentation in the legal framework as regards evidence, the EU adopted the European Investigation Order (EIO) Directive,[23] which was introduced in May 2017, to replace the existing instruments in this area.[24] The EIO Directive sets up a comprehensive system that allows EU Member States to obtain evidence in criminal cases at all stages of criminal proceedings in other Member States and aims to simplify and speed up cross border criminal investigations in the EU. The purpose of an EIO is to have one or several specific

[18] Convention on Cybercrime [2001] ETS No. 185.
[19] European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030.
[20] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099.
[21] Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 1.0, Strasbourg, France, 18 March 2013.
[22] See Recitals 43 – 45 EIO Directive.
[23] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L131/1.
[24] A number of (corresponding provisions of) other legal instruments were replaced by the EIO Directive, this includes the European Convention on Mutual Assistance in Criminal Matters (including Protocols and bilateral agreements); the Convention implementing the Schengen Agreement; the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol; and the European Evidence Warrant Framework Decision. See Article 34 of the EIO Directive.

investigative measures carried out in another Member State and thus enables judicial authorities in one Member State (the issuing state) to request that evidence be gathered in and transferred from another Member State (the executing state) based upon the principle of mutual recognition of decisions taken to obtain evidence. In principle, the EIO applies to all investigative measures aimed at gathering evidence, except when it comes to gathering evidence in Joint Investigation Teams (JITs).

The EIO improves on existing EU laws covering this field by ensuring quick, effective and consistent cooperation between Member States. These objectives are ensured through the establishment of setting strict deadlines for gathering the evidence requested and by limiting the grounds for refusing such requests. This is necessary to ensure that the issuing Member State can meet its procedural deadlines. The EIO also reduces paperwork by introducing a single standard form for authorities to request help when seeking evidence. While the Directive aims at introducing a single regime for gathering evidence, additional rules and practical arrangements between Member States may be necessary for certain types of investigative measures considering the differences in national laws. If this is the case, this should be mentioned in the EIO. Furthermore, the EIO Directive is replacing, but not repealing traditional MLA mechanisms. For example, the European Arrest Warrant[25] (EAW) remains in effect and still needs to be used in certain cases, for example if a person needs to be transferred to another Member State for the purpose of prosecution within the context of an EIO. Another example is that, while the EIO is focussed on gathering evidence, sometimes confiscation needs to take place. For this it is still relevant to rely on traditional MLA mechanisms. According to Espina, traditional MLA mechanisms are still in effect, among other things, since the EIO Directive cannot repeal MLA Conventions due to the formal rules of withdrawal, and because of the fact that the EIO Directive is not binding on all Member States; considering, for example, the reservations made by Ireland and Denmark.[26] Nevertheless, the EIO Directive is currently the leading legal instrument when it comes to the cross-border investigative measures within criminal proceedings aimed at gathering evidence among Member States bound by the EIO and those Member States should give precedence to the EIO over other MLA mechanisms.[27]

As regards fundamental rights and freedoms, the EIO emphasises that, when executing an EIO, the investigative measure chosen needs to be necessary, proportionate, and have as little interference with fundamental rights as possible. It even goes as far as allowing refusal of an EIO if fundamental rights are breached. The Directive refers to the EU Charter of Fundamental Rights and international human rights instruments, such as the European Convention for the protection of human rights and fundamental freedoms.[28] The Directive also refers to certain fundamental rights from a criminal law perspective in particular, such as the presumption of innocence, right of defence[29] and the '*ne bis in idem*' principle.[30] Apart from this, privacy and data protection are also of great importance when gathering evidence, in particular because the EIO allows for cooperation as regards interception of telecommunications, including traffic and location data.[31] Within the context of the EIO, data processing needs to be necessary and proportionate for the purpose of preventing, investigating, detecting and prosecuting crimes. Member States also need to be transparent as regards processing of personal data and data subjects' rights. Privacy and data protection will be discussed in more detail in section 3 of this report.

The Directive is divided into 7 chapters: the EIO, procedures and safeguards for the issuing state, procedures and safeguards for the executing state, specific provisions for certain investigative measures, interception of telecommunications, provisional measures and final provisions. The first chapter is dedicated to understanding

[25] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1. See paragraph 2.1.4 below for more details.
[26] J.A. Espina Ramos, *The European Investigation order and its relationship with other judicial cooperation instruments*, EUCrim 1/2019, p. 53.
[27] See Recital 35 EIO Directive.
[28] See Recital 12 EIO Directive.
[29] Ibid.
[30] The 'ne bis in idem' principle determines that a person cannot be prosecuted for the same offense twice. See Recital 17 EIO Directive.
[31] See EIO Chapter V

what an EIO is and what its obligations are. It defines who the actors involved are (the issuing state or authority and the executing state or authority),[32] sets the scope of the EIO (investigative measures and gathering evidence),[33] determines the types of criminal proceedings for which an EIO can be used and the content and form of the EIO.[34] As regards the content and form of the EIO, Article 5 determines that the EIO needs to be requested by completing Annex A to the Directive. This standard form includes information about the issuing authority, the object and reasons for the EIO, the necessary information available on the person(s) concerned, a description of the criminal act and of the investigative measures and evidence to be obtained. The European Commission (the Commission) is currently working on the e-Evidence Digital Exchange System (eEDES[35]), a secure online portal for electronic requests and responses for obtaining digital evidence. The standard EIO form is to be integrated within this platform. The developments of the Commission's initiative will be followed throughout the course of the INSPECTr project and reported in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

The second and third chapter of the EIO Directive determine the procedures and safeguards for the issuing state and the executing state. It determines that the EIO needs to be necessary and proportionate, and that the requested investigative measures would have been ordered under the same conditions as in a similar national case.[36] The executing authority is then obliged to recognise the EIO without further delay, and execute within the time limits in Article 12, unless one of the grounds mentioned in Article 11 applies.[37] The executing Member States responds to the request by acknowledging its reception and by completing Annex B to the Directive. Considering the differences in national criminal laws, as mentioned before, an EIO may request for an investigative measure that does not exist under the law of the executing Member State. If that is the case, Article 10 determines that the executing authority has recourse to another similar investigative measure. According to Articles 7 and 13, the EIO, and the resulting evidence, can be transferred by any relevant means of transmissions for the exchange of evidence. Some examples of these means of transmission include the secure telecommunications system of the European Judicial Network, Eurojust, or other channels used by judicial authorities or LEAs.

Chapter 4 of the EIO Directive provides for specific provisions for certain investigative measures:

- Temporary transfer for persons held in custody (Articles 22 and 23): allowing for the temporary transfer of a person in custody to another Member State if the presence of this person on the territory of that state is necessary for gathering evidence;
- Hearing by telephone conference, videoconference or other audio-visual transmission (Articles 24 and 25): allowing for an EIO to be issued in order to hear a witness or an expert by telephone or video conference or other audio-visual means;
- Information on bank and other financial accounts (Articles 26 and 27): in order to determine whether the natural or legal person subject to criminal proceedings controls one or more accounts in the executing state and obtain details of these accounts;
- Real-time evidence gathering: allowing for gathering evidence in real-time, continuously and over a certain period of time, such as monitoring banking operations;
- Covert investigations: where the issuing state requests the assistance of the executing state in covert investigations, i.e. officers acting under covert or false identity for the purpose of investigations into crimes.

[32] Article 2 EIO Directive.
[33] Article 3 EIO Directive.
[34] Article 4 EIO Directive.
[35] See for more information on eEDES: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>.
[36] Article 6 EIO Directive.
[37] See Article 9(1) EIO Directive

As regards the interception of telecommunications, chapter 5 of the EIO Directive determines that an EIO may be issued if technical assistance is needed from another Member State (Article 30). If there is no technical assistance needed for the interception on the territory of another Member State, Article 31 determines that this Member State needs to be notified of the interception.

The procedure in the EIO Directive seems pretty clear and straight forward. However, in reality, there are certain practical difficulties. These difficulties include among others differences in culture and language, making it sometimes difficult to cooperate among Member States. The TREIO project is aimed at setting up training within the context of the EIO coupled to the upcoming eEDES system. The TREIO project[38] will be followed throughout the course of the INSPECTr project and reported in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

2.1.2 EU 2000 Convention

Type of instrument	Convention
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0712(01)&from=EN
Status	In force
Focusses on	Mutual assistance in criminal matters
Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive

The Convention on mutual assistance in criminal matters[39] (EU 2000 Convention) was adopted by the Council[40] in 2000 in accordance with Article 34 of the Treaty on European Union (TEU) in order to improve judicial cooperation in criminal matters. The EU 2000 Convention was based on the principles of and designed to supplement the European Convention on Mutual Assistance in Criminal Matters and its additional Protocol,[41] which will be discussed in paragraph 2.2.1 below.

Based on this Convention Member States may request each other for mutual assistance in criminal matters and criminal proceedings.[42] Within the context of this Convention, a requesting Member State may request for mutual assistance to a requested Member State, which needs to comply with the formalities and procedures indicated by the requesting Member State. Requests for mutual assistance are made in writing, transmitted and executed directly between judicial authorities with territorial competence or via the central authorities of

[38] <https://treio.eu>.
[39] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/3.
[40] 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 [2000] OJ C 197/1.
[41] Article 1 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01) [2000] OJ C 197/3.
[42] Article 3 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01) [2000] OJ C 197/3

Member States or – in case of emergency – via Interpol, Eurojust or Europol.[43] The requested Member State then needs to execute the request for assistance as soon as possible.

The EU 2000 Convention provides for a number of specific forms of mutual assistance in Title 2 of the Convention. These include restitution to the rightful owner, temporary transfer of persons held in custody for purpose of investigation, hearing by videoconference, hearing of witnesses and experts by telephone conference, controlled deliveries, joint investigation teams, covert investigations, criminal liability regarding officials and civil liability regarding officials (Articles 8 – 16). Furthermore, it provides for mutual assistance in the interception of telecommunications in title 3 of the Convention (Articles 17 – 22). The EU 2000 Convention is a more traditional form of MLA which can also be used to obtain digital evidence. The downside of such procedures for mutual assistance is however, that they often take a long time, which can be problematic considering the volatile nature of digital evidence.

As of the entry into force of the EIO Directive, the EIO Directive takes precedence over the EU 2000 Convention and the corresponding provisions of EU 2000 Convention were replaced by the EIO Directive for the Member States bound by the EIO Directive. This means that countries who are bound by the EIO Directive need to request for judicial cooperation via the EIO system and that for those countries the corresponding provisions of the EIO Directive apply. For example, if the Netherlands wishes to obtain evidence from Germany via the interception of telecommunication, the Netherlands needs to issue an EIO and can no longer use the EU 2000 Convention. The EU 2000 Convention does however remain in force for those countries to whom the EIO Directive does not apply, such as Ireland and Denmark.

2.1.3 Schengen implementing Convention

Type of instrument	Convention
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN
Status	In force
Focusses on	External borders, police cooperation
Relevance	Police cooperation, secure Schengen Information System (SIS)
Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive[44]; Bulgaria, Romania, Croatia and Cyprus not yet part of the Schengen Area; Does not apply in Ireland; SIS operated by Bulgaria, Romania and Ireland

Starting as the Benelux Economic Union in 1948, Belgium, the Netherlands and Luxembourg had already abolished common border controls. Over time, this grew out into a bigger area without internal border controls. Nowadays, it is referred to as the Schengen Area consisting of 26 countries, including most of the EU Member States and some non-EU countries, such as Switzerland and Norway. The EU Member States that are not part of

[43] Articles 5 and 6 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01) [2000] OJ C 197/3.
[44] Article 24 EIO Directive.

the Schengen area are Bulgaria, Romania, Croatia, Cyprus and Ireland. Bulgaria, Romania and Croatia are currently in the process of joining. Ireland opted out of the Convention implementing the Schengen agreement. By abolishing the internal borders, Schengen States made rules to ensure the security of those living or travelling in the Schengen Area, including tightened controls at their common external border and enhancing police and judicial cooperation.[45] This facilitates cross-border police cooperation, for example as regards missing persons, or criminal offences, and allows for faster judicial cooperation via the Schengen Information System (SIS), including a faster extradition system and exchange of evidence. The Schengen acquis is the body of law regulating the Schengen Area.[46] Title III of the Schengen Implementing Convention is devoted to police and security and includes general provisions on police cooperation, provisions on mutual assistance in criminal matters, application of the '*ne bis in idem*' principle, extradition, transfer of the enforcement of criminal judgements, narcotic drugs and firearms and ammunition. Within this context LEAs assist each other for the purpose of preventing and detecting criminal offences and can request for assistance. To facilitate this, the SIS was introduced to enable competent authorities to enter and consult alerts on certain categories of wanted or missing persons and objects. The large, secure and protected EU database, which also includes Automated Fingerprint Identification System (AFIS), is exclusively accessible to the authorised users within competent authorities, such as national border control, police, customs, judicial, visa and vehicle registration authorities. Europol and Eurojust also have limited access rights to carry out certain types of queries on specified alert categories. SIS allows the use of biometrics, new types of alerts and the possibility to link different alerts. Member States supply information to the system through national networks (N-SIS) connected to a central system (C-SIS). This IT system is supplemented by a network known as SIRENE (Supplementary Information Request at the National Entry), which is the human interface of the SIS. While they are not (yet) part of the Schengen Area, Bulgaria and Romania started using the SIS fully, Croatia still has some restrictions as regards the use of SIS, and Ireland does operate SIS, but cannot issue or access Schengen-wide alerts for refusing entry and stay in the Schengen Area.

As of the entry into force of the EIO Directive, the EIO Directive takes precedence over the Convention implementing the Schengen Agreement and the corresponding provisions of Convention implementing the Schengen Agreement were replaced by the EIO Directive for the Member States bound by the EIO Directive. This means that countries who are bound by the EIO Directive need to request for judicial cooperation via the EIO system and that for those countries the corresponding provisions of the EIO Directive apply. For example, if the Netherlands wishes to obtain evidence from Germany within the context of police cooperation, the Netherlands needs to issue an EIO and can no longer use the SIS for this. The Convention implementing the Schengen Agreement does however remain in force for those countries to whom the EIO Directive does not apply, including Denmark. Ireland opted out of the Schengen Area as well as the EIO Directive, meaning that for mutual assistance including Ireland, traditional MLA mechanisms remain in place and that the SIS can be used.

[46] The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L 239/19. See also: Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L 381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63; Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1.

2.1.4 European Arrest Warrant

Type of instrument	Decision
Link to full text	https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF
Status	In force
Focusses on	Extradition
Relevance	May be used in combination with EIO or mutual assistance requests and includes the handing over of evidence in connection with the extradition

In 1999, the European Council agreed that formal extradition procedures as regards persons who are fleeing from justice after having been sentenced and persons suspected of having committed an offence needed to be abolished. To give effect to this agreement, Council Framework Decision 2002/584/JHA on the European arrest warrant (EAW)[47] was adopted. The EAW is a judicial decision issued by a Member State with a view to the arrest and surrender by another Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order.[48] The Decision simplifies and speeds up procedures whereby EU citizens, who have committed a serious crime in another Member State can be returned to that country to face justice. Similar to the previously mentioned legal instruments, the EAW is executed based on the principle of mutual recognition, which is seen as the cornerstone of judicial cooperation[49] as it simplifies the system and removes potential delays. An EAW may be issued for acts that are punishable in the Member State issuing the EAW. Article 2 of the EAW Decision provides the scope of the EAW and lists a number of offences that give rise to surrender[50] pursuant the EAW, this includes for example participation in a criminal organisation, terrorism and sexual exploitation of children and child pornography.

The EAW is requested by a judicial authority to the judicial authority in the executing Member State where the person is being sought.[51] Based on Article 8 of the Decision, the EAW request must contain information on the identity of the person concerned, details regarding the issuing judicial authority, the final judgment, the nature and legal classification of the offence, facts of the case and the penalty. When the location of the requested person is known, the issuing judicial authority transmits the EAW directly to the executing judicial authority.[52] It may also decide to issue an alert for the requested person in the SIS as described above.[53] If the issuing judicial authority does not know the competent executing authority, it may make inquiries through the contact points of the European Judicial Network (EJN).[54] Transmission may also be effected via the secure system of the EJN or Interpol.[55] The EAW furthermore, provides that property which may be required as evidence may be seized, and

[47] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1.
[48] Article 1 (1) EAW Decision.
[49] See Recital 6 and Article 1 (2) EAW Decision.
[50] Surrender of the suspect by one police force to another foreign police force.
[51] See Article 1 (1) EAW Decision.
[52] Article 9 (1) EAW Decision.
[53] Article 9 (2) EAW Decision.
[54] Article 10 EAW Decision.
[55] Article 10 (3) EAW Decision.

handed over at the request of the issuing judicial authority or on the initiative of the executing judicial authority.[56]

The EAW Decision has been criticised enormously. In fact, it has prompted more challenges before constitutional Courts of the Member States than any other EU law. The most important concern in this regard is relates to trust in the prosecutorial, and judicial process of the issuing state mainly in that there might be insufficient guarantees that the surrendered person will receive a fair trial in the issuing state.[57]

2.1.5 Decision on exchange of information and intelligence

Type of instrument	Decision
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006F0960&from=EN
Status	In force
Focusses on	Exchange of information and intelligence
Additional comments	Replaces related provisions of the Schengen implementing Convention as regards exchange of information and intelligence for the purpose of criminal investigations

The Decision on exchange of information and intelligence[58] aims at simplifying rules based on which LEAs can effectively exchange information, intelligence in criminal investigations and criminal intelligence operations. This is of particular relevance considering the timely need to access accurate and up to date information as well as intelligence in order to detect, prevent and investigate crimes.[59] According to this Decision, police, customs and other authorities authorised by national law to detect, prevent and investigate crimes can request their counterparts in other Member States for information and intelligence. Information and intelligence within the meaning of this Decision is any type of information or data held by LEAs, public authorities or private entities which is available to LEAs. Based on this Decision, Member States need to ensure that the conditions for those requests are not stricter than requests on a national level.[60] This means that Competent authorities need to treat request for information or intelligence from another Member State the same as requests within the Member State. Additionally, they also need to respond within eight hours for urgent cases and within one week for non-urgent cases. Following Article 6 of the Decision, exchange can take place via any existing channels for international cooperation using the form annexed to the Decision.

[56] Article 29 EAW Decision
[57] Chalmers, D., Davies, G., Monti, G., *European Union Law*, Cambridge: University Press, 2010, p. 599.
[58] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89.
[59] Article 1 (1) and Recital 4 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89.
[60] See Article 3 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89.

2.1.6 Joint Investigation Teams

Type of instrument	Council Framework Decision
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0465&from=EN
Status	In force
Focusses on	Joint Investigation Teams
Additional comments	The EIO Directive does not apply to the gathering of evidence in JITs

A Joint Investigation Team (JIT) is a team made up of members of two or more Member States, set up for a specific purpose and a limited period of time.[61] These teams investigate criminal offences with cross-border elements which require coordinated and concerted action in the Member States involved.[62] The Decision was initially set up to combat drug and human trafficking and terrorism, but is nowadays also often used for cybercrimes. The Member States setting up the JIT decide on its composition, purpose and duration, and may also allow representatives of Europol and the European Anti-Fraud Office (OLAF) and representatives of third countries take part in the team's activities. Article 13 of the EU 2000 Convention provides for the setting-up of joint investigation teams. However, due to the slow ratification of the EU 2000 Convention, the Council adopted the Framework Decision on JITs, which the Member States were to implement by 1 January 2003.[63]

Operating in the territory of a Member State requires JITs to act in conformity with the applicable law of that Member State, meaning that investigative measures need to follow the rules and regulations of that country. Members of the JIT from Member States, other than the Member State in which the team operates, are referred to as being 'seconded' to the team.[64] These seconded members may be present when investigative measures are taking place, may be entrusted with the task of taking certain investigative measures and may request their own competent authorities to take measures under the same conditions as their national investigations.[65] If the assistance of another Member State, than those which have set up the team or from a third country (i.e., non-EU), is required a request for MLA can be made, using the applicable legal instruments.[66] Information lawfully obtained by the JIT may be used for the purpose for which the team was set up, for detection, investigation and prosecution of criminal offences, for preventing immediate and serious threat to public security and for other purposes if so agreed between the Member States that set up the JIT.[67] Increasingly, this is one of the most relevant instruments for EUROPOL to share its expertise in collection, preservation and facilitation of exchange of digital evidence, in particular in the context of cybercrimes.

[61] Article 1 Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.
[62] See Article 1 (1, b) Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.
[63] On the relevance of the Joint Investigation Teams a cross-border tool for operational cooperation see: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security* COM (2015) 185 final, p. 9, available at <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf>.
[64] Article 1 (4) Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.
[65] Article 1 (5, 6 and 7) Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.
[66] Article 1 (8) Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.
[67] Article 1 (10) Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1.

2.1.7 NIS Directive

Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
Status	In force
Focusses on	High level of security and information systems
Relevance	CSIRTs
Additional comments	Proposal for a revised NIS Directive presented on 16 December 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823

The Directive on Security of Network and Information Systems[68] (NIS Directive) provides legal measures for a high level of cybersecurity in the EU to respond to cybersecurity challenges.[69] Among other things, the Directive facilitates the exchange of information, cooperation and common security requirements for operators of essential services and digital service providers to cover all relevant incidents and risks.[70] The Directive ensures the preparedness of Member States as regards Network and Information Security (NIS) by obliging them to have a national NIS strategy,[71] and by having a competent national NIS authority and one or more Common Security Incident Response Teams (CSIRTs) to ensure security,[72] in particular for sectors that are vital for economy and society, such as energy, transport, health and banking.[73] These CSIRTs monitor incidents at national level, provide early warnings, respond to incidents, provide risk and incident analysis, participate in the EU-wide CSIRTs network and establish cooperation relationships with the private sector.[74] CSIRTs prevent and contain IT incidents, primarily from a technical point of view, they deal with incident management and incident handling. While they do not have the same powers as LEAs, they play an important role in supporting investigations and work closely with LEAs considering that incidents can be the result of criminal activities. CSIRTs can for example discover suspicious activity of which it can inform LEAs, but they can also play a role in the investigation by providing technical expertise, support the gathering and preservation of evidence and sharing the information they have or have access to. In case of a formal involvement of CSIRTs in criminal investigations, the prosecutor

[68] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[69] See recital 4 and 5 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[70] See Article 1 (2, b and d) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[71] See Article 7 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[72] See Article 9 (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[73] See Recitals 9 – 13 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[74] See Article 12 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

is often consulted who needs to give consent for the involvement of the CSIRT in gathering, handling and analysing evidence.[75]

On 16 December 2020, the European Commission presented the proposal for the new NIS2 Directive, which will replace the current NIS Directive. NIS2 is not likely to have major consequences on current CSIRTs practices. Developments for this proposal will be followed throughout the course of the INSPECTr project and reported in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

2.1.8 ENISA guidelines

Type of instrument	Best practices
Link to full text	https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-handbook/view https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders
Relevance	Guidelines for CSIRTs for gathering digital evidence

ENISA is the European Union's Agency for Network and Information Security (NIS), a centre of expertise at European level for the purpose of ensuring a high and effective level of NIS within the EU. Its mission is to achieve a high common level of cybersecurity across the EU in cooperation with the wider community, i.e. public as well as private sector. ENISA assists the EU and the Member States, and cooperates with the private sector in order to help them meet requirements of NIS, it provides guidance, advice and assistance within its objectives.[76]

As previously discussed, CSIRTs may have a supporting role in investigations. In order to guide CSIRTs on how to handle digital evidence, ENISA drafted several documents, including a handbook[77] and a guide[78], in order to bridge the gap between CSIRTs and LEAs. These documents provide guidance for CSIRTs on how to deal with evidence and evidence gathering. It describes what digital evidence is, what the different sources of evidence are, what the principles for evidence gathering are and what to do with the evidence.

The handbook is meant as an exercise and explains what is necessary for good digital evidence gathering in terms of both the volatile and changing nature of digital evidence, as well as legal obligations for the evidence to be ultimately admissible in court. According to this handbook, there are five internationally accepted practical principles that are considered a good basic guideline: data integrity, audit trail, specialist support, appropriate training and legality.[79] Data integrity and audit trail means that the data cannot be altered or lost and that all actions need to be recorded. This is an important aspect of digital evidence gathering considering that digital evidence can easily be changed, moved or even deleted. CSIRTs need to be aware of this and the person in charge

[75] See for more information on the roles of CSIRTs and LEAs and their cooperation: ENISA, *Cooperation between CSIRTs and Law enforcement: interaction with the Judiciary* [2018], available at <https://www.enisa.europa.eu/publications/csirts-le-cooperation>.
[76] Article 1 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.
[77] ENISA, *Identification and handling of electronic evidence – Handbook, document for teachers* [2013] September 2013, available at <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-handbook/view>.
[78] ENISA, *Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders* [2014], available at <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders>.
[79] ENISA, Identification and handling of electronic evidence – Handbook, document for teachers [2013].

is responsible for the integrity of the digital evidence. This also starts the chain of custody for which actions need to be recorded for the evidence to be eventually admissible in court. Specialist support and appropriate training refer to the expertise and training of the first responders, meaning that a specialist or external adviser may need to be notified by the person in charge, and that first responders should be trained to be able to search and seize digital evidence if no experts are available. Finally, legality means that law, forensic and procedural principles as well as the aforementioned principles are abided by. The person and agency in charge of the case are responsible for this and need to take into account the laws and regulations of their own country. Within this context, the handbook furthermore refers to the Cybercrime Convention, which will be discussed in the next paragraph, as an important legal document.

2.1.9 Proposed legislation

Type of instrument	International negotiations; Regulation and Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN
Status	Recommendation to open negotiations; Proposal, not in force
Focusses on	Facilitation of judicial cooperation with third countries; European Production and Preservation Order and harmonised rules for legal representatives for gathering evidence in criminal proceedings

According to the European Commission (the Commission), more than half of all criminal investigations today include a cross-border element due to the number of international e-mails and messaging via apps that are being transmitted nowadays.[80] To be able to use such messages as evidence in court, a request needs to be made to the country holding the digital evidence using the legal instruments described in this report. Taking this 'shift' to a more digital nature of evidence into account, the Commission proposed new rules with the aim to make the exchange of digital evidence easier and faster for police and judicial authorities. There are two paths followed by the Commission: international negotiations and internal rules.

International negotiations aim at improving cooperation with third (non-EU) countries, including with the United States of America (USA), as crimes do not stop at EU borders. As such, the Commission proposed two sets of negotiations. The first is an agreement between the EU and the USA on cross-border access to digital evidence for judicial cooperation in criminal matters[81] which aims at avoiding conflicting obligations for service providers between the EU and the USA. The second is an authorisation to participate in negotiations on a second Additional Protocol to the Cybercrime Convention[82] which aims at more effective MLA, including for example direct

[80] See: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>.

[81] Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final.

[82] Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final.

cooperation with service providers in other jurisdictions. These negotiations will be followed throughout the lifetime of the INSPECTr project and reported in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

For improving the internal rules to make cross-border evidence gathering within the EU easier and faster, the Commission proposed a Regulation[83] and a Directive[84] for the creation of a European Production and Preservation Orders for digital evidence in criminal matters as well as harmonised rules for legal representatives for gathering evidence in criminal proceedings. These new legal instruments will not replace the EIO Directive, but will provide an additional tool for authorities. A production order is an instruction from an issuing authority, such as LEAs, to a service provider, to deliver or make available certain information which is considered to be digital evidence. A preservation order requires the service provider to preserve the digital evidence in view of the subsequent request for production.[85] These tools are considered to be necessary due to the fact that network-based services can be provided from anywhere in the world. As a consequence, the digital evidence is often stored outside of the jurisdiction of the Member State investigating a crime. As such, the investigating authority needs to request the Member State where the service provider is based for mutual assistance. In view of the growing number of digital evidences, these requests through the official channels can take a long time. Combining this with the lack of a clear framework for cooperation with service providers makes it challenging for service providers to comply with LEA requests, in particular LEAs from another country. The new Regulation will allow LEAs to approach the service providers directly, without the involvement of a judicial authority in another Member State. The Directive will lay down harmonised rules, obliging service providers in the EU to designate at least one legal representative for the receipt of, compliance with and enforcement of production and preservation orders and any other orders issued in the context of gathering evidence in criminal proceedings. Having legal representatives means that LEAs will have a clear point of access to address service providers.

The proposals are currently at the stage of first reading by the European Parliament. The European Parliament has been working on this legislation and produced a draft report[86] on the subject with 267 amendments to the proposal, while the different political groups introduced a total of 841 amendments[87]. It is safe to say that this legislation still has a long way to go. Content and developments of this proposed legislation will be followed throughout the lifetime of the INSPECTr project and reported in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

2.1.10 CSAM

The EU legal instruments discussed above are legislation that is relevant to digital evidence and LEA powers when gathering and handling digital evidence in criminal proceedings. This sub-section focusses on one crime in particular: Child Sexual Abuse (CSA) online considering that the INSPECTr project is using CSA as a use case and the recent developments in this field on an EU level. While the legislation mentioned in this paragraph is not necessarily relevant to digital evidence and LEA powers as such, it is important to report on the developments in this field.

In our increasingly digital world, online Child Sexual Abuse Material (CSAM) continues to increase. The amount that has been created or that is in circulation online cannot be quantified in absolute terms, because new content is constantly being added and only a proportion of older content has been identified and taken down. LEAs, national authorities, safer internet hotlines or reporting mechanisms and service providers or industry all work

[83] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 final.
[84] 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, COM (2018) 226 final.
[85] See Article 2 of the Proposed Regulation.
[86] Available at <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#title3>.
[87] See <https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf>.

together in the fight against CSAM. Industry has been called upon to take down CSAM materials from their services. Over the last decade, industry has set up reporting mechanisms for materials to be taken down once notified and adopted more automated systems to detect and take down CSAM. Microsoft for example developed 'PhotoDNA', software that creates a unique digital signature of an image known (a hash) which can then be compared against the database of other hashes in order to identify illegal content. The main database of hashes of CSAM is held by the National Center for Missing and Exploited Children (NCMEC), a USA based non-profit organisation. PhotoDNA detects, disrupts and reports CSA and is freely available. Apart from images, Microsoft also developed a grooming detection technology, which scans chat conversations for potentially problematic conversations. Other service providers have also shown similar initiatives. While these technologies were not developed to assist LEAs per se, it is sometimes used to report a CSA case. These voluntary practices of detecting, reporting and removing CSAM have however come into a new light by recent legal developments.

The 2002 e-Privacy Directive[88] regulates confidentiality of communications and the rules regarding tracking and monitoring online. With the entry into force of the General Data Protection Regulation (GDPR), the e-Privacy Directive required updating and is likely to be replaced by the e-Privacy Regulation[89] proposed in 2017. A year later, the EU Electronic Communications Code (EECC)[90], a new Directive which reforms the framework for the regulation of electronic communications services and networks, was introduced. With the entry into force of the EECC, the definition of 'electronic communications service' changed and now includes the so-called 'number-independent interpersonal communications services' (NI-ICS), i.e. services using numbers as a mere identifier, such as instant messaging. As of the entry into force of the EECC, this definition will also be applied to the e-Privacy Directive. As a result of this NI-ICS providers will be legally required to be in compliance with the e-Privacy Directive, which will interfere with the voluntary anti-CSAM activities. To 'fix' this, the Commission proposed a Regulation for the temporary derogation, valid until 2025, from certain provisions of e-Privacy Directive as regards the use of technologies by NI-ICS for the processing of personal and other data for the purpose of combatting CSA online, in line with the 2020 EU strategy for a more effective fight against CSA. This quick 'fix' by the Commission has however been the subject of scrutiny by the European Parliament because of privacy reasons.[91] Following lengthy debates, the European Parliament and the Council compromised and found a political agreement with a more narrow scope for a temporary and strictly limited derogation.[92] It remains to be seen how this will develop further and whether these voluntary practices will be included in the e-Privacy reform or if it will be included in the new legislation to combat CSA announced by the Commission.

These developments will be followed and reported on in D2.2, the final legislative compliance report due at the end of the INSPECTr project.

2.2 Council of Europe

Section 2.2 discusses the Council of Europe legal instruments which may be directly or indirectly relevant to digital evidence.

[88] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37,

[89] Proposal for a Regulation of the European Parliament and of the Council 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) COM (2017) 010 final.

[90] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36.

[91] <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf>.

[92] See <https://www.europa-nu.nl/id/vliec7g9hxzh/nieuws/fighting_sexual_abuse_of_children?ctx=vim2bx14ecsu&s0e=vifdkm1d06kk>.

2.2.1 European Convention on Mutual Assistance in Criminal Matters

Type of instrument	Convention
Link to full text	https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016800656ce
Status	In force
Focusses on	MLA
Relevance	Cross-border gathering of evidence
Additional comments	The EIO Directive replaces the corresponding provisions of this Convention for the Member States bound by the EIO Directive

The 1959 European Convention on Mutual Assistance in Criminal Matters[93] is a Council of Europe legal instrument, which has a wider reach than the EU's legal instruments, considering that it has 50 state parties, including all of the EU Member States. The Contracting Parties to the Convention agree to afford each other the widest measure of mutual assistance in criminal matters.[94] Mutual assistance under this Convention can be requested by way of letters rogatory sent to the requested Party.[95] This means that the requesting Party can send a letter rogatory relating to a criminal matter for the purpose of obtaining evidence, including the hearing of witnesses, experts, etc. The 1978 and 2001 Additional Protocols[96] improved the Convention, in particular considering the way in which mutual assistance can be requested which makes it easier, quicker and more flexible in view of technological developments and better takes into account data protection. With the 2001 Additional Protocol requests for mutual assistance are done in writing by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and are returned through the same channels.[97] In urgent cases, requests can take place through the International Criminal Police Organisation (Interpol).[98] The 2001 Additional Protocol furthermore, modernises the Convention by including provisions on video and telephone conference hearings, spontaneous information, temporary transfer of detained persons, cross-border observations, covert investigations and JITs,[99] similar to the provisions in the EU legal instruments discussed in paragraph 2.1. While this improves the Convention, this traditional MLA system is a slow process, in particular when it comes to digital evidence with its volatile nature.

As of the entry into force of the EIO Directive, the EIO is the instruments that needs to be used by the Member States bound by the EIO Directive. This means that countries who are bound by the EIO Directive need to request for judicial cooperation via the EIO system and that for those countries the corresponding provisions of the EIO Directive apply. For example, if the Netherlands wishes to obtain evidence from Germany, the Netherlands needs to issue an EIO and can no longer rely on this Convention. The Convention does however remain in force for those countries to whom the EIO Directive does not apply, such as Ireland and Denmark, as well as third (non-EU) countries party to the Convention.

[93] European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030.
[94] Article 1 (1) European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030.
[95] Article 3 (1) European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030.
[96] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099 and Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182.
[97] Article 4 (1) Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182.
[98] Article 4 (7) Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182.
[99] See Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182, Articles 9, 10, 4, 3, 17, 19 and 20 respectively.

2.2.2 Cybercrime Convention

Type of instrument	Convention
Link to full text	https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
Status	In force
Focusses on	Cybercrime
Relevance	Also applies to digital evidence
Additional comments	Legally binding, large number of signatories beyond the EU

The 2001 Council of Europe Convention on Cybercrime (Cybercrime Convention)[100] is the first and most important international legally binding treaty in the field of cybercrime considering that is has (currently[101]) 65 ratifications and 3 signatures not yet followed by ratification (including Ireland and Sweden). Among the 65 ratifications are all of the member states of the Council of Europe (which includes all of the EU Member States and the United Kingdom) except Russia, and also includes 31 countries who are not member states of the Council of Europe, including the USA, Canada, Australia, Israel, and more.[102] The reason why this Convention is so important is because it has a large reach, beyond the EU. It goes as far as to harmonise national criminal law of offences and connected provisions in the area of cybercrime in all the States Parties to the Convention, and improves international cooperation between those countries. To digital evidence, this Convention is of particular importance because cybercrimes, by their nature, consist of digital evidence. In other words, the Cybercrime Convention may also apply digital evidence that is not necessarily born out of a cybercrime as it also provides for national procedural law powers that are necessary for the investigation and prosecution of offences committed by means of a computer system or evidence in digital form.[103]

The Cybercrime Convention is addressed to the State Parties as an 'assignment' take measures at national level, which reflects the content of the Convention, and thus harmonising national laws of the States Parties to the Convention. This means that all States Parties to the Convention should have substantive criminal law provisions on: illegal access, illegal interception, data interference, system interference, misuse of devices, computer related forgery, computer related fraud, offences related to child pornography and offences related to infringements of copyright and related rights which at least reflect the content of Articles 2 – 11 of the Cybercrime Convention, while remaining free to have stricter rules in this regard. As to the aforementioned offences, States Parties need to ensure in their national laws that these offences are punishable and that legal persons can also be held liable. It also means that State Parties to the Convention need to have legislative and other measures that are necessary to establish the powers and procedures provided for in the Convention for the purpose of criminal investigations when it comes to the aforementioned criminal offences, other criminal offences committed by means of a computer system and the collection of digital evidence of a criminal offence. With regard to these procedural powers, the Cybercrime Convention determines that these powers need to be proportionate, regulated by law and accompanied by adequate safeguards, in order to ensure an adequate protection of human rights and liberties. These procedural powers, that allow LEAs to secure digital evidence, should at least include expedited preservation of stored computer data, expedited preservation and partial

[100] Convention on Cybercrime [2001] ETS No. 185.
[101] Latest update: 27 April 2021.
[102] See <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=opXpZL6v>.
[103] See Council of Europe, "Explanatory report to the Convention of Cybercrime" (ETS No 185), p. 4.

disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data and interception of content data which at least reflect the content of Articles 16 – 21 of the Cybercrime Convention, while remaining free to have stricter rules in this regard.

Apart from the aforementioned substantive and procedural measures that State Parties to the Convention need to have, the Convention also determines that State Parties need to adopt measures to establish jurisdiction when: an offence is committed in its territory, on board a ship flying its flag, on board an aircraft registered under its laws or by one of its nationals if the offence is punishable. States Parties are furthermore bound to cooperate with each other in accordance with Articles 24 – 35 of the Cybercrime Convention and other relevant legal instruments applicable to them. The Convention includes provisions on extradition, spontaneous information, and general principles. These general principles determine that States Parties need to afford each other mutual assistance to the widest extent possible, for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of digital evidence of a criminal offence. Articles 29 – 35 include specific provisions on mutual assistance, as regards expedited preservation of stored computer data, expedited disclosure of preserved traffic data, access of stored computer data, real-time collection of traffic data and the interception of content data. Based on Article 32 of the Convention, States Parties may access publicly available computer data (regardless of its location), and access or receive computer data (located in another State Party) with the consent of the person who has lawful authority to disclose the data without the authorisation of another State Party to the Convention. Whether or not this is allowed depends, however highly on the circumstances of the case, meaning that in most cases, mutual assistance needs to be requested, which can be a time-consuming procedure which is a challenge for the volatile nature of digital evidence. While the Cybercrime Convention is a huge step forward, in spite of harmonisation, there are still big differences in national enforcement legislation and approach. This can be problematic considering that an investigative measure needed to obtain evidence in another country may not be available in this country, which may lead to delays or even admissibility issues if there is no mutual recognition.

2.2.3 Electronic Evidence Guide

Type of instrument	Best practices
Link to full text	https://rm.coe.int/0900001680a22757
Relevance	Guidelines for identifying and handling digital evidence

The electronic evidence guide[104] was drafted following joint EU and Council of Europe initiatives and has been updated several times since 2013. The aim of the document is to guide countries that are in the process of developing and establishing their own rules and protocols for dealing with digital evidence and was designed for a wider audience, including LEAs, judges, prosecutors and others involved in the justice system. The guide explains: what digital evidence is, what its characteristics are and why it is important to handle it correctly. As mentioned throughout this report, digital evidence is, due to its very nature, highly volatile as it is or can be invisible to the untrained eye. Additionally, it can be easily altered or destroyed (even through normal use) and can be copied without degradation. This volatile nature of digital evidence makes it important to handle it correctly, so as to ensure the eventual admissibility in court. This means that the evidence needs to be authentic, complete, reliable, believable and obtained proportionately. Like the ENISA guidelines, the electronic evidence guides includes the same five principles to follow when dealing with digital evidence: data integrity, audit trail, specialist support, appropriate training and legality. The guide furthermore explains what the sources of digital

[104] Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges, version 2.1 [2020].

evidence are, how to gather it, analyse it and prepare it for presentation in court. It also explains jurisdiction and judicial cooperation, as well as describing the roles of the actors involved in the process.

3 Privacy and Data Protection

As described in the previous sections, the collection, analysis, prioritisation and sharing of digital evidence across jurisdictions for criminal investigations is constrained by law. LEAs and other actors involved in the area need to abide by substantive and procedural criminal law when investigating a crime and gathering evidence. When doing so, they need to execute their investigative powers and procedures with regard for human rights and fundamental rights. Most human rights and fundamental freedoms, including the right to privacy, are not absolute. This means that (depending on the circumstances) public authorities may interfere with this right if it is: provided for by law, necessary and proportionate in a democratic society and in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In particular privacy and data protection are important within the context of digital evidence. The reason for this, among other things, is that the digital evidence required for a criminal case never stands alone. It exists on a device or on an account that contains a lot of information: not only the name and personal information of the person who owns the device or uses the account, but also information on other people. Think, for example, of a mobile phone or an e-mail account, which includes an address book full of names, contact details and possibly even more information. Investigations and gathering digital evidence, thus needs to be necessary and proportionate to the purposes compatible with the prevention, investigation, detection and prosecution of crime. This means, among other things, that only the necessary information can be gathered, and that privacy and data protection need to be taken into account. Conditions and safeguards include: judicial or other independent supervision, grounds justifying application, limitation of the scope and the duration of investigative powers and procedures. This can however, be very challenging, in particular in the bigger cases which pose a threat to national security, such as terrorism. In such cases, there is a need to strike a balance between security and fundamental rights. This can be challenging, because the two need to be able to coexist. Mainly, as security can only be sound and effective if it is based on fundamental rights and freedoms, and individuals' rights cannot be secured without safe networks and systems. Security measures thus, need to be proportionate and guided by core values such: as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

According to Article 8 of the European Convention on Human Rights (ECHR)[105] and Article 7 of the Charter of Fundamental Rights of the European Union (the Charter)[106], everyone has the right to respect for his private and family life, his home and his correspondence. Correspondence within the context of privacy covers mainly written materials sent through post and telecommunications. When Information and Communication Technologies (ICTs) started to emerge in the sixties and seventies, there was a growing need for regulation of safeguards to protect individuals' personal data from automatic processing. In light of the emerging ICTs and growing amount of personal data, the right to privacy as enshrined in the ECHR was no longer adequate to provide safeguards against the processing of information coming from new ICTs. As a consequence, the right to the protection of personal data or data protection came into existence. Data protection is very much related to privacy and may even be seen as an important aspect of privacy, but it covers personal data in a broader sense, regardless of the origin of the data. Data protection is also referred to as a 'third generation' fundamental right, considering that it emerged by way of modern developments following emerging ICTs. As these rapid technological developments and globalisation bring challenges to data protection, considering the increase of the amount of data that is gathered and shared, Article 8 of the Charter, as well as Article 16 (1) of the TFEU, determine that everyone has the right to the protection of personal data concerning him or her. This right to data protection was further elaborated upon in the Council of Europe Convention for the protection of individuals, with regard to the

[105] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 005.
[106] Charter of Fundamental Rights of the European Union [2000] OJ C 364/01.

processing of personal data (Convention 108+)[107] and in the EU Data Protection Directive 95/46/EC[108], which has been replaced by the General Data Protection Regulation (GDPR)[109]. Considering that digital evidence is born out of ICTs and the focus of the INSPECTr project is within the EU context, this section will focus on data protection relevant to LEAs when investigating a crime as enshrined in EU legal instruments: the GDPR and the Data Protection LEA Directive.

3.1 GDPR

Type of instrument	Regulation
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Status	In force
Focusses on	Data protection
Relevance	General data protection rules, directly applicable

The GDPR lays down general rules for data protection: it provides rules for the protection of personal data[110] and free movement of such data. Unlike many of the other legal instruments discussed in this report, the GDPR is a Regulation. Whereas Directives set out objectives for the EU which require Member States to implement harmonising rules within national law and leave Member States free to choose how to implement them; Regulations are legally binding in their entirety, apply automatically and uniformly to all Member States without the need for implementation into national law. As such, it is a step-up for data protection governance within the EU considering that the legal discrepancies between Member States have faded with the entry into force of the GDPR. The GDPR applies to data processing that is wholly or partly by automated means and to processing other than by automated means which forms or will form part of a filing system.[111] It does not apply to data processing by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties or safeguards against and prevention of threats to public security.[112] This means that data processing by LEAs when investigating crimes falls outside the scope of the GDPR and is covered by the LEA Directive which will be discussed in the following sub-section. If LEAs or other competent authorities process data for other purposes than the aforementioned purposes, then the GDPR applies.

[107] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108. Convention 108 was modernised in 2018 by the adoption of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [2018] ETS No. 223 and is now referred to as Convention 108+.

[108] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, hereinafter GDPR.

[110] Personal data as any information that can directly or indirectly identify or help to identify a person. Indirectly identifiable means that data relates to an individual, but not necessarily immediately identifies the individual. This is also considered to be personal data considering that an individual can still be identified by combining the data with other sources.

[111] See Recital 15 GDPR.

[112] See Article 2 GDPR.

The GDPR includes duties and obligations for controllers and processors[113], meaning that data processing cannot be taken lightly. In order to process personal data, the risks to the rights and freedoms of persons need to be taken into account by adhering to the six principles for processing personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.[114] As such, data processing needs to be lawful, fair and transparent; needs to have a clear purpose while collecting only the data needed for this purpose and making sure that the data is kept up to date and not for longer than necessary; and that appropriate technical and organisational measures are put in place. Processing is lawful when at least one of the six legal grounds for processing mentioned in Article 6 GDPR applies: consent of the data subject; performance of a contract; compliance with a legal obligation; protection of the vital interests of the data subject; performance of tasks in the public interest; or a legitimate interest.[115] If there is no legal ground for processing, processing is considered to be unlawful. For processing of special categories of data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, the stricter rules of data processing in Article 9 of the GDPR apply. As regards transparency[116], the GDPR, determines that that controllers and processors need to be transparent and provide data subjects, among other things, with information concerning who processes the data, for what purpose, to whom the data is disclosed, what kind of data is being processed, what the rights of data subjects are and how to exercise them.[117] As regards appropriate technical and organisational measures, such measures need to be put in place to protect against unauthorised or unlawful processing, accidental loss, destruction or damage. This can include for example access restrictions and other security measures such as pseudonymisation and encryption or measures which ensure data protection by design[118] and by default[119]. Only meeting these duties and obligations is, however, not enough. Controllers and processors are accountable, and therefore, they also need to be able to demonstrate compliance upon request and cooperate with supervisory authorities.[120] Being able to demonstrate compliance means that controllers and processors need to be able to show that they fulfil their obligations under the GDPR. There are tools to help demonstrate accountability, some of which have to be mandatorily put in place.

An intrinsic quality of digital evidence is that it is not limited to countries' borders. The data can be transferred and stored anywhere in the world. Offering a similar level of protection within the EU is one of the reasons why the GDPR was created. However, when personal data moves across borders outside the EU, there is an increased

[113] Controllers determine the purpose and means of data processing, while processors merely process the data on behalf of a controller and do not determine purpose and means.

[114] See Article 5 GDPR.

[115] See Article 6 GDPR.

[116] The idea behind transparency is that organisations and companies gather a lot of data from people, for example in order to provide services or to sell products. This data can tell these organisations and companies a lot about a person. Persons thus give up some of their privacy in order to receive the services or purchase the goods. This is why processing personal data needs to be lawful and fair and why the GDPR provides persons with rights. In order to exercise these rights, persons need to know what data concerning them are collected, used, consulted or otherwise processed. This is referred to as the principle of transparency. A person needs to know who processes the data, what the purpose of processing is, what the risks, rules, safeguards and rights are and how to exercise them.

[117] See Articles 12, 13 and 14 GDPR. Data subjects' rights include the right of access, the right to rectification, the right to erasure (also referred to as the right to be forgotten), the right to restriction of processing, the right to data portability and the right to object. Data subjects furthermore have the right to be notified of rectification, erasure and restriction and the right not to be subjected to automated processing, such as profiling

[118] Data protection by design measures are built in technical safeguards which ensure the protection of the rights of data subjects at the earliest stages of the design of processing operations. The GDPR gives pseudonymisation and encryption as examples of a measure which ensures data protection by design.

[119] Data protection by default are measures which ensure that, by default, only personal data which are necessary for that specific purpose can be processed. This applies to the amount of data, the extent of processing, the period of storage and the accessibility of the data. This means that for example user profiles which have different settings should be pre-set in the most privacy friendly setting. Appropriate technical and organisational measures can be for example settings in ICT systems which control access to data.

[120] See Article 57(1)(e) GDPR.

risk to maintain the high level of protection offered by the GDPR. It might be for example more difficult for people to exercise their data protection rights. This is why the GDPR provides for strict rules for transfer of data outside the EU.

Even though the GDPR determines in Article 3 that its territorial scope reaches across the globe, and applies to data processing of activities of an establishment of a controller or processor in the EU and of personal data of data subjects who are in the EU, the actual exercise of rights is more difficult if the data is processed outside the EU. This means that the GDPR applies regardless of whether or not processing takes place in the EU, and regardless of whether or not the controller or processor is established in the EU. One major criticism is that territorial scope can be limiting and problematic in today's world, where electronic information is processed, shared and stored across several territorial jurisdictions and spaces. This is why in the area of law enforcement, debate is taking place on whether it is time for jurisdiction to change.[121] We are however, not there yet, which is one of the reasons why the GDPR has a strict transfer regime to third countries. The general principle in Article 44 GDPR is that data cannot be transferred to a third country unless the conditions of Chapter V are met. According to Article 45 GDPR transfer to a third country can take place if there is an adequacy decision, i.e. a decision by the Commission determining that a third country ensures an adequate level of data protection.[122] There are currently 12 adequacy decision in effect after the invalidation of the EU-US privacy shield.[123] These adequacy decisions do however, not cover the exchange of data by LEAs to which the data protection LEA Directive applies. The Commission is currently negotiating with the United Kingdom (UK) for the adoption of two adequacy decisions for transfers of personal data to the UK under the GDPR and under the LEA Directive. For third countries, for whom there is currently no adequacy decision, transfers can only take place if the controller or processor has provided for appropriate safeguards, or if the data subject has given explicit consent for data processing in the third country.

[121] Mention is being made of universal or investigative jurisdiction to aid in the sphere of online policing. See D.J.B. Svantesson, 'Law enforcement cross-border access to data', *Preliminary Report* November 2016; D.J.B. Svantesson and L. van Zwieten, 'Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution', *Computer law & Security Review* 32 (2016), p. 671-682. See also A. McQuinn and D. Castro, 'How law enforcement should access data across borders', *Information Technology & Innovation Foundation*, July 2017.

[122] Transfer has an important role in the GDPR. While the free flow of information has always been promoted by data protection legal frameworks, the major concern was that data protection legislation could be circumvented by moving processing operations to countries with no or less strict data protection laws. European data protection legal frameworks have therefore always been cautious about transferring data to third countries who are not part of the legal regime. In order to prevent data from being transferred to 'data havens', the principle of equivalent protection was introduced, meaning that there should be no restrictions on transborder data flows to states with legal regimes which ensure data protection equivalent to data protection offered by the GDPR.

[123] See <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Last checked on 3 May 2021.

3.2 LEA Directive

Type of instrument	Directive
Link to full text	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN
Status	In force
Focusses on	Data protection in the context of law enforcement
Relevance	Specific harmonising LEA data protection rules

In order to prevent, investigate, detect and prosecute crimes and to prevent against threats to public security, LEAs need to be able to gather and share data, including across borders. This judicial and police cooperation in criminal matters needs to be facilitated, while ensuring data protection, which is equivalent in all Member States. Therefore, the Data Protection LEA Directive[124] was adopted to protects citizens' data when their data is used by LEAs. The LEA Directive strengthens the rights of data subjects and the obligations of LEAs when processing the data. This Directive was adopted due to the specific nature of data processing in the area of judicial and police cooperation, which needed specific rules as opposed to the general rules in the GDPR.[125] Moreover, it applies to all authorities that process personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties and safeguarding and preventing threats to public security. Any data processing which falls outside this scope is covered by the GDPR.[126]

The Directive is aimed at harmonising rules to protect data that is processed within the context of law enforcement, and ensuring that data can be exchanged among competent authorities.[127] Similar to the GDPR, the Directive includes rights for data subjects, and obligations for controllers and processors.[128] The Directive determines that processing of personal data, within the context of the LEA Directive, needs to be lawful and fair.[129] It does not prevent investigations, rather it facilitates LEAs carrying out their activities, including for example covert operations, as long as the data is collected for and processed in a manner that is compatible with specified, explicit and legitimate purposes.[130] Data furthermore, needs to be adequate, relevant and not excessive, meaning that no excessive data should be collected, and that the data is not kept longer than necessary. This includes data processed beyond the context of prevention, investigation, detection or prosecution of criminal offences as this is sometimes necessary in order to develop an understanding of criminal activities and to make links between different criminal offences. This data also needs to be accurate considering the great impact it may have if this is not the case, considering that it may include statements that are based on the subjective perception of persons, which are not always verifiable. Article 7 of the LEA Directive therefore determines that a distinction needs to be made between personal data based on facts and personal data based on personal assessments. Data that is inaccurate, incomplete or no longer up to date needs to be erased or

[124] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.
[125] See Recital 10 LEA Directive.
[126] See Recital 11 LEA Directive.
[127] See Recital 15 LEA Directive.
[128] See Recital 7 LEA Directive.
[129] See Recital 26 LEA Directive.
[130] Ibid.

rectified, and cannot be transmitted or made available. As to the erasure of data, it needs to be ensured, using appropriate time limits that the data is not kept for longer than necessary, depending on the purpose for processing.[131] Similar to the GDPR, the LEA Directive also provides that appropriate security needs to be ensured by using appropriate technical and organisational measures, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.[132] The Directive applies to the processing of personal data of data subjects. While the GDPR speaks of data subjects in general, the Directive includes different categories of data subjects as this is inherent to processing within the law enforcement context: a clear distinction needs to be made between suspects, convicts, victims, witnesses, informants, associates, etc.[133] While the GDPR, in principle, prohibits the processing of special categories of data, the Directive allows this where strictly necessary, subject to appropriate safeguards and only if authorised by law, to protect the vital interests of the data subject, or if this data was already made public by the data subject.[134]

As extensively discussed in section 2 of this report, it is of the utmost importance to be able to share information among LEAs across the globe as digital evidence due to its very nature is not bound by borders. Chapter V of the Directive therefore, provides for transfers of personal data to third countries. Transfers to third countries can only take place if it is necessary for the purpose of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties safeguarding and preventing threats to public security, and if the data is sent to a competent authority who is charged, according to national law, with this purpose.[135] Similar to the GDPR, transfers are allowed on the basis of an adequacy decision taken by the Commission[136] or, in the absence of an adequacy decision, if appropriate safeguards have been taken.[137] If there is no adequacy decision and no appropriate safeguards have been taken, the transfer can only take place if: it is necessary to protect the vital interests of the data subject or other persons, to safeguard the legitimate interest of the data subject, to prevent an immediate and serious threat to public security and in individual cases for the purpose of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties and safeguarding and preventing threats to public security or for the establishment, exercise or defence of legal claims relating to this purpose.[138] These derogations are interpreted restrictively and should be limited to what is strictly necessary. There are currently no adequacy decisions that cover data exchanges in the area of law enforcement, only one with the UK for which the Commission started negotiations.[139] This means that transfers to third countries should, in principle, only take place after authorisation by the Member State from which the data were obtained, unless there is an immediate threat. If there is an adequacy decision in place, transfers can take place without authorisation. As there are currently no adequacy decision in the area of law enforcement, transfers are allowed if appropriate safeguards have been provided in a legally binding instrument, such as bilateral or multilateral agreements, including cooperation agreements between Europol or Eurojust and third countries. It should furthermore, be noted that all EU Member States are affiliated with Interpol and that Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combatting international crime. Interpol thus aids in an efficient exchange of data.

[131] Article 5 LEA Directive.
[132] Article 29 LEA Directive.
[133] Article 6 LEA Directive.
[134] Article 10 LEA Directive.
[135] Article 35 LEA Directive.
[136] Article 36 LEA Directive.
[137] Article 37 LEA Directive.
[138] Article 38 LEA Directive.
[139] See <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

4 National legislation and practices

Section 2 and 3 discussed international and European legal instruments relevant to digital evidence, including data protection considerations. It is however not enough to look only at these instruments considering that criminal law is still very much based upon national laws and traditions. While many of the previously discussed legal instruments have been implemented into national law and as such a minimum level of harmonisation was achieved, all countries have a different legal system and have implemented differently, according to their national laws and traditions. Some countries may even have implemented stricter rules. This means that although national laws are in basis similar, in reality they can be quite different. These differences could, in some cases, challenge cross-border cooperation, as a requested measure may be different or may not even exist in another Member State. Furthermore, some Member States have opted out of certain international agreements, meaning that these agreements do not apply in those Member States and that other legal instruments need to be relied upon for MLA. In addition to these international agreements, some Member States may have bilateral or multilateral agreements, which also apply between those countries. At least two have been reported within the context of this research. In order to understand the national legal frameworks of the countries where the LL are taking place, a questionnaire has been sent to the LEAs participating in the INSPECTr project. This section looks at these national laws based on the answers provided in the questionnaires annexed to this Deliverable and then discusses the differences and similarities of these national legal frameworks and practical realities of international policing. If the INSPECTr platform is going to be used in the future, it is important that the national laws of all participating countries are taken into consideration.

4.1 Ireland

In Ireland there is no overarching criminal law, rather, Irish criminal law is embedded in several specific Acts categorised by type of crime, such as the Criminal Justice Act 2001 for theft and fraud, the Child Trafficking and Pornography Act 1998, the Non-Fatal Offences Against the Person Act 1997 and the Criminal Justice Act 2017 for offences relating to information systems. In these laws, which are preventative by nature, offences form the basis of (potential) investigations. The Irish police, or An Garda Síochána, have the power to investigate these criminal offences under the Garda Síochána Acts (1924/2005) and the Office of the Director of Public Prosecutions has the power to prosecute these criminal offences under the Prosecution of Offences Act 1974. Investigation takes place on the basis of specific laws such as the aforementioned and according to best practices and internal process codes. These best practices and internal process codes include the Garda Crime Investigations Techniques manual and the UK Association of Chief Police Officers (ACPO) Good Practice Guide for digital evidence[140]. The guidelines are used for gathering digital evidence as well as by courts when assessing the handling and seizure of digital evidence. Once the evidence is gathered, law enforcement is entitled to examine its probative value.

Irish law does not make a distinction between physical evidence and digital evidence. General (traditional) evidentiary rules apply to both physical and digital evidence. Digital evidence is however mentioned in both the Criminal Justice Act 2001 and in the Criminal Justice Act 2017 where it is defined as ‘property’ and as such protected. There are, however, certain specific investigative measures for digital environments, including obtaining data from third-party data owners and interception of telecommunications. The Data Protection Act 2018 and the Communications Act 2011 determine what type of data Service Providers are required to retain. This data can then be obtained by law enforcement for investigative purposes. Interception of telecommunications requires prior authorisation from the Minister for Justice based on the Interception of Postal Packets and Telecommunications Message (Regulation) Act 1993.

[140] This practice guide was developed by the ACPO of England, Wales and Northern-Ireland and provides guidelines for law enforcement and others involved in investigating cyber security incidents and crime.

As regards sharing digital evidence between competent authorities, the Department of Justice with the assistance of the Director of Public Prosecution and the Police is empowered to share digital evidence with requesting competent authorities based on a request for mutual assistance. Intelligence is only shared on a case by case basis.

Data protection in Ireland is regulated in the Data Protection Act 2018. The LEA Directive has been fully implemented into this Act. In line with the LEA data protection Directive, Irish police are required to take appropriate technical and organisational measures to protect the data against unauthorised or unlawful processing and accidental loss, destruction or damage. All persons processing data on behalf of the Irish police need to be aware of and comply with these technical and organisational measures to keep personal data processed for law enforcement purposes secure. Security measures within the police organisation include processes and procedures for identity and permission-based access management and associated controls, with user and password management for all databases. As previously mentioned, Irish law, including the Data Protection Act, does not make a distinction between physical evidence and digital evidence, so general (traditional) evidentiary rules apply to both physical and digital evidence. As such, the provisions of the Data Protection Act apply equally to all types of personal data processing.

When it comes to judicial cooperation, the Criminal Justice (Mutual assistance) Act 2008 provides for cross-border gathering and exchanging of evidence, including digital evidence. The Department of Justice is the competent national authority for issuing and receiving MLA requests. This means that all cross-border request to and from Ireland need to go through the Department of Justice. As mentioned in section 2.1.1, Ireland has opted out of the EIO Directive, meaning that requests to and from Ireland cannot be made under that Directive. The provisions of the Cybercrime Convention and of the NIS Directive have however been implemented in the Irish Criminal Justice (Offences Relating to Information Systems) Act 2017. This Act gives effect to the provisions of the Convention relating to offences against information systems and their data, and search and seizure powers in relation to such data.

4.2 Estonia

In Estonia there are 3 major criminal laws: the Law Enforcement Act for preventive purposes and the Code of Criminal Procedure and the Penal Code for investigative and prosecution purposes. The Penal Code provides for the criminal offences including their punishments and penalties and the Code of Criminal Procedure includes procedural rules (pre-trial and during court). As such, Estonia distinguishes between measures for preventive purposes and measures for purposes of investigation and prosecution.

General rules for gathering evidence are also included in the Code of Criminal Procedure. Estonian law does not make a distinction between physical evidence and digital evidence. General (traditional) evidentiary rules apply to both physical and digital evidence. Digital evidence is not defined in Estonian law. There are however guidelines for gathering and handling digital evidence.

Estonian law distinguishes between gathering data for preventive purposes and gathering data for investigative purposes. Investigative measures always require a legal basis, such as a warrant. Evidence is inadmissible if it is not obtained according to the provisions in the Code of Criminal procedure.

The Estonian Constitution guarantees the right to privacy and data protection. These rights are not absolute and can be interfered with in order to protect public health, public morality, public order or to prevent or prosecute a crime. Estonia has fully implemented the LEA Directive in chapter 4 of the Estonian Personal Data Protection Act as well as in certain parts of other laws, including the Police and Border Guard Act and the Code of Criminal Procedure. Processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties is thus primarily covered by these laws as well as by internal guidelines. Security of processing is guaranteed by access restrictions to databases.

Chapter 19 of the Estonian Code of Criminal Procedure covers judicial cooperation. Section 435 of this Code determines which judicial authorities are competent to engage in international cooperation. Police cooperation and information exchange takes place through the communications channels of Interpol and Europol and in compliance with their rules and regulations.

The EIO Directive and the Cybercrime Convention have been fully implemented into the Estonian Code of Criminal Procedure and Electronic Communications Act. As such, requests for mutual assistance to and from Estonia can be made within the EIO framework or by sending letters rogatory within the framework of the European Convention on Mutual Assistance in Criminal Matters. For international exchanges there are guidelines available based best practices as well as regulations of Interpol and Europol.

4.3 France

The French legal framework includes a number of major, overarching laws: the Security Code for preventive measures and the Penal Code and the Criminal Procedural Code for investigative measures. As such, French law provides for a strict distinction between preventive and investigative measure, in fact, in several decisions and declarations, the Constitutional Council has reiterated that preventive measures should not be carried out for criminal prosecution and vice-versa. This implies that there are two types of activities: administrative police activities for preventative policing and judicial police activities for criminal prosecution. These activities are furthermore also governed by Constitutional principles as well as other laws implementing EU legislation.

Preventive measures need to be carried out in accordance with the legal framework. When French police detect a criminal offense, they are bound to report this to the criminal prosecutor under the Criminal Procedural Code, the activity then becomes a judicial police activity. Any evidence collected then needs to be gathered following the judicial procedures in the Criminal Procedural Code for the evidence to have judicial value. All investigative measures therefore require a legal basis and need to be guided by the legal principles of the corresponding legal framework, depending on the measure and type of investigation. Under the Criminal Procedural Code there are three main types or stages of judicial procedure: preliminary investigations, expedited investigations and letter rogatory. During the preliminary and expedited investigations, the investigations are led by the criminal prosecutor, often requiring police to ask the prosecutor in charge for permission to carry out (intrusive) investigative measures. For certain measures, such as search and seizure of property, the Criminal Procedural Code requires a court order.

French law does not make a distinction between physical evidence and digital evidence. Thus, general (traditional) evidentiary rules apply to both physical and digital evidence. The Criminal Procedural Code determines that offenses can be established by any type of legally obtained evidence and that the judge decides of his own conviction, based on the evidence brought before him during proceedings. However, certain laws have been adopted in the French legal system as regards the collection and analysis of digital evidence. These include the 'special investigative measures' in the Criminal Procedural Code and provisions implementing the Cybercrime Convention. Information is always gathered by investigators, qualified persons or experts under the general investigation rules of the Criminal Procedural Code; under the Security Code in case of preventive measures; or under the Data Protection Act in case of personal data. This information becomes digital evidence by being integrated into an automated data processing system. Following this integration, the rules on analysis of data under the Criminal Procedural Code and the Data Protection Act apply. In case of a multimedia medium seized during a search, a copy can be made of the data in order to protect the integrity of the original data as evidence. This copy is then inserted in the automated data processing system. In case of digital evidence in a remote system, the Code of Criminal Procedure includes several provisions of requisition, interception, access, search and seizure. The copies of the data need to be attached to the physical procedure and destroyed after the case is closed. Analysis of the digital evidence is based on the Criminal Procedural Code. Sharing digital evidence is, in principle, forbidden under French law as investigations are covered by secrecy, unless otherwise provided by law. This means that there are certain exceptions in law based on which data can be shared, for

example if it is allowed based on an international agreement. The Security Code and the Criminal Procedural Code allows for the exchange of data between competent authorities, judicial authorities and intelligence agencies. This also includes CSIRTs if the CSIRT is a competent authority, i.e. if the CSIRT is a public CSIRT, as opposed to a private one where information needs to be requested from.

French data protection law is codified in the French Data Protection Act. The LEA Directive has been fully implemented into this Act. The Act requires that automated data processing software need to be declared and subjected to an impact assessment. This software needs to be used for a specific purpose within the preventive legal framework or within the investigative legal framework, it cannot be used for both. The national framework furthermore provides for operational guidelines which determine, among other things, who is authorised to process digital evidence. All databases are access restricted with strong authentication and connections are traced and controlled regularly. Digital evidence cannot be used for another purpose, except for opening a new case and sharing information allowed by law. In order to protect the integrity of the data, the original is cloned and the copy exploited by the investigators.

Judicial cooperation in French law is governed by the Criminal Procedural Code, which provides for the exchange of information or intelligence between French judicial authorities and foreign judicial authorities. Based on this Code, the criminal prosecutor and the investigators are responsible for requests for mutual assistance to and from France. Both EIO Directive and the Cybercrime Convention have been fully implemented into French law, in fact, the Cybercrime Convention was even implemented before parliamentary approval by public authorities who had already incorporated most of the provisions into various laws.

In the French legal system, SIAs carry out their activities based on the Security Code, which requires these activities to be carried out on a legal basis by a competent authority in the exercise of a mission entrusted to them. Actions are justified for the prevention of threats as determined by law, which allows them for example to interfere with the right to data protection if this is necessary because of a public interest, as long as it is within the limits of the law and in accordance with the principle of proportionality. On some occasions, as determined by law, data, intelligence or information gathered for preventive purposes may be shared using the procedure in the Criminal Procedural Code with judicial authorities. Vice-versa, judicial authorities can request for certain information via judicial requisition if they are aware of their existence. SIAs can share information with the criminal prosecutor and with LEAs if the information does not include national secrets. SIAs cannot access criminal cases and evidence, with the exception of terrorism cases.

4.4 Belgium

In the Belgian legal framework there are three main laws governing preventive and investigative measures: the Law on the Police Function, the Criminal Procedural Code and the Penal Code. In this legal framework there is no distinction between preventive and investigative measures. Belgian law does not make a distinction between physical evidence and digital evidence, general (traditional) evidentiary rules apply to both physical and digital evidence. Digital evidence is not defined in Belgian law, however, some concepts relevant to digital evidence have been explained in the explanatory memorandum to the Digital Criminality Law. All investigative measures require a legal basis, such as an authorisation by a judge, which are mostly found in the Criminal Procedural Code. When gathering digital evidence, an official report is made which describes what information is gathered and how this is done. All evidence is then deposited at the registry of the court. A forensic backup can be made by the Computer Crime Unit. The Criminal Procedural Code also includes rules on data retention and storage of electronic communications by electronic network providers and service providers. During investigations, the principle of proportionality is applied by judicial authorities by taking into account the gravity of the offence.

Specific investigative measures such as telephone tapping, the interception and recording of communication provide conditions for judicial authorities to interfere with private communications. When obtaining evidence from service providers, including cloud services, the Belgian Criminal Procedural Code provides for direct cooperation with service providers by determining that digital evidence can be gathered from them if the

provider is established in Belgium. In addition to this, the Belgian Criminal Procedural Code also provides for search of stored computer data. As regards online observation or infiltration, only specific LEA services and/or personnel are authorised to do this. The LEA Directive has been fully implemented into the Belgian Data Protection Act and Police Act. As regards biometric data, additional safeguards were provided, stricter than the LEA Directive. Operational guidelines are furthermore available and determine that processing digital evidence requires prior authorisation of a Judge or of the public prosecutor in charge of the investigation. Who is authorised to process digital evidence depends on categories of data and where evidence is located rather than on whether or not it is digital evidence.

The EIO Directive and the Cybercrime Convention have been fully implemented into the Digital Criminality Law, Penal Code and Criminal Procedural Code. For judicial cooperation within the EU, the EIO is used. For judicial cooperation with third countries as well as with countries that have opted out of the EIO Directive, MLA and the Cybercrime Convention is used. Depending on the stage of proceedings and on the nature of the investigative measure concerned, the public prosecutor or the investigative judge may request or authorise cross-border transfer of digital evidence to and from Belgium.

For sharing information between LEAs and CSIRTs, Belgian law provides that information can be shared for preventive purposes when the classification of the information allows this. For investigative purposes, information is shared when the CSIRT has been appointed as criminal expert by the Public Prosecutor's Office. As regards exchange of information between LEAs and SIAs, an agreement exists for State Security Military Security for transmission of classified information.

4.5 Latvia

The Latvian legal framework provides for a strict distinction between preventive and investigative measures, with preventive measures being regulated in the Operational Activities Act and investigative measures being regulated in the Criminal Procedural Code. The Criminal Procedural Code provides that factual information obtained under the Operational Activities Act and information that has been recorded by technical means, may only be used as evidence if it can be examined in accordance with the procedures in the Criminal Procedural Code. All investigative measure in the Criminal Procedural Code require a legal basis, often a decision by an investigating judge unless otherwise provided by law. Exceptions may be emergency situations which require swift action with the consent of the public prosecutor. In such cases the investigating judge still needs to be informed the next day by presenting the materials that justified the necessity and emergency of the investigative action, as well as the minutes of the investigative action. The investigative judge will then examine the legality and validity of the investigative action in order to determine whether or not the evidence is admissible.

Latvian law does not make a distinction between physical evidence and digital evidence. Thus, general (traditional) evidentiary rules apply to both physical and digital evidence. However, digital evidence is defined by the Latvian Criminal Procedural Code as information regarding facts in the form of electronic information that has been processed, stored, or broadcast by automated data processing devices or systems. As opposed to physical evidence, which is considered to be any object that was used for, has traces of or contains information about a criminal offence. When it comes to gathering, analysing and sharing digital evidence the Law on Forensic Experts, the Administrative Procedure Act, the Civil Procedure Act and the Police Act apply on top of the Criminal Procedural Code. The Law on the Security of Information Technologies furthermore applies to gathering, analysis and sharing of digital evidence by CSIRTs. The Criminal Procedural Code includes a chapter on special investigative action providing for interception of telecommunications, which is allowed if there are grounds to believe that the information will be revealed that would not have been revealed without the investigative action. If the service provider is located in another country, Articles 22 and 31 of the Cybercrime Convention apply.

Data protection in Latvia is codified in the Electronic Communications Act. This law covers gathering, analysis and sharing of digital evidence by third-party data owners such as service providers. It determines that service providers cannot disclose any information about their users or subscribers unless if this information is necessary

for authorities. As regards data processing by LEAs, the LEA Directive has been fully implemented into Latvian law in the Law on Processing of Personal Data in Criminal and Administrative Violation Proceedings, which mentions the necessary safeguards to be taken when gathering and analysing personal data in investigative measures. According to this law, evidence may be processed only by those authorities whose officials (such as police and prosecution) are entitled to conduct criminal proceedings under the Law on Processing of Personal Data in the Criminal and Administrative Violation Proceedings. Based on the Law on State Information Systems all databases have a strong authentication system for authorised access. As regards retention of digital evidence, there is no specific legislation governing how long digital evidence can be stored, so this varies depending per institution and even per department.

When it comes to judicial cooperation, the Cybercrime Convention and the EIO Directive have been fully implemented into Latvian law. The Criminal Procedural Code includes a chapter on assistance to a foreign country in the performance of procedural actions. For requests for mutual assistance to and from Latvia, the International Cooperation Department of the Central Criminal Police Department of the State Police of Latvia is responsible. Latvia is allowed to share digital evidence cross-border under the Cybercrime Convention or under the EIO Directive. It furthermore has reported a multilateral agreement with Estonia and Lithuania; a bilateral agreement with Belgium; and is currently negotiating bilateral agreements with several countries as regards judicial cooperation in criminal matters.

4.6 Romania

In Romania there is a distinction between preventive measures provided in the Criminal Code and investigative measures provided in the Criminal Procedural Code. Legal procedures as regards gathering data for crime prevention are furthermore included in the Romanian Police Act. Digital data obtained for preventive purposes can also be used as digital evidence in prosecution. All investigative measures require a legal basis such as a warrant following the Criminal Procedural Code. The Romanian legal framework makes a distinction between physical evidence and digital evidence in terms of collecting and analysing evidence. Concepts and definitions regarding the collection of digital evidence, included interception of telecommunications and computer-assisted search, are included in chapter IV of the Criminal Procedural Code. Depending on the type of crime, specific provisions are also included in other normative Acts.

The Romanian Constitution provides for the fundamental rights to data protection and privacy. It determines that public authorities need to respect and protect intimate, family and private life and that the secret of letters, telegrams, other postal items, telephone calls and other legal means of communication is inviolable. The LEA Directive has been fully implemented into Romanian national law. National operational guidelines on processing digital evidence are furthermore included in the Romanian Police Act, which determines that evidence is gathered and processed by police authorities and prosecutors. The general rules for evidence management also apply to digital evidence, even though digital evidence analysis has a distinct procedure under the Criminal Procedural Code. There are no special provisions for the preservation of digital evidence. As regards access to digital evidence databases, the Romanian national legislation provides authority specific access to databases. On an individual level, a person's access to a database is subject to authorisation and conditions for ensuring data security. Personal data collected for the purpose of preventing, discovering, investigating, prosecuting and combating criminal offences may not be processed for any other purpose, unless otherwise provided by law.

As regards judicial cooperation, the Cybercrime Convention and the EIO Directive have been fully implemented into the Romanian legal framework in the International Judicial Cooperation Act and the Law on the cooperation of the Romanian public authorities with Europol. Based on these laws, the investigative officers under the supervision of public prosecutor can make a request for mutual assistance based on the EIO Directive, under the Cybercrime Convention or via Eurojust, depending on the country whose assistance is sought. There is no distinction between the transfer of physical evidence and digital evidence, general (traditional) evidentiary rules apply to both physical and digital evidence.

There are no specific rules regarding the exchange of digital evidence among LEA's. Information and data are exchanged on request on a case by case basis. Legally obtained information may be shared between LEAs and SIAs. The Romanian Intelligence Service Act determines that data and information indicating the preparation or commission of a criminal act may be shared between LEAs and SIAs as provided by the Criminal Procedural Code.

As regards gathering, analysis and sharing digital evidence by CSIRTs, the NIS Directive has been fully implemented into Romanian national law. According to this law, the Romanian National Computer Security Incident Response Team (CERT-RO) is the competent national authority supervising digital service providers and operators of essential services as mentioned in the NIS Directive. As such, CERT-RO consults and cooperates with criminal investigation bodies including police and prosecution.

4.7 Differences, similarities and practical realities

When it comes to understanding the legal framework as regards digital evidence, including data protection considerations, this report shows that there is no straight forward answer as to what the applicable law is. Criminal law is still very much based upon national laws and traditions as can be seen in the answers provided by the LEAs participating in the LLs. While some harmonisation has taken place by way of the legal instruments discussed in sections 2 and 3, the actual implementation of these instruments varies per country and not all countries are partners to all instruments. This means that, also when it comes to the exchange of digital evidence, countries rely on various instruments, using various channels. While countries do know their way around this system and channels, some MLA instruments may take longer for a request to be answered than other, which can be problematic when it comes to digital evidence and its volatile nature. Furthermore, these differences in national legislation and approach can sometimes also result in difficulties gathering digital evidence. This is because a country may request a certain investigative measure which does not exist or is not the same in another country. Apart from this, some other practical or cultural realities have been reported over the years in various projects.[141] This includes for example language barriers, i.e. not all actors involved understanding English as well as issues with interpretation following translations.

When asking the LEAs involved in the project general questions about their national legal framework, these differences were already visible. The Irish legal system in particular stands out from the others considering that Ireland has a common law[142] legal system whereas the others have a civil law[143] legal system. The Irish legal framework has no overarching criminal law, while the other countries do have overarching criminal laws. In Ireland, criminal offences are outlined in various Acts which are specific to the type of criminality. As such, there is also no strict distinction between preventive and investigative measures. In Ireland, criminal legal provisions are preventive by nature, whereas, in the legal frameworks of the other countries (except Belgium), a distinction is made between preventive and investigative measures. Ireland furthermore stands out as it has opted out of several EU legal instruments, such as the EIO Directive, meaning that digital evidence cannot be shared with Ireland within the EIO framework and the new eEDEs platform. For all the other countries, EIO's are also available. Ireland has further more signed the Cybercrime Convention, however, it has not ratified it. While signing means that the terms of the Convention have been agreed upon by the States Parties to the convention, ratification is required following national procedures in order to become binding law. With the implementation of the NIS Directive, which has provisions that are similar to the provisions of the Cybercrime Convention, Ireland has already partly given effect to the provisions of the Cybercrime Convention. Ratification of the Cybercrime Convention will most likely follow after the entry into force of a new Irish Cybercrime Act.[144] This means that

[141] Such as the EVIDENCE project <http://www.evidenceproject.eu> and the TREIO project <https://treio.eu>.
[142] In common law the body of law is mainly derived from case-law.
[143] In civil law the body of law is derived from codified legal Acts. Civil law can furthermore be divided within different 'schools', by which the body of law is influenced, such as Napoleonic and Germanic law. Estonia and Latvia follow a more Germanic legal tradition whereas Belgium, France and Romania follow a more Napoleonic legal tradition.
[144] See <http://www.justice.ie/en/JELR/Pages/SP19000010>.

MLA to and from Ireland cannot be requested based upon the Cybercrime Convention yet either. The conclusion that can be drawn from this is that digital evidence can be shared cross-borders, however, it highly depends on the parties involved which legal instrument and which channel needs to be used for this. Often the secure channels of Interpol or Europol are used for police cooperation and the exchange of information, as indicated by Estonia. Estonia furthermore reports that there are guidelines for the working process of international exchanges which are based on best practices and regulations of Interpol and Europol. While improvements have been made to facilitate judicial cooperation, which simplifies and speeds up MLA, the practical reality remains that there still is room for improvement as mentioned by Belgium. When it comes to deciding the legal instrument of choice for asking for judicial cooperation, it depends on the country and on the type of information or evidence requested what kind of assistance is asked with reference to which legal instrument. The table below shows a simplified overview of this based on the information provided in the questionnaires and on the legal instruments.

Ireland →	← MLA (EU 2000 Convention) →	← Estonia, France, Belgium, Latvia, Romania
Estonia →	← EIO or MLA (Cybercrime Convention) or bi/multilateral agreement* →	← France, Belgium*, Latvia*, Romania
France →	← EIO or MLA (Cybercrime Convention) →	← Estonia, Belgium, Latvia, Romania
Belgium →	← EIO or MLA (Cybercrime Convention) or bi/multilateral agreement* →	← Estonia, France, Latvia*, Romania
Latvia →	← EIO or MLA (Cybercrime Convention) or bi/multilateral agreement* →	← Estonia*, France, Belgium*, Romania
Romania →	← EIO or MLA (Cybercrime Convention) →	← Estonia, France, Belgium, Latvia

While there are differences between the countries, as this overview also shows, there are also similarities. What all countries do have in common is that all measures require a legal basis for beginning investigations, depending on the country and on the measure, this can be a decision of an investigative judge or permission of the public prosecutor. When it comes to digital evidence, the general tendency among the six countries is that there are no specific rules for digital evidence, general evidentiary rules apply to both physical and digital evidence, including to the transfer of digital evidence. The exception is Romania, where a distinction between physical and digital evidence is made in terms of collection and analysis of digital evidence. Also, no specific definition of digital evidence exists in the six countries, except that in Ireland digital evidence is categorised as 'property' under property protection laws. As regards the system of fundamental rights and specifically as regards the right to data protection, all six countries reported that the LEA data protection Directive as discussed in section 3.2 of this report has been fully implemented within their national laws. This means that all data processing by LEAs needs to abide by the rules set out in the LEA Directive as implemented within their national laws. Following these rules and to keep the data processed by LEAs secure, safeguards, such as access controls, have been built into the LEA databases. While these rules are necessary in our technology-driven world, there are also side-effects to the data protection legislation which can negatively impact LEA investigations. France for example has indicated that the data protection reform which adopted the GDPR and the LEA Directive has had a great impact on data processing in the EU and increased overall awareness of data protection, as mentioned by Latvia. Following these rules, controllers are encouraged to take technical and organisational measures, such as anonymisation, pseudonymisation and measures on storage and deletion of data after a certain amount of time. While these are good measures to counter, for example, cybercrimes, the adverse effect is that the data may no longer be available to LEAs following data retention rules. This could make investigations more difficult.

Digital evidence is not only shared cross-borders, it might happen that it needs to be shared between various national agencies. While Latvia and Belgium report that they do not have specific rules governing these exchanges, the other countries do have rules in place. Estonia, Romania and France all report their own variation of an internal security code which governs the sharing or exchange of data between competent judicial authorities and SIAs. Estonia has a e-file system for this, which is a database for processing procedural information and personal data which is also used for forwarding data and documents. Romania indicates that, if the preparation or commission of certain criminal offences is suspected following investigations, the data can be shared with criminal investigation bodies. This is the same in France, where data can be exchanged between competent judicial authorities and some intelligence agencies as regards criminal offenses and terrorist cases in particular. In Ireland competent judicial authorities can share digital evidence following a request and can be shared with SIAs on a case by case basis.

As regards practices affecting unregulated cyber investigations, such as observation on the internet and infiltration of social media, the six countries have indicated that general investigative rules are applied for this. This includes for example the general conditions for conducting surveillance activities, wire-tapping and covert observations. Within this context, France has indicated that, with the exception of observation of the public internet, officers need to be trained and empowered to be able to use these kinds of techniques. SIAs can furthermore access network operators' infrastructure for observation on the internet and infiltration on social media for preventive purposes of specific types of threats as indicated by law. Belgium also reports that infiltration is only allowed by specific LEA services and personnel. France and Belgium also report specific legal provisions allowing network operators to assist LEAs in the observation on the internet and infiltration on social media. Estonia and Romania report that general rules for granting access to communication networks apply.

The table below shows an overview of the differences and similarities between national laws as discussed in this section. For more detailed information about national laws in the countries participating in the LL, the full answers to the questionnaires are available in the annex.

Table of comparison

Section 1	**Ireland**	**Estonia**	**France**	**Belgium**	**Latvia**	**Romania**
1. Distinction between preventive and investigative measures	No	Yes	Yes	No	Yes	Yes
2. Laws governing preventive and investigative measures	No overarching criminal code, specific Acts include: -Criminal Justice Act -Child Trafficking & Pornography Act -Non-Fatal Offences Against the Person Act	-Law Enforcement Act -Criminal Procedural Code -Penal Code	-Security Code -Penal Code -Criminal Procedural Code	-Law on the Police Function -Criminal Procedural Code -Penal Code	-Criminal Procedural Code -Operational Activities Law	-Criminal Code -Criminal Procedural Code
3. Legal basis required for investigative measures	No, but the framework requires all actions of Garda members to have a legal and ethical basis based on laws that provide for the search under warrant of places or persons, and the seizure of goods, property or data.	Criminal Procedural Code https://www.riigitataja.ee/en/eli/518052020007	The legal system requires a legal basis for all investigative measures, but not specifically a warrant	Yes	Criminal Procedure Law	Criminal Procedural Code
4. Distinction between physical evidence and digital evidence	No	No	No, but certain laws have been enacted to guide the collecting and analysing digital evidence	No	No	Yes, Criminal Procedural Code makes a distinction
5. Laws governing gathering, analysing and sharing of digital evidence	-Data Protection Act -Communications Act	Handling digital evidence by police is governed by guidelines	-Gathering: Criminal Procedural Code (judicial), Security Code (preventive), Data Protection Act (personal data), -Analysis: Criminal Procedural Code	Criminal Procedural Code	-Law on Forensic Experts - https://likumi.lv/ta/en/en/id/280576-law-on-forensic-experts -Criminal Procedural Code - https://likumi.lv/ta/en/	Criminal Procedural Code

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

			-Sharing: Criminal Procedural Code		en/id/107820-criminal-procedure-law -Administrative Procedure Law - https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law -Civil Procedure Law - https://likumi.lv/ta/en/en/id/50500-civil-procedure-law On Police - https://likumi.lv/ta/en/en/id/67957-on-police	
6. Laws governing sharing digital evidence between competent authorities, and third-party data owners	Mutual Assistance request	-Security Authorities Act -Criminal Procedural Code	-Security Code -Criminal Procedural Code	No specific laws or regulations	No specific laws or regulations	Law regarding the organisation and functioning of the Romanian Intelligence Service
7. Definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations	-None, Communications Act and guidelines such as ACPO apply	None	General framework of Criminal Procedural Code	There are no legal definitions, some concepts in explanatory memorandum to the Law concerning digital criminality	Definitions of types of data can be found in Electronic Communications Code https://likumi.lv/ta/en/en/id/96611	Criminal Procedural Code
8. Legal procedures or codes of conduct regulating the gathering of data for crime prevention	Communications Act	Law Enforcement Act https://www.riigiteataja.ee/en/eli/508052020005/consolide)	-Data Protection Act -Security Code		No	-Law on the Functioning of the Romanian Police -Provision regarding activity carried out by the Romanian Police -Strategy for the Modernisation of the Romanian Police -Recommendation R 19/1987 Council of Europe
9. Legal procedures or codes of conduct regulating the	-The Garda Crime Investigations Techniques manual	Criminal Procedural Code	Criminal Procedural Code	Criminal Procedural Code	Criminal Procedural Code https://likumi.lv/ta/en/	Criminal Procedural Code

collection of digital evidence in criminal investigations	-Best practice guides such as ACPO				en/id/107820-criminal-procedure-law	
10. Provision covering lawful interception for investigative purposes in a digital environment	-Interception of Postal Packets and Telecommunications Message (Regulations) Act -The Criminal Justice (Surveillance) Act	No specific legal provision - general provision in the Criminal Procedural Code https://www.riigiteataja.ee/en/eli/518052020007/consolide	Criminal Procedural Code	Criminal Procedural Code	-Operational Activities Law https://likumi.lv/ta/en/en/id/57573-operational-activities-law - Criminal Procedural Code https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law	Criminal Procedural Code
11. Legal provision covering lawful interception on terminal devices for investigative purposes	No	No	Criminal Procedural Code -"*Cour de Cassation*" Crim.16 November 2013, n° 12-87.130	Criminal Procedural Code	Criminal Procedural Code	Criminal Procedural Code
12. Legal provision covering computer-assisted search for investigative purposes	No	No	Data Protection Act	Criminal Procedural Code	No	Criminal Procedural Code
13. legal provision covering the seizure of digital evidence (data itself and/or media carrying the data)	No, but the Garda Crime Investigations Techniques manual and best practice guides such as ACPO are use	No	-Criminal Procedural Code -National platform for judcial interception	No	Criminal Procedural Code https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law	Criminal Procedural Code
Section 2	**Ireland**	**Estonian**	**France**	**Belgium**	**Latvia**	**Romanian**
1. System of fundamental rights, privacy and data protection	Communications Act	-EU Charter of Fundamental Rights of the European Union -Constitution of the Republic of Estonia	Yes	-Data Protection Act -Criminal Procedural Code	-Electronic Communications Code https://likumi.lv/ta/en/en/id/96611-electronic-communications-law -Law on Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceedings	The Romanian Constitution

					https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa	
2. Implementation of the LEA Data Protection Directive (EU) 2016/680	Yes, -Data Protection Act	Yes, -Data Protection Act https://www.riigiteataja.ee/en/eli/523012019001/consolide	Yes, -Data Protection Act	Yes, -Data Protection Act -Police Act	Yes, -Law on Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceedings https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa	Yes, -Law No. 363/2018 on processing personal data by competent authorities for the purpose of prevention, investigation, prosecution and combatting criminal offences -No greater guarantees are provided than those of Directive EU 2016/680
3. Rules or operational guidelines on who is authorised to process digital evidence	The Data Protection Act applies equally to all types of personal data processing, it does not distinguish digital evidence	General provisions of the Criminal Procedural Code	No difference between the general framework of evidence, and the framework of digital evidence	Processing digital evidence requires prior authorisation. In reality, it does not depend on the form of data (digital or not) but categories of data and where evidence is located	Law on Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceeding Lhttps://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa	Law on the functioning of the Romanian Police. The general rules for evidence management also apply to digital evidence, even though digital evidence analysis has a distinct procedure in the Criminal Procedureal Code
4. Standard Operating Procedures (SOPs) or codes of conduct for the preservation of digital evidence	No	-Criminal Procedural Code -Internal guidelines for handling digital evidence and general rules for handling evidence	Criminal Procedural Code. Original data are cloned to protect their integrity, a copy is exploited by investigators	No	No. Retention period for digital evidence varies per institution and per department	No
5. Specifications rules on the preservation of digital evidence	No	Yes, -Internal guidelines partially govern the issue of the preservation of digital evidence	Yes	No specific rules, general rules apply	No	No specific rules on preservation of digital evidence. Criminal Procedural Code and provisions in other normative acts apply
6. Access restrictions	Yes	Yes	Yes	General rules for access	Yes,	Yes

to databases					Law on State Information Systems https://likumi.lv/ta/en/en/id/62324	
7. Safeguards against function creep	Yes	Yes	Yes	General rules for access	No	Yes
8. GDPR impact on policing	No	Yes	No, but better quality of data	Not yet observed till now	No, but greater awareness of data protection	No
Section 3	**Ireland**	**Estonia**	**France**	**Belgium**	**Latvia,**	**Romania**
1. Laws governing cross-border cases, competent authorities for cross-border exchange	The Criminal Justice (Mutual assistance) Act provides for the collection and exchange of digital or any evidence with a requesting Central authority outside the State	-Criminal Procedural Code -International Cooperation in Criminal Procedure -Police cooperation and information exchange take place via Interpol and Europol and in compliance with their rules and regulations	Criminal Procedural Code	-National legislation implementing the EIO Directive -In relation to third countries, international conventions (MLA, Cybercrime Convention) are applicable	-Criminal Procedural Code https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law -Cybercrime Convention and Additional Protocol -Competent authority is the International Cooperation Department of the Central Criminal Police Department of the State Police of Latvia	-The EIO Directive supplemented by Law no. 224/2006, Law no. 222/2008, Law no. 300/2013 and Law no. 236/2017,. -Law no. 56/2018 on the cooperation of the Romanian public authorities with (Europol). Government Emergency Ordinance No. 103 of 13
2. Competent authority for approving and making requests for transferring case data or digital evidence	The Department of Justice	Competent judicial authorities as mentioned in the Criminal Procedural Code	Criminal prosecutor (or judge), investigators (police officers)	Public prosecutor or the investigative judge	International Cooperation Department of the Central Criminal Police Department of the State Police of Latvia.	The investigative officers under the supervision of case prosecutors
4. Laws governing the collection of digital evidence out of a cloud service		Inquiry sent within the EIO framework or letter rogatory	Criminal Procedural Code	No	Cybercrime Convention	MLA or EIO
5. Implementation Cybercrime Convention	Majority of the provisions in the Convention are provided for in Irish law	Yes, -Criminal Procedural Code -Electronic Communications Act	Yes -Law No. 2005-493	Yes -Digital criminality Code -Penal Code -Criminal Procedural Code	Yes	Yes, -Law No. 64/2004
6. Implementation of the EIO Directive	No -Ireland opted out of this Directive	Yes	Yes	Yes	Yes https://likumi.lv/ta/en/	Yes

					en/id/107820-criminal-procedure-law	
7. Specific rules on transfer of digital evidence		General rules apply	International Conventions and the general legal framework of the Criminal Procedural Code	General rules apply	-Criminal Procedural Code -Law on the Processing of Personal Data in Criminal Proceedings and Administrative Violation Proceedings -International agreements	No specific rules
8. Guidelines or procedures for cross-border exchange		Yes, -catalogues of best practice of SPOC and SIS, regulations of Interpol and Europol, legislation on data protection and state secrets	No	No	No	No
Section 4	**Ireland**	**Estonia**	**France**	**Belgium**	**Latvia**	**Romania**
1. Guidelines or procedures for exchange of digital evidence between national authorities		Methods of good practice	-From administrative authorities to judicial authorities: Criminal Procedural Code -From judicial authorities to administrative authorities: Criminal Procedural Code -Mutual exchanges: specific legal frameworks	Agreement for the exchange of information between LEA and security agencies	No	No specific regulations, information and data are requested and exchanged on a case-by-case basis
2. LEAs and SIAs sharing information		Transfer of information is governed Security Authorities Act	Yes, -Criminal Procedural Code -Information can be shared with LEAs upon request if it is not covered by National secret		No separate rules	Information can be shared if it was obtained legally
3. Laws governing gathering, analysing and sharing digital		-Criminal Procedural Code -Security Authorities Act	Security Code		None	-Law on the organisation and functioning of the

evidence SIAs						Romanian Intelligence Service -Criminal Procedural Code
4. Executive powers for SIAs		Yes	No -they can search and use intrusive techniques according to the Security Code		No	No -unless if caught in the act of committing a criminal offence
5. Rules on transfer of information from intelligence services to LEAs or prosecution authorities		Security Authorities Act https://www.riigiteataja.ee/en/eli/503062020002	Yes, -Criminal Procedural Code -Information can be shared with LEAs upon request if it is not covered by National secret		No	-Law on the organisation and functioning of the Romanian Intelligence Service -Criminal Procedural Code
6. Restrictions for gathering, analysing and sharing of digital evidence collected by SIAs		No	No -SIAs can access certain databases with limited prerogatives -SIAs cannot access criminal cases and evidences (except for terrorist cases), but they can receive information provided by judicial authorities		No separate rules for this	Digital evidence to be obtained legally and it has to pertain to national security
Section 5	**Ireland**	**Estonia**	**France**	**Belgium**	**Latvia**	**Romania**
1. Laws governing gathering, analysing and sharing digital evidence by CSIRTs	None		None, depends on the statute of CSIRT's		Law on the Security of Information Technologies https://likumi.lv/ta/en/en/id/220962	NIS Directive implemented by Law No. 362/2019

2. LEAs and CSIRTs sharing information or digital evidence	-Nothing prevents this sharing information -There can be an exception as regards the GDPR -Governed by agreed Memorandum of Understanding		-Private CSIRTs can share some information -LEAs can request information	-Yes, for preventive purposes, depending on the classification of the information -In criminal investigations information is shared when the CSIRT has been appointed as criminal expert by the Public Prosecutor's Office	No information about such actions	Yes, CERT-RO shall consult and cooperate, as appropriate
3. Laws governing gathering, analysing and sharing digital evidence by third-party data owners		Communications Act https://www.riigiteataja.ee/en/eli/528052020005	-Communications Act, -Criminal Procedural Code, -Security Code	Criminal Procedural Code	Electronic Communications Law https://likumi.lv/ta/en/en/id/96611-electronic-communications-law	Criminal Procedural Code
4. Laws governing the collection of digital evidence from internet service providers		General conditions in the Criminal Procedural Code. If the internet service provider is located in a foreign country: EIO or MLA request	Criminal Procedural Code	Criminal Procedural Code (freezing of data in a foreign country)	Criminal Procedural Code. Direct contact with service providers outside the jurisdiction of Latvia is not envisaged	-Criminal Procedural Code, provision on preservation of computer data
5. Procedures for LEAs to access digital evidence databases of private companies			Criminal Procedural Code	Criminal Procedural Code (seizing of data)	Criminal Procedural Code https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law	No specific procedures, the general provisions of the Criminal Procedural Code require a search warrant
6. Laws governing observation on the internet or other networks, infiltration online		Criminal Procedural Code https://www.riigiteataja.ee//en/eli/518052020007	According to the Criminal Procedural Code, officers must be specifically trained and empowered	Observation (both on- and offline), infiltration and search & seizure is done based on the Criminal Procedural Code	Criminal Procedural Code https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law	No special regulations on observing the internet or other network, general rules of the Criminal Procedural Code apply
7. Laws, operational procedures for LEA access of network operators infrastructure		The Criminal Procedural Code has procedures for wire-tapping or covert observation of information and covert surveillance	Security Code for preventive purposes and the Criminal Procedural Code for investigative purposes and prosecution	-Criminal Procedural Code -Electronic Communications Act	Special investigative actions in the Criminal Procedural Code	General rules of the Criminal Procedural Code apply

8. Laws and operational procedures allowing network operators to assist LEAs		Electronic Communications Act https://www.riigiteataja.ee/en/eli/528052020005	Security Code for preventive purposes and the Criminal Procedural Code for investigative purposes and prosecution	Criminal Procedural Code (cooperation obligation)		General rules of the Criminal Procedural Code apply, as well as Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector: data needs to be made available based on a court order

5 Conclusions

This Deliverable provides a reference framework from a legal perspective to be implemented in the INSPECTr platform, which will facilitate standard solutions for forensic investigations across LEAs within the EU. This legal analysis is highly important considering that LEAs are regulated and constrained by law in their activities. An important note to make is that this report contains an analysis of the current legal status quo. The law is dynamic, always changing, in particular in view of technological developments. This is why it is important to keep track of legal developments, which will be done throughout the lifetime of the INSPECTr project and will be reported on in D2.2 at the end of the project. In this Deliverable, the legal requirements for law enforcement powers and evidence requirements were discussed by looking at the relevant legal instruments on an international and European level and on a national level. It is important to note that there is a lot of fragmentation in this area of law: quite a large number of (national and international) legal instruments and agreements are applicable to investigations, to gathering evidence and, most importantly as regards cross-border collaboration, to the exchange of digital evidence as can be seen by reading this Deliverable. These laws regulate what powers and restrictions LEAs have and how they interact with other agencies and parties on a national and on an international level.

The INSPECTr platform will allow an investigator to visualise and bookmark important evidential material, and export it to an investigative report by using various knowledge discovery techniques. This will allow for cross-correlation analysis with existing case data and improve knowledge discovery within a case, between separate cases and between interjurisdictional investigations. As regards the cross-correlation analysis with existing case data which improves knowledge discovery within a case, it is important to note that all countries have their own rules on access to databases. This includes access restrictions with strong authentication, determining who has access to which database and which files and with whom (which authorities, SIAs, CSIRTs, etc.) it may be shared under which circumstances. These rules include data protection consideration, in particular the provisions of the LEA data protection Directive as implemented by national law. The Directive applies to all authorities that process personal data for the purpose of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties and safeguarding and preventing threats to public security. Any data processing which falls outside this scope is covered by the GDPR. Within the context of this Directive, data processing needs to be lawful and fair, allowing LEAs to carry out their activities as long as the data is collected for and processed in a manner that is compatible with specified, explicit and legitimate purposes. This data needs to be adequate, relevant and not excessive, and should not be kept longer than necessary. As such, considering that the INSPECTr platform will be set up for investigative purposes, the platform needs to take into account these rules and restrictions to be able to guarantee a secure channel for interjurisdictional investigations.

Due to its very nature, digital evidence may be located or stored anywhere in the world. Because of this increased cross-border dimension due to technology and globalisation, sharing information and evidence across borders has become extremely relevant. To be able to do this, countries cooperate by way of MLA. This MLA and exchange of digital evidence can take place on basis of various international and European legal instruments and bilateral and multilateral agreements. Currently, the leading legal instrument for this within the EU is the EIO, which will be digitised within the eEDES system operating on the e-CODEX platform. However, Ireland has opted out of the EIO Directive, meaning that for exchanges with Ireland, other instruments need to be relied upon for MLA requests. This includes the EU 2000 Convention and the Cybercrime Convention, which goes beyond the EU and can also be used for quite a large number of third (non-EU) countries. A note that needs to be made here is that the Cybercrime Convention has not yet been ratified by Ireland, although it has implemented certain provisions that are similar to the provisions of the Cybercrime Convention, thus partly giving effect to the provisions of the Cybercrime Convention. Although the developments within the area are a great improvement to the gathering and sharing of digital evidence, in particular as regards speed and efficiency, the practical reality is that it can still be a time-consuming procedure. This is a challenge, in particular considering the volatile nature of digital evidence. Not only can the evidence move or disappear altogether within a heartbeat, it can also easily

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

be altered which may cause problems with admissibility in court. The second challenge is that, in spite of harmonisation, there are still differences in national enforcement legislation and approach. While there is increasingly more attention to setting common standards for gathering and exchange of digital evidence, some countries still apply traditional evidential rules to digital evidence. Because of this, one country may request a measure which is not available in another country, which can delay the request. Apart from this, cultural aspects and language barriers in particular, but also seemingly trivial matters such as different time-zones and nuances of local laws and customs and differences in LEA capacities can also challenge cross-border cooperation. In order to overcome some of these challenges, international and European organisations such as Interpol, Europol and Eurojust, aid in facilitating MLA requests. As regards the cross-correlation analysis between interjurisdictional investigations within the INSPECTr platform, the various international and European legal instruments need to be taken into account in determining what investigation data can be shared with which authorities across borders. This is not an easy task considering that there is no straight forward answer on which legal instrument to apply in cross-border cases. The integrity and authenticity the evidence should furthermore be guaranteed during the entire chain of custody, from seizure to trial.

References

Legislation and treaties

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] ETS No. 099

Charter of Fundamental Rights of the European Union [2000] OJ C 364/01

Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/3

Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 005

Convention on Cybercrime [2001] ETS No. 185

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 [2000] OJ C 197/1

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89

Council Framework Decision of 13 June 2002 on joint investigation teams [2002] OJ L162/1

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1

Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L131/1

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

European Convention on Mutual Assistance in Criminal Matters [1959] ETS No. 030

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1

Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L 381/4

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1
Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [2001] ETS No. 182

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L 239/19

Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/01

Policy documents

Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final

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, COM (2018) 226 final

Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final

Proposal for a Regulation of the European Parliament and of the Council 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) COM (2017) 010 final

Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final

Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final

Guidelines

Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 2.1 [2020]

ENISA, *Electronic evidence - a basic guide for First Responders, Good practice material for CERT first responders* [2014], available at https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

ENISA, *Identification and handling of electronic evidence – Handbook, document for teachers* [2013] September 2013, available at https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-handbook/view

Literature and other sources

A. McQuinn and D. Castro, 'How law enforcement should access data across borders', *Information Technology & Innovation Foundation*, July 2017

Chalmers, D., Davies, G., Monti, G., *European Union Law*, Cambridge: University Press, 2010

D.J.B. Svantesson and L. van Zwieten, 'Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution', *Computer law & Security Review* 32 (2016)

D.J.B. Svantesson, 'Law enforcement cross-border access to data', *Preliminary Report* November 2016

J.A. Espina Ramos, *The European Investigation order and its relationship with other judicial cooperation instruments*, EUCrim 1/2019

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013

Annex - Questionnaires national legal framework

Ireland

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

Information about the respondent

Contact person:	
Organisation, country and position:	An Garda Síochána, Ireland.

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	The criminal legislative provisions are by their nature preventative, with the offences forming the basis for any potential investigation. Investigations are within the remit of An Garda Síochána (Irish Police) and provided for under the Garda Síochána Acts 1924/2005 which empower law enforcement to investigate criminal offences. Prosecution is vested in the Office of the Director of Public Prosecutions which is established by the Prosecution of Offences Act 1974.
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	Criminal offences are outlined in a range of legislative provisions and Acts which are specific to the type of criminality such as Criminal Justice (Theft & Fraud Offences) Act 2001, Child Trafficking & Pornography Act 1998 or the Non-Fatal Offences Against the Person Act 1997. There is no overarching criminal code such as that which exists in the US or Canada. Investigations are carried out by An Garda Síochána under the Garda Síochána Acts as above, and in accordance with both best practice and internal process codes.

3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	The legislative framework requires all actions of Garda members to have a legal and ethical basis based on laws that provide for the search under warrant of places or persons, and the seizure of goods, property or data.
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	Digital evidence is defined as property under property protection laws (Criminal Justice (theft & Fraud Offences) Act 2001 as above) and is similarly defined in the Criminal Justice (Offences relating to Information systems) Act 2017 regarding search and seizure or the prosecution of offences. The general rules of evidence apply to both physical and digital evidence. In addition the courts are mindful of the ACPO guidelines with regards to the handling and seizure of digital evidence.
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	This is very much dependant on the nature of the gathering and sharing. As discussed at 3, a variety of laws govern the gathering of evidence and these are dependent on the offence involved. There is no distinct law governing the analysis of digital evidence as once it is seized under warrant, law enforcement are entitled to examine it for probative or evidential value. Digital evidence can be secured from Service Providers under the Data Protection Act 2018 or the Communications (Retention of Data) Act 2011. Prosecutors are obliged under court precedent to share all evidence with defence parties in a court prosecution, post charging of the suspect.
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	The Department of Justice is empowered, with the assistance of the DPP and the Garda to share digital evidence with requesting competent authorities on foot of a legally sound Mutual Assistance request. Data or digital evidence is not shared between third parties or other agencies where it has been seized under warrant. Intelligence is shared on a case by case basis.
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	The legislation does not define the process for collecting digital evidence. It also does not define what type or form of digital evidence can and cannot be seized or collected except for the Communications (Retention of Data) Act 2011 which lists the type of online data that service providers are required to retain, and which law enforcement can seek to be disclosed. It does define data as outlined above at 4. The collection of data is based on best practice and recognised guidelines such as ACPO.

8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	The Communications (Retention of Data) Act 2011 which lists the type of online data that service providers are required to retain, and which law enforcement can seek to be disclosed. However this is for investigative purposes and not for prevention of crime for which there is no legislative provision.
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	The legislative provisions referenced above provide for the collection of digital evidence under warrant from the courts. In addition the Garda Crime Investigations Techniques manual and best practice guides such as ACPO cover the collection of digital evidence.
10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	Telecommunications messages may be intercepted where it is authorised by order of the Minister for Justice & law reform in accordance with the Interception of Postal Packets and Telecommunications Message (Regulations) Act 1993. The Criminal Justice (Surveillance) Act 2009 provides for the surveillance of persons and communications under court order in criminal investigations.
11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	No.
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	No.
13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	As at 4 & 9 above.

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	As referenced in Section 1 of this questionnaire, Section 6(1)(a) of the Communications (Retention of Data) Act 2011 outlines the powers for An Garda Síochána to request telecommunications data from a service provider where required for the prevention, detection, investigation and prosecution of a serious offence. The 2011 Act provides that Telecoms service providers must retain certain consumer communications data for two years under Section 3 of Act, including data necessary to trace and identify the source, destination, date, time and duration of a communication, as well as the users' communications equipment and the location of mobile communication equipment. The Act does not apply to the content of communications. The Communications (Retention of Data) Act 2011 is available at the following link. http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html This data, processed for law enforcement purposes by An Garda Síochána, must be processed in line with Section 71(1)(f) of the Data Protection Act 2018, which requires that appropriate technical and organizational measures are taken to protect the security of the data and protect against (i) unauthorized or unlawful processing, and (ii) accidental loss, destruction or damage.

	Further to this Section 72 of the 2018 Act requires An Garda Síochána to ensure all persons processing data on behalf of An Garda Síochána are aware of and comply with the relevant technical and organizational measures taken to keep personal data processed for law enforcement purposes secure. Sections 89-95 of the 2018 Act set out all the rights, and restrictions of rights, of data subjects in respect of the processing of their personal data. Where such data is collected for one law enforcement purpose, Section 71(5) of the 2018 Act allows for further processing for a different law enforcement purpose where An Garda Síochána (or another Competent Authority) is authorized to do so under law and the processing is necessary and proportionate to the purpose identified.
2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	Yes, the LED was fully transposed into national law in Ireland via Parts 5 and 6 of the Data Protection Act 2018. Part 5 relates to processing by Competent Authorities and Part 6 relates to the functions of the national supervisory authority within the meaning of, and for the purposes specified in the Directive. No.
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	The Data Protection Act 2018 does not distinguish between processing of digital evidence, as opposed to any other type of evidence, by Members of An Garda Síochána and its provisions apply equally to all types of personal data processing undertaken by An Garda Síochána. The DPU is unable to assist in respect of the operational guidelines, aspect of this question.

4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	No provision requiring SOPs or Codes of Conduct specifically for the preservation of digital evidence, is provided for in national Data Protection legislation.
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	No specific measures are included in the Data Protection Act 2018 governing the preservation and retention of digital evidence. All data processing for law enforcement purposes must be done in accordance with the requirements as set out in response to Question 1 above. Section 71(7) of the 2018 Act also provides that a controller shall ensure, in relation to personal data for which it is responsible, regardless of the form that the data takes, that an appropriate time limit is established for either the erasure of the data, or the carrying out of periodic reviews of the need for the retention of the data.
6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	In addition to the safeguards referenced in response to Question 1 above, An Garda Síochána have defined processes and procedures in place for identity and permissions based access management and associated controls, which includes user and password management in respect of all databases employed by An Garda Síochána in performing its statutory function.
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	As referenced above in response to Question 1, where data is collected for one law enforcement purpose, Section 71(5) allows for further processing for law enforcement purposes where An Garda Síochána is authorized to do so under law. This is subject to the proviso that that the processing is subject to appropriate safeguards for the rights and freedoms of data subjects and that the processing is necessary and proportionate to the purpose identified.
8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	No.

	Processing of personal data for law enforcement purposes is outside of the scope of the GDPR and is governed by the LED, which was transposed into national legislation in Ireland by the Data Protection Act 2018. Section 41 of the Data Protection Act 2018 is directed at, and for the benefit of, 3rd party data controllers and provides an explicit legal basis for the processing of data i.e. provision to An Garda Síochana, when required for the purposes of the detection, prevention, investigation and prosecution of criminal offences. Some difficulties were initially experienced in the months immediately following the coming into effect of the GDPR in respect of 3rd parties being of the misunderstanding that the GDPR prevented them providing information/data to An Garda Síochána when it is investigating criminal offences. This misunderstanding has largely been overcome.

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	The Criminal Justice (Mutual assistance) Act 2008 provides for the collection and exchange of digital or any evidence with a requesting Central authority outside the State.

2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	The Department of Justice is the Central Authority for mutual assistance requests from and to the State. It contains a Mutual Assistance section which is the competent authority for the processing of such requests.
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain.	
3a. Ireland	n/a
3b. Estonia	Yes
3c. France	Yes
3d. Belgium	Yes
3e. Latvia	Yes
3f. Romania	Yes
3g. Northern Ireland	Yes
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the cloud service provider, the data centre and/or the suspect are located in a foreign country or when the physical storage location is unknown and may be abroad?	
5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	DPU Comment – Understand that majority of the provisions in the Cybercrime Convention are provided for in Irish law in particular the Criminal Justice (Offences Relating to Information Systems) Act 2017, which gave effect to an EU Directive on attacks against information systems. The key provisions of the Directive mirror the key provisions of the Cybercrime Convention. The legislation also gives effect to provisions of the Convention relating to offences

	against information systems and their data, and search and seizure powers in relation to such data.
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	DPU Comment – Understand that Ireland opted out of this Directive
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	
8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	
2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	

3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	
6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	Not aware of any existing codes, laws or regulations covering the above.
2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	Not aware of anything which prevents AGS or any CSIRT in this jurisdiction from sharing information. There be an exception with regard to GDPR and personal information. Such exchanges are normally governed by agreed Memorandum of Understanding. None are currently in place that we are aware of.

3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	
5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	
6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	
7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	
8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

Thank you!

Estonia

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

Information about the respondent

Contact person:	
Organisation, country and position:	Prevention and Offences Investigation Bureau Development Department Estonian Police and Border Guard Board

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	Estonia distinguishes between measures for preventive purposes and measures for purposes of investigation and prosecution. Evidence is inadmissible if it does not comprise the necessary elements of evidence set out in subsection 63 (1) of the Code of Criminal procedure.
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	Risk measures stem from the Law Enforcement Act and investigative and prosecution measures are governed by the Code of Criminal Procedure and the Penal Code. The Penal Code provides for the necessary elements of a criminal offence and punishments and the Code of Criminal Procedure lays down the rules for pre-trial procedure and court procedure for criminal offences.
3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	Investigative activities require a legal basis. According to sections 91 and 142 of the Code of Criminal Procedure, a warrant is needed, for instance, for conduct of a search and seizure.

	(You can find English version in Riigi Teataja at https://www.riigitataja.ee/en/eli/518052020007)
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	The Code Criminal Procedure lays down the general conditions of taking of evidence. There is no separate definition of digital evidence in the Code of Criminal Procedure. General conditions set out in the Code apply to both physical as well as digital evidence. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/518052020007/consolide)
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	For taking evidence, distinction is made between physical and digital evidence. Handling digital evidence by the police is governed by guidelines for handling digital evidence and the rules for handling evidence, unless otherwise provided in the above guidelines.
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	Communication of information to security authorities is governed by section 31 of the Security Authorities Act and communication of information by security authorities is governed by section 32 of the same act. Section 210 of the Code of Criminal Procedure states that E-File processing information system is a database maintained for the processing of procedural information and personal data, which enables electronic forwarding of data and documents and section 212 of the same code provides for investigative jurisdiction of pre-trial proceedings and section 213 provides for the role of Prosecutor's Office.
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	Definitions or concepts regarding the collection of digital evidence have not been provided.

8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	Gathering of data for the purpose of crime prevention is governed by the Law Enforcement Act. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/508052020005/consolide)
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	For investigation purposes, digital evidence is gathered based on the Code of Criminal Procedure.
10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	There is no specific legal provision covering lawful interception for investigative purposes in a digital environment. The Code of Criminal Procedure has a general provision (section 126^7 of the Code of Criminal Procedure), which governs wire-tapping or covert observation of information. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/518052020007/consolide)
11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	There is no specific provision covering lawful interception on terminal devices for investigative purposes. The Code of Criminal Procedure has a general provision (section 126^7 of the Code of Criminal Procedure), which governs wire-tapping or covert observation of information. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/518052020007/consolide)
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	There is no specific legal provision.
13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	There is no specific legal provision.

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	With regard to Estonian law, EU is the primary law, including the Charter of Fundamental Rights of the European Union, article 7 of which guarantees inviolability of private life and article 8 protection of personal data. Section 26 of the Constitution of the Republic of Estonia guarantees inviolability of family and private life, which can be restricted in the cases and pursuant to a procedure provided by law. One can interfere with any person's family or private life to protect public health, public morality, public order or to apprehend the offender. According to section 43 of the Constitution of the Republic of Estonia, Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Derogations from this right may be made in the cases and pursuant to a procedure provided by law if they are authorised by a court and if they are necessary to prevent a criminal offence, or to ascertain the truth in a criminal case.
2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	Estonia has implemented Directive (EU) 2016/680 into its national law. Processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties is primarily covered by Chapter 4 of the Personal Data Protection Act (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/523012019001/consolide). The Personal Data Protection Act entered into force on 15 January 2019. Moreover, in the framework of the data protection reform, sectoral legislation, such as the Police and Border Guard Act, the Code of Criminal Procedure, etc. were amended or updated by the Act to Implement Personal Data Protection.
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	The legal framework has a general provision. Subsection 31 (5) of the Code of Criminal Procedure states that A list of the positions in which the officials have the right to participate in criminal proceedings within the limits of competence of an investigative body shall be approved by the heads of the bodies specified in subsection (1) of this section. The Code of Criminal Procedure in force does not lay down the conditions or restrictions for handling information that has been taken over in the course of criminal proceedings or recorded on a data medium, which has been handed

	over to a person conducting proceedings, including searching for evidentiary information and using information in criminal proceedings.
4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	Clause 206 (1) 3) of the Code of Criminal Procedure provides for how to proceed with the physical evidence or objects taken over or subject to confiscation. There are internal guidelines, which give guidance to handling digital evidence, and general rules for handling evidence.
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	Internal guidelines partially govern the issue of the preservation of digital evidence.
6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	There are access restrictions to databases.
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	Collection of digital evidence should be based on sections 9 and 64 of the Code of Criminal Procedure. Evidence is inadmissible if the aforementioned sections are not complied with.
8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	Yes, it generally does. For example, data protection principles (with certain exceptions) and definitions are laid down in the General Data Protection Regulation and Directive 2016/680. In Chapter 4 of the Personal Data Protection Act implementing the directive, terms laid down in Article 4 of the General Data Protection Regulation no. 2016/679 are applied in order to ensure the equivalent use of terms regarding the field of personal data for governing the field connected with the processing of personal data. The definition of the special categories of personal data emanates from Article 9(1) of the General Data Protection Regulation. In addition, Directive 2016/680 defines in Article 3(7) the competent authority, which is law-enforcement authority within the meaning of Chapter 4. In view of the directive, the complexity of different use of terms in national law and the law of the European Union also lies in the fact that procedures of state supervision relating to risk combating do not fall within the scope of the directive according to the national law.

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	Collection of evidence is based on Chapter 19 of the Code of Criminal Procedure – International Cooperation in Criminal Procedure. Police cooperation and information exchange take place through the communications channels of Interpol and Europol and in compliance with their rules and regulations.
2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	Judicial authorities competent to engage in international cooperation in criminal procedure are laid down in section 435 of the Code of Criminal Procedure.
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain Yes, they are. Since the listed countries are EU countries, except for Northern Ireland, which is a part of the United Kingdom, cooperation with these countries takes place pursuant to Division 8 of Chapter 19 of the Code of Criminal Procedure (Cooperation in Criminal Procedure among Member States of European Union).	
3a. Ireland	
3b. Estonia	

3c. France	
3d. Belgium	
3e. Latvia	
3f. Romania	
3g. Northern Ireland	
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the cloud service provider, the data centre and/or the suspect are located in a foreign country or when the physical storage location is unknown and may be abroad?	If a cloud service provider or provider of another service is located in our judicial area despite the fact that their data centre is not in Estonia, we can send an enquiry within the framework of EIO or letter rogatory.
5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	Yes, law on the ratification of the convention was adopted in Estonia on 12.02.03 in full. The provisions of the Convention on Cybercrime have been integrated into Estonian legislation, e.g. Code of Criminal Procedure; Electronic Communications Act – obligation to preserve data, section 111^1; obligation to provide information, section 112.
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	Yes, the directive has been implemented into national law of Estonia in full. The EIO is rather a potentially effective tool.
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	General rules, which are applicable also to digital evidence

8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	In international exchange, there are guidelines for the working process, which are based on the catalogues of the best practice of SPOC and SIS, regulations of Interpol and Europol; also legislation regarding data protection and state secret.

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	Methods of good practice are implemented in the case of which another state authority makes an official enquiry about the requested digital evidence to an authority holding the digital evidence.
2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	Transfer of information is governed by sections 31 and 32 of the Security Authorities Act.
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	Security and Intelligence Agencies follow the Code of Criminal Procedure and the Security Authorities Act.
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	Security and Intelligence Agencies have executive powers.
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	Transfer of information is governed by sections 31 and 32 of the Security Authorities Act. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/503062020002)

6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	Current legislation does not regulate separately the collection, analysis or sharing of digital evidence.

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	
2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	Section 113 of the Electronic Communications Act governs obligation to grant access to communications network. According to this provision, a communications undertaking must grant a surveillance agency or security authority access to the communications network for the conduct of surveillance activities or for the restriction of the right to confidentiality of messages, correspondingly. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/528052020005)
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	Chapter 3 of the Code of Criminal Procedure lays out general conditions for proof and taking of evidence, which govern, inter alia, the collection of digital evidence. If the internet service provided is located in a foreign country, an application is submitted on the basis of EIO or MLAT to a respective foreign country for execution.
5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	

6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	Chapter 3^1 of the Code of Criminal Procedure lays down general conditions for conduct of surveillance activities. Section 126^2 of the Code of Criminal Procedure provides for the bases for conduct of surveillance activities, and the grant of permission for surveillance activities is governed by section 126^4 of the Code of Criminal Procedure. Section 126^5 of the Code of Criminal Procedure provides for covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things; section 126^7 provides for wire-tapping or covert observation of information; section 126^9 provides for the use of police agents and section 126^8 staging of criminal offence. Surveillance activities are conducted both directly through the institution specified in subsection 1262 (1) of the Code of Criminal Procedure as well as the institutions, subordinate units and employees administered by them and authorised to conduct surveillance activities, and through police agents, undercover agents and persons recruited for secret cooperation. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee//en/eli/518052020007)
7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	Sections 126^7 and 126^5 of the Code of Criminal Procedure establish a procedure for the wire-tapping or covert observation of information and covert surveillance.
8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	Section 113 of the Electronic Communications Act governs granting access to communications network. (You can find English version in Riigi Teataja at https://www.riigiteataja.ee/en/eli/528052020005)

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

Thank you!

France

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

Information about the respondent

Contact person:	
Organisation, country and position:	

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	Yes. The French Legal system provides for a strict distinction. This distinction is mainly based on the aim of each operation, creating a virtual frontier between "administrative police operation" and "judicial police operation". This distinction implies the two jurisdictional competences of the French legal system, the administrative and the judicial one. The administrative competence defines preventive police operations. The judicial competence regards criminal prosecution. The principle (*Conseil Constitutionnel* - Constitutional Council) is that preventive operations should not be carried out for criminal prosecution, and vice-versa (*Conseil constitutionnel* - Decision *n°2015-713 du 23 juillet 2015 DC and CC Décision n°2005-532 du 19 July 2006, based on the French Déclaration des droits de l'homme et du citoyen* (Declaration of Human and Citizen Rights) *-1789, article 2, 16, and on the article 66 of the French constitutional law -4 octobre 1958*). When criminal offenses are detected, police officers have to use the procedure of the article 40 of *Code de procedure pénale* (CPP) to denounce the offense to the judicial authority (criminal prosecutor).

	Therefore, if a service wants to use administrative type of data as evidence, it has to collect it following the judicial procedures. This guarantees the collected pieces of evidence to have judicial value.
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	The main codes governing police measures are CSI - "*Code de la sécurité interieure*" (Interieur Security Code), for the preventive measures, *Code penal* (Penal Code) *and* CPP for the investigative measures. Even though the operations are also governed by constitutional principles, and transpositions of European directives. For example, directive ° 2016/680 of April 27, 2016 is transposed in chapter XIII of the "*Loi informatique et libertés*" LIL (Data Protection Act), governing the establishment and use of automated processing of personal data.
3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	The legal system requires a legal basis for all investigative measures, but not specifically a warrant ("warrant" in the French system has not the same meaning of the "Anglo-Saxon" one). Each action, operation, search or seizure has to have a legal basis and to be guided by the legal principles of the corresponding legal framework. It depends on the measure and type of investigations. The French CPP defines three main types of judicial procedures : *« Enquête préliminaire"* (Preliminary investigation - Art 75 to 78 CPP), "*Enquête de flagrance"* (Flagrant investigation/expedited investigation - Art 53 to 73 CPP), commission rogatoire (Letter rogatory - Art 151 and following from CPP). For the "*preliminaire*" and "*flagrance*" procedures, the criminal prosecutor leads the investigations. The police officers have often to ask prosecutor in charge permissions to carry out some intrusive measures (such as special investigative measures in the fight against organized crime ...). Some of the measures have to be decided by a judge (*Juge des libertés et de la detention* – Liberty and custody judge). For example, in a preliminary investigation, the police officers have to ask for a permission, delivered by a judge to proceed to a search and seizure <u>if the owner disagrees.</u> Concerning prevention measures, the actions (data gathering, analyzing…) have to be carried out in a legal framework. Intelligence services are legally authorized to carry out some methods which go against the protection of

	privacy. It is possible, if these operations, actions, are led in the legal framework of the Art L801-1 and following of CSI*: "Respect for private life, in all its components, in particular the secrecy of correspondence, the protection of personal data and the inviolability of the home, is guaranteed by law. The public authority may only interfere with it in the sole cases of necessity of public interest provided for by law, within the limits set by the latter and in compliance with the principle of proportionality."* So it has to be: - Legal (procedures of title II Livre VIII CSI) - Carried out by the competent services - In the exercise of the missions entrusted to them (Art L811-2 and L811-4 CSI) - Justified by the prevention of threats legally specified in article L811-3 - The infringements which they cause to respect for private life are proportionate to the grounds invoked. This is controlled by an independent administrative authority (*Commission nationale de controle des techniques de renseignement* - National Commission for the Control of Intelligence Techniques). There is also a hierarchical control, a parliamentary control (specific commission) and a jurisdictional control (specific form of the *Conseil d'Etat*, the French highest administrative court).
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	Not really. First, the general rules governing pieces of evidence during a judicial trial are in the preliminary article, article 427 and subsequent, and article 173 of CPP. Article 427 precises that "*Except in cases where the law provides otherwise, the offenses can be established by any mode of evidence and the judge decides on his own conviction. The judge can only base his decision on evidence brought to him during the proceedings and contradictorily discussed before him."* **A public authority cannot bring an evidence if police officers collected it by an illegal or disloyal measure.** *Main decisions:* *Crim. 12 juin 1952, Imbert* *Crim. 9 oct. 1980, Tournet*

	Crim. 23 juill. 1992, Mlle X… et autres *Crim. 6 avr. 1993, J.-L. T…* *Crim. 11 juin 2002, Dhaisne, Jacinto et Labradero* Second, certain laws have been specifically enacted to guide the functioning of the justice system in collecting and analyzing digital evidence. So, the answer depends on what is considered as digital evidence: 1 - First, an information **becomes digital evidence** by being gathered as part of the general investigations and integrated into an automated data processing system: the legal framework is that of the investigation framework, then that of automated data processing (analyzing framework). See question number 5 about that. 2 –Second, **digital proof of a multimedia medium seized during a search** (large sense) localized on the national territory: - Enquete de flagrance: see the articles 56, 57, 57-1 (concerning access to a computer during a search by example), 59, 60, 60-3 CPP - Enquete préliminaire 76, 76-3, 77-1 du CPP - Commission rogatoire : 81, 94, 95, 97, 97-1 et 99-5 du CPP In this case, a judicial police officer can realize a copy of the data (to protect the integrity of the original data as a proof), and/or exploit the digital evidence on a place of search. The owner of the system has to be present or the officer has to require two witnesses. He may also ask a specialist of his unit to exploit the data, or requires a qualified person to do this. These operations can be carried out at the police station in the same way. The copy of the data seized can be analyzed by specialists: a judicial expert can also be required to do this (Art 156 to 169-1 CPP).

	The information extracted, and interesting the investigations can be inserted in an automated data processing system (see question 5). <u>3 – Third,</u> digital proof in a remote system: - Requisitions (Art 60-1, 77-1-1 and 99-3 CPP) in order to receive documents or information from a digital system, or a data processing system. - Requisitions (art 60-2 al 1, 77-1-2 and 99-4 CPP) in order to be made available to the information contained in a computer system (limited to information useful for the manifestation of the truth) - Requisitions to kept information consulted on the internet (Art 60-2 al2, 77-1-2 al2, 99-4 al2) - Interception of correspondence sent by electronic communication (Art 100 al.2, 100-1, 100-3 to 100-7, 706-95, 74-2 du CPP, and art. 32 du *code des postes et communications electroniques* (Postal and electronic communications code). On this question, see the decree 2014-1162 du 9 October 2014 concerning the *"plateforme nationale des interceptions judiciaires* (PNIJ) (National judiciary interceptions platform), and answer to question 13. - Access to stored correspondence (Art 706-73 and 706-73-1, 706-95-1, 706-95-2 CPP- available for fighting major crimes and organized crime) retrieve remotely and without the knowledge of the person concerned the electronic correspondence stored and accessible by means of a computer identifier - Distant search and seize: Art 57-1 CPP, authorized to access and collect "data accessible from the initial system" located in France even if the computer system that stores them is located outside the territory. Then, legal framework is the search and seize a general one. - Exploitation of data stored remotely: On this subject, (*Crim., 16 November 2013, n° 12-87.130*). If police officers know exactly where

	data are located, they have to use penal international instruments (*Convention of Budapest art.32*), if data are not public, or if they a have no authorization of the legal owner. As they relate to a particular investigation, all copies of the data exploited must be attached to the physical procedure or destroyed after the mission ended (see the decisions of the French "*Cour de Cassation*" (Court of Cassation): *Crim., 8 Juillet 2015, 15-81.731 et Crim., 21 Juin 2016, n° 16-80126*).
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	Gathering: *CPP* (judicial) *CSI* (preventive), LIL (personal data), Analyze: *CPP* : - *Logiciels de rapprochements* : Livre I, Titre IV, Chap III (art 230-20 and subsequent – Art R40-39 à R40-41 CPP) o *Logiciels d'analyse criminelle - Décret 2012-687 du 7 mai 2012* - *Bases et analyse sérielle : CPP Livre I, Titre IV, Chapt II, Section 2 "Des fichiers d'analyse sérielle", article 230-12 CPP and following.* - *Fichiers de Police (*Police automated databases for DNA, biometric data, criminal record…etc.*).* Sharing: - Forbidden by article 11 of the CPP (Principle: investigations are covered by secrecy unless otherwise provided by law) - Allowed by : - Art 695-9-31 du *CPP* (Refering framework decision 2006/960/JAI Conseil du 18 décembre 2006), it concerns "information" - Art L 235-1 CSI (it concerns data from personal data processing files, if allowed by an international engagement) - "*Décret no 2014-187 du 20 février 2014 relatif à la mise en oeuvre de traitements de diffusion de l'information opérationnelle au sein des*

	services et unites de la police et de la gendarmerie nationale". Refered to Art 695-9-49 *CPP*). - Police automated data processing decree
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	*Code de la sécurité intérieure - Code de procedure pénale* (Art 40 for everything, 706-25-2 for the terrorist offenses) for sharing /exchanging data between competent authorities, judicial authorities, and some Intelligence agencies. Concerning third-party, data owners, etc., it depends on the "procedural statute" of the data owner. It can be a required person, (see requisition of question 5), a witness (general legal framework of the proof, if a witness or a third person gives some evidence to a police officer). CSIRTs have to be competent authorities, private persons (third party, victims, witnesses, required person…), or intelligence agencies. Then, the corresponding legal framework applies.
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	Digital evidence can be gathered and analyzed by investigators (general framework of the CPP, art.57-1), a qualified person (art 60 CPP), or an expert (art 81 du CPP, persons registered by the Court of appeal, art 157 CPP).
8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	Loi "*Informatique et libertés*" (LIL) of 6 January 1978, Chapter XIII (transposing the directive 2016/680) and *Code de la sécurité intérieure*
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	*Code de procedure penale*
10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	Yes. Called "special investigative measures", theses legal provision are contained in the CPP (Livre I – Titre IV / Livre IV- Titre XXV- Chapt II – Section 1 à 9 – Articles 706-73 to 706-106;).

11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	*Code de procedure penale* : - Art 100-1 and following - art 706-95-1 and following for stocked "mail" access - Art 57-1, exploiting data registered (stocked) on the national territory (on that subject decision of French "*Cour de Cassation*" Crim.16 November 2013, n° 12-87.130, validating gathering of data stocked out of the territory by judicial police officers as investigations (criminal file) - Budapest's convention (2001, 13 November)
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	All automated data processing software has to be declared and subjected to an impact assessment (*Loi informatique et liberté of 6 January 1978*). It has to be used for a specific purpose: preventive measures (administrative framework) or repressive measures (judicial framework). <u>It cannot be used for both purposes.</u> <u>If it is used for repressive measures (judicial framework), it has to be allowed by a national decree (called "*decret pris en Conseil d'Etat*").</u>
13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	The legal framework is the general framework of judicial evidence. All computer media and their content can be seized and analyzed, if they contain data relevant to the current investigation. Data have to be copied on another computer media (work copy) to be analyzed without modifying or compromising the data initially seized (Art 57-1 CPP). Judicial interceptions are gathered through the "*Plateforme Nationale d'interception judiciaire*' (National platform for judicial interception) (PNIJ art 230-45 and follow). It is a specific framework, where data are extracted, analyzed, and conserved by the "platform". When the investigations are finished, the file is closed and data is held in a numeric judicial seal.

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	Yes. See questions 3, 4, 5 of the first section.
2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	Yes, the law « *Loi Informatique et Libertés (6 January 1978)* » has been modified. The Chapter 13 of this law was created and devoted to the transposed provisions of the directive. An independent administrative authority is still to be in charge of this law (*Commission nationale informatique et libertés* - CNIL). This authority receives declaration, impact assessments, and is able to control the good or bad use of automated data processing (purposes, the security of access, sensitive information uses, etc…). Information collected for preventive purposes cannot be directly, and automatically, used by other automated data processing for another purpose. Same answer as question 12 section 1: "All automated data processing software have to be declared and subjected to an impact assessment (Loi *informatique et liberté of 6 January 1978*). It has to be used for a specific purpose: preventive measures (administrative framework) or repressive measures (judicial framework). It cannot be used for both purposes.

	If it is used for repressive measures (judicial framework), it has to be allowed by a national decree (called "*decret pris en Conseil d'Etat*")."
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	No difference between the general framework of evidence, and the framework of digital evidence. The national framework determines operational guidelines (see answer to question 4 section 1). Who is authorized to process digital evidence: - Judicial police officer - Police specialist (technical assistance, if an agent is member of the same police unit or member of a specialized service jointly responsible to the investigation) - Qualified person (to realize a copy, to exploit data) Art 60 CPP - Judicial experts (Art 156 and following from CPP) Digital evidences cannot be used for another purpose, except of opening a new case, and except of sharing information allowed by the law (Art CPP). On this question, see question 7 section 3, question 1 section 4.
4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	Original data are cloned to protect their integrity (Art 60-3, Art 77-1-3, Art 99-5 CPP. A copy will be exploited by investigators.
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	Evidence seized = general legal framework (criminal prosecutor is responsible until a decision from the Court art 41-4 CPP. He can destroy it after 6 months without return request). On this subject, see the end of question 4 section 1. Information extracted from evidence seized: - If they are used in an automatic data processing called "*logiciels d'analyse criminelle*" (criminal analysis processing of the question 5 Section 1), the data are attached to the file, so all evidence is jointed to the physical procedure, other data are destroyed. - If data are inserted in a legal automatic data processing (cross-checking…) the information is conserved through the legal framework of each data processing.

6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	All databases accesses are restricted (Strong authentification). The connections are traced and controlled regularly.
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	Yes. See question 1, 3, 4, 12 of section 1 and questions 1, 2, 5, 6 of section 2. But if other offenses are detected during the investigations, a new case (a different one) is open with the data or evidence attached to this new case.
8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	Gathering, analyzing and sharing data by police services is not directly impacted by GDPR. But we could imagine that these activities could be indirectly impacted. - A good impact may be a better quality of the data; - GDPR has a great impact on the data processing regulation in UE. Data processing owner are of automated data systems are encouraged to keep personal data as short as possible, to anonymize or pseudonymize it, etc. If it is a good thing because of all criminal uses of stolen personal data, it could have a perverse effect: the more time passes, the less data is available for investigations. For example, some companies remove links between payment Card number and other personal data after a few months…When the police is working on fraud cases (often discovered after several months) it could be more difficult to collect useful information.

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	*Code de procedure penale Titre X* (Art 694 and subsq).
2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	Criminal prosecutor (or "*Juge d'instruction*"), investigators (police officers)
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain.	
3a. Ireland	NB : Ireland has not ratified the Cybercrime Convention.
3b. Estonia	
3c. France	
3d. Belgium	
3e. Latvia	
3f. Romania	
3g. Northern Ireland	
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the cloud service provider, the data centre and/or the suspect are located in a foreign country or when the physical storage location is unknown and may be abroad?	See question 4 section 1, "Third".

5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	The convention has been implemented by the *loi n° 2005-493 du 19 mai 2005 autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.* Before this parliamentary approval, the public authorities had already incorporated into national law most of the stipulations of the convention. The following laws can be cited : - *loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* (article 40 – payment fraud); - *loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure* (articles 16 to 20); - *loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*; - *loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	Yes, the directive has been implemented into French law by the following texts: - *loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (article 118);* - *ordonnance n° 2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale;* - *décret n° 2017-511 du 7 avril 2017 relatif à la décision d'enquête européenne en matière pénale.*
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	The general legal framework (Code of Criminal Procedure Title X, art 694 and subsequent) provides for the exchange of information or intelligence (apart from specific international convention) between French judicial authorities and foreign authorities, by adapting the 2006 framework decision / 960 / JHA of the Council of 18 December 2006 "(see art 694-15 et seq. Concerning" European investigation order "- Directive 2014/41 / EU of 3 April 2014)

	Articles 695-2 and subsequent offer the possibility of creating a "joint investigation team" between France and other states.
8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	See question 7.

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	As explained in question 4 section 1, data becomes evidence since a seizure, since it comes in a criminal procedure. 1 - From administrative authorities to judicial ones: An administrative authority can give to the judicial one some data, intelligence report or some information, by using the procedure of the art 40 CPP. The authority doesn't give all the data but only the information allowing to discover a criminal offense, and identify the criminals. If the judicial authority/LEA's needs information and knows that an administrative one have them, there will be a request with a "judicial requisition" 2 - From judicial authorities to an administrative one:

	Forbidden by the article 11 of the Code de procedure pénale (Principle: investigations are covered by secrecy unless otherwise provided by law) Allowed by: - 706-25-2 CPP for terrorist offenses - "Décret no 2014-187 du 20 février 2014 *relatif à la mise en oeuvre de traitements de diffusion de l'information opérationnelle au sein des services et unites de la police et de la gendarmerie nationale*". Refered to Art 695-9-49 Code de procedure penale). - Police automated data processing decree 3- Mutual exchanges: to fight more efficiently some offenses, some specific legal frameworks allow authorities to exchange information, intelligence or documents to detect these offenses (especially public finance frauds).
2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	Intelligence Agencies can share information with judicial authorities: criminal prosecutor (Art 40 CPP). They could share some information with LEA's if they're not covered by National secret. If LEA's needs information, they have to request it by "judicial requisition".
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	*Code de la sécurité intérieure*
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	Arrests cannot be made by intelligence services (it is possible only for police services). They can search, and use some intrusive technics (Livre VIII, *Code de la sécurité interieure*).
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	Yes. See question 2.

6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	Intelligence services cannot collect digital evidence from criminal proceedings. They can access certain databases with limited prerogatives (for example the criminal record). They cannot access criminal cases and evidences, except for terrorist offenses cases but they can just receive information given by judicial authority (see question 4 section 1, "second").

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	There is no specific law. It depends on the statute of CSIRT's (public, private, administrative, judicial…).
2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	Private CSIRT's could share some information for the prevention, during investigation and prosecution. Police can request them by a judicial requisition (criminal prosecution). For prevention, LEAs can insert the information in their intelligence collection.
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	*Code des postes et communications electroniques*, *Code de procédure pénale, Code de la securité intérieure*.
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	See question 4 section 1.
5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	Yes, see question 4 section 1.

6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	Except for the observation of the public internet, to be able to use this kind of technique during criminal investigations, officers must be specifically trained and empowered (Art 230-46, art 706-87-1 du CPP)
7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	Prevention: Available to Intelligence services (Livre VIII *Code de la sécurité intérieure*) only for prevention of threats specified in Art 811-3 CSI. Investigations / Prosecution : See question 6 .
8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	Prevention Livre VIII *Code de la sécurité interieure* Investigation/ Prosecution : *Code de procédure pénale* (judicial requisition, see question 4, section 1, Third.

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

Thank you!

Belgium

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

Information about the respondent

Contact person:	
Organisation, country and position:	Commissioner, Federal Police, Belgium

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	No strict distinction No
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	Law on the Police Function (Aug 5, 1992) (= Wet op het Politieambt) Code of Criminal Procedure (Nov 17, 1808) (= Wetboek van Strafvordering). Penal Code (June 8, 1867) (= Strafwetboek)
3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	Yes
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	No distinction, general rules on seizures are applicable to digital evidence. See art 39 bis §1er Belgian Code of Criminal Procedure (Art. 39bis. § 1er. Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures

	consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.)
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	Code of Criminal Procedure (Nov 17, 1808) (= Wetboek van Strafvordering)
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	No specific laws or regulations
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	There are no legal definitions in Belgian criminal law. Some of the important concepts have been explained in the explanatory memorandum to the Law concerning digital criminality (Nov 28, 2000). (= Wet inzake informatiecriminaliteit).
8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	An official report (proces-verbaal) is made describing the gathering of information and the inventory of all information gathered. All evidence is deposited at the registry of the court.
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	Articles 39bis, 39ter, 39quater, 46bis, 88bis, 88ter, 90ter-90decies of the Criminal Procedure Code.
10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	Articles 90ter to 90decies of the Criminal Procedure Code.
11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	Articles 90ter to 90decies of the Criminal Procedure Code.
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	Articles 39bis and 88ter of the Criminal Procedure Code cover the “open” search in a computer system, while articles 90ter to 90decies relate to the “covert” search in a computer system.

13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	An official report (proces-verbaal) is made describing the gathering of information and the inventory of all information gathered. All evidence is deposited at the registry of the court. A forensic backup can be made by specialized team (Computer Crime Unit) and this backup is treated as other evidence. Article 39bis of the Criminal Procedure Code covers the seizure of digital evidence in criminal procedures.

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	The act of 29 May 2016 regulates the retention and storage by electronic network providers and service providers of data generated by electronic communication. (Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques). The relevant rules are integrated in the Belgian code of criminal procedure. It applies and precises the proportionality principle appreciated by judicial authorities in charge of the investigation. The categories of data accessible for Belgian LEA are circonscribed, the modalities of access with prior autorisation of the juge in charge of the investigation. The processing is evaluated taking into account the gravity of the offence. Belgian code of criminal procedure: art. 90 ter to 90 decies regulating, telephone tapping, the analysis, the interception and recording of communication not accessible for the public or of data from a IT system of a part of it. In particularly, they provide conditions for judicial authorities to interfere in private communication. The system of fundamental rights does not impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes.

2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	Yes, the directive was implemented in BE by Data Protection Law (Loi du 30/07/2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel) and the Police Act 05/08/1992 was revised in order to comply with the new data protection rules see article 44/1-44/11/13. Regarding biometric data, additional safeguards are provided than those established in the Police-justice directive. The drafting of some implementing rules on those legislations is still ongoing.
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	Yes, processing most of digital evidence requires the prior authorisation of the Juge or the Public prosecutor in charge of the investigation. In reality, according Belgian Law it does not depend on the form of data (digital or not) but categories of data and where evidence is located.
4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	No
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	No specific rules, general rules applicable
6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	General rules for access applicable in handling of information
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	General rules for access applicable in handling of information
8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	Not yet observed till now

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	National legislation implementing the European Investigation Orders (EIO) in criminal matters: Law of 22 May 2017. In relation to third countries, international conventions (MLA, Budapest convention) are applicable.
2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	Only the public prosecutor or the investigative judge, depending on the stage of proceedings and on the nature of the investigative measure concerned, may request or authorise crossborder transfer of digital evidence.
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain.	
3a. Ireland	YES: MLA conventions
3b. Estonia	YES: EIO
3c. France	YES: EIO
3d. Belgium	/
3e. Latvia	YES: EIO
3f. Romania	YES: EIO

3g. Northern Ireland	YES: EIO until end of December 2020 (end of Brexit transitional period), afterwards Budapest Cybercrime Convention
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the cloud service provider, the data centre and/or the suspect are located in a foreign country or when the physical storage location is unknown and may be abroad?	Belgian Code of Criminal Procedure (Art. 88ter and 90ter), on the prerequisite that the service provider is offering services on the Belgian soil. In addition to this direct cooperation with service providers, the possibility to conduct a search in stored computer data is also implemented in the Belgian legislation on the basis of Art. 88ter of the Code of Criminal Procedure.
5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	Belgium has ratified the Cybercrime Convention on 20/08/2012. It has been fully implemented in our national law, first of all by the law of 28 November 2000 on digital criminality, and later laws that have modified certain articles of the Penal Code and the Criminal Procedure Code in order to be fully in line with the Convention.
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	Yes, the directive has been implemented into national legislation by the law of 22 May 2017. The EIO is definitely an effective tool. Nevertheless, in this regard, it should be emphasised that there is still room for improvement when it comes to more efficient cooperation between Member states regarding digital evidence. A more swift transmission of information or data as envisaged in the draft EU e-evidence regulation, could be an important step in this direction.
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	General rules are applicable to the transfer of digital evidence.
8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	Law of 9 December 2004 regulates the crossborder exchange of information between law enforcement services for criminal purposes (implementation of the EU Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the MS of the EU).

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	An agreement for the exchange of information between LEA and security agencies exists, for the State Security (Sûreté de l'Etat) and the ADIV (Military Security). The transmission of classified information is part of the Law of 11 December 1998 on the classification of security habilitations, security certificates and security recommendations. Finally, the transmission of classified information, transmitted by the judicial authorities is described in the Letter of the Prosecutor General's Office COL 11/2005.
2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	
6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	
2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	For prevention purposes, LEA can share information with CSIRT when the classification of the information allows this sharing with 3rd parties. In criminal investigations information is shared when the CSIRT has been appointed as criminal expert by the Public Prosecutor's Office
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	Article 39ter of the Criminal Procedure Code (freezing of data). Articles 90ter to 90decies of the Criminal Procedure Code (interception of data).
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	Article 39quater of the Criminal Procedure Code (freezing of data in a foreign country).
5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	Yes. Article 39bis of the Criminal Procedure Code (seizing of data).
6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	Observation (both on- and offline): Article 47sexies of the Criminal Procedure Code. Infiltration: Article 46sexies of the Criminal Procedure Code. Only specific LEA services/personnel are authorised to perform this (defined in Royal Decree dd 19/11/2018). Search & seizure: Article 39bis of the Criminal Procedure Code.

7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	Digital search and seizure for investigation and prosecution: Articles 46bis, 88bis and 90ter of the Criminal Procedure Code. Article 126/1 of the Electronic Communications Act.
8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	Articles 88quater of the Criminal Procedure Code (cooperation obligation).

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

Thank you!

Latvia

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

Information about the respondent

Contact person:	
Organisation, country and position:	State police of Latvia, chef expert, State police of Latvia, head of unit

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	Yes. Investigation is regulated by Criminal Procedure Law, preventative actions are regulated by Operational Activities Law. https://likumi.lv/ta/en/en/id/57573 Paragraph 3 of Section 127 of Criminal Procedure Law states that information regarding facts acquired in operational activities measures, and information that has been recorded with the assistance of technical means, shall be used as evidence only if it is possible to examine such information in accordance with the procedures laid down in Criminal Procedure Law.
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	Investigation is regulated by Criminal Procedure Law (https://likumi.lv/ta/en/id/107820-criminal-procedure-law), preventative actions are regulated by Operational Activities Law (https://likumi.lv/ta/en/en/id/57573).
3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	Criminal Procedure Law Section 212. Permission for the Performance of Special Investigative Actions

	(1) Special investigative actions shall be performed on the basis of a decision of an investigating judge, except in cases determined in this Chapter. (2) A decision of an investigating judge shall not be necessary if all the persons who will work or live in the publicly inaccessible location during the performance of a special investigative action agree to the performance of such operation. (3) Within the meaning of this Chapter, locations that one may not enter, or wherein one may not remain, without the consent of the owner, possessor, or user are publicly inaccessible. (4) In emergency cases, the person directing the proceedings may commence special investigative actions by receiving the consent of a prosecutor, and, not later than on the next working day, a decision of an investigating judge. **Search and seizure** **Section 180. Decision on a Search** (1) A search shall be conducted with a decision of an investigating judge or a court decision. An investigating judge shall take a decision based on a proposal of the person directing the proceedings and materials attached thereto. (2) The decision on a search shall indicate who will search and remove, where, with whom, in what case, and the objects and documents that will be sought and withdrawn. (3) In emergency cases where, due to a delay, sought objects or documents may be destroyed, hidden, or damaged, or a person being sought may escape, a search shall be performed with a decision of the person directing the proceedings. If a decision is taken by an investigator then a search shall be performed with the consent of a prosecutor. (4) A decision on a search shall not be necessary in conducting a search of a person to be detained, as well as in the case determined in Section 182, Paragraph five of this Law. (5) The person directing the proceedings shall inform an investigating judge of the search indicated in Paragraph three of this Section not later than on the next working day after conducting thereof, presenting the materials that

	justified the necessity and emergency of the investigative action, as well as the minutes of the investigative action. The judge shall examine the legality and validity of the search. If the investigative action has been conducted illegally, the investigating judge shall recognise the acquired evidence as inadmissible in criminal proceedings, and shall decide on the actions with the withdrawn objects.
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	Criminal Procedure Law Section 134. Material Evidence (1) Material evidence in criminal proceedings may be anything that was used as an object for committing a criminal offence, or that has preserved traces of a criminal offence, or contains information in any other way regarding facts and is usable in proving. The same thing may be a material evidence in several criminal proceedings. (2) If a thing is to be used in proving in connection with the thematic information included therein, such thing shall be considered not as material evidence, but rather as a document. Criminal Procedure Law Section 136. Electronic Evidence Evidence in criminal proceedings may be information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems. **Section 136. Electronic Evidence** Evidence in criminal proceedings may be information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems. In Latvia we don't have separate rules for digital evidence gathering, analysing and sharing. We apply general evidence rules designed for physical evidence.
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	Law On Forensic Experts - https://likumi.lv/ta/en/en/id/280576-law-on-forensic-experts

	Criminal Procedure Law - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law Administrative Procedure Law - https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law Civil Procedure Law - https://likumi.lv/ta/en/en/id/50500-civil-procedure-law On Police - https://likumi.lv/ta/en/en/id/67957-on-police
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	In Latvia we don't have separate regulations for it.
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	Definitions of types of data can be found in Electronic Communications Law. https://likumi.lv/ta/en/en/id/96611
8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	In Latvia we don't have separate regulations for it.
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	Criminal Procedure Law Chapter 10 *Investigative Actions* regulating the collection of evidence - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	Operational Activities Law - https://likumi.lv/ta/en/en/id/57573-operational-activities-law Criminal Procedure Law Chapter 11 *Special Investigative Actions* regulating the lawful interception for investigative purposes in a digital environment - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law

11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	Criminal Procedure Law chapter 11 Special Investigative Actions. **Section 218. Control of Means of Communication** (1) The control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation. (2) The control of telephones and other means of communication with the written consent of a member of a conversation, or the sender or recipient of information, shall be performed if there are grounds to believe that a criminal offence may be directed against such persons or the immediate family thereof, or also if such person is involved or may be enlisted in the committing of a criminal offence. **Section 219. Control of Data Located in an Automated Data Processing System** (1) The search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the information of the owner, possessor, or maintainer of such system or data shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the information located in the specific system may contain information regarding facts included in circumstances to be proven. (2) If there are grounds to believe that sought data (information) is being stored in a system, located in another territory of Latvia, that may be accessed in an authorised manner by using the system referred to in a decision of an investigating judge, a new decision shall not be necessary. (3) The person directing the proceedings may request, for the commencement of an investigative action, that the person who oversees the functioning of a system or fulfils duties related to data processing, storage or transmission provide the necessary information, ensure the completeness of the information and technical resources present in the system and make the data to be controlled unavailable to other users. The person directing the

	proceedings may prohibit such person to perform other actions with data subject to control, as well as shall notify such person of the non-disclosure of an investigative secret. (4) In a decision on control of data present in an automated data processing system an investigating judge may allow the person directing the proceedings to remove or store otherwise the resources of an automated data processing system, as well as to make copies of these resources. **Section 220. Control of the Content of Transmitted Data** The interception, collection and recording of data transmitted with the assistance of an automated data processing system using communication devices located in the territory of Latvia (hereinafter - the control of transmitted data) without the information of the owner, possessor, or maintainer of such system shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the information obtained from data transmission may contain information regarding facts included in circumstances to be proven.
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	There are no such norms in the Criminal Procedure Law, general norms are applicable.
13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	Criminal Procedure Law Chapter 10 *Investigative Actions regulating the collection of evidence* - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law Section 179. Searches (1) A search is an investigative action whose content is the search by force of premises, terrain, vehicles, and individual persons for the purpose of finding and removing the object being sought, if there are reasonable grounds to believe that the object being sought is located in the site of the search. (2) A search shall be conducted for the purpose of finding objects, documents, corpses, or persons being sought that are significant in criminal proceedings.

	Section 186. Withdrawal Withdrawal is an investigative action whose content is the removal of objects or documents significant to a case, if the performer of the investigative action knows where or by whom the specific object or document is located and a search for such object or document is not necessary, or such object or document is located in a publicly accessible place.

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	**Electronic Communications Law** https://likumi.lv/ta/en/en/id/96611-electronic-communications-law Section 68. Data Confidentiality (1) An electronic communications merchant has the obligation not to disclose information regarding users or subscribers without the permission of the user or subscriber, as well as information regarding the electronic communications services or value added services received by them, except when such information is necessary for the authorities referred to in Section 70, Paragraphs eight, 8.1 and nine of this Law, as well as for the institutions specified in Section 71.1, Paragraph one of this Law for the performance of the functions laid down in laws and regulations, and for the purposes referred to in Sections 71.2 and 71.3. (2) An electronic communications merchant is prohibited to disclose information, without the consent of a user or subscriber, which he or she transmits or which is transmitted in providing electronic communications services to users or subscribers, except in the cases if such information is necessary for the performance of the functions laid down in laws and

	regulations of the institutions determined in Section 71.1, Paragraph one of this Law and for the purposes referred to in Section 71.2. Section 71.1 Use and Processing of Data to be Retained (1) Data to be retained shall be retained and transferred to pre-trial investigation institutions, bodies performing operational activities, State security institutions, the Prosecution Office and the court in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings, as well as to the Competition Council for investigating violations of the competition law which manifests as restrictive agreements. Information regarding the given name, surname, personal identity number or name, registration number, address, user ID, telephone number and location of such subscriber or registered user to whom Internet protocol (IP) address has been assigned during the connection shall be stored and transferred to the State Police to ensure the protection of the rights and legal interests of the persons offended in the electronic environment within cases regarding the physical and emotional abuse of a child. (2) An electronic communications merchant shall ensure the retention of retained data in such volume as they are acquired or processed in providing electronic communications services, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in this Law. The electronic communications merchant does not have an obligation to perform additional measures to acquire the data to be retained if in providing electronic communications services, the technical equipment of the merchant does not generate, process and register such data. (3) An electronic communications merchant shall ensure the transfer of data to be retained to the authorities referred to in Paragraph one of this Section on the basis of a request therefrom. (4) The Cabinet shall determine the procedures for the requesting by and transfer of data to be retained to the authorities referred to in Paragraph one of this Section.

	(5) The Data State Inspection according to the procedures and in the volume stipulated by the Cabinet shall once per year compile statistical information regarding the requests to receive data to be retained from the authorities referred to in Paragraph one of this Section and regarding the issuing of such data. (6) An electronic communications merchant does not have the right to disclose information regarding the fact that data to be retained has been requested by or transferred to the authorities referred to in Paragraph one of this Section, as well as information regarding users or subscribers in relation to whom data to be retained has been requested or transferred, except in the cases laid down in laws and regulations. (7) Processing of data to be retained may be performed only by an authorised person of the electronic communications merchant. (8) Data to be retained shall be extinguished at the end of the time period specified in Section 19, Paragraph one, Clause 11 of this Law, except for the data, which the authorities referred to in Paragraph one of this Section have requested up to the end of the time period for the retention of data, but which have not yet been issued, as well as data, which is necessary for the provision of further services, payment accounting for services provided, the examination of claims, recovery of payments or ensuring interconnections. Detailed regulation mentioned in the **Law On Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceedings** https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa In this law is mentioned necessary safeguards to be taken when gathering and analysing digital personal data in the investigation of crimes.
2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the	Directive (EU) 2016/680 was fully transposed into the Law On Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceedings, and the Law does not provide higher safeguards than those established in the Directive.

execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	**Law On Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceedings** https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	In criminal proceedings, evidence may be processed only by those authorities whose officials (for instance police officers, prosecutors etc.) are entitled to conduct the criminal proceedings regarding to law On Processing of Personal Data in the Criminal Procedure and Administrative Violation Proceeding (https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa).
4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	We are not aware that there are legal norms in Latvian regulatory enactments that would regulate how long digital evidence should be stored. At present, in each institution, even within one institution, the retention period for digital evidence varies from one department to another.
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	In Latvia we don't have separate regulations for it.
6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	All databases have a strong authentication system for authorised access. Law On State Information Systems. https://likumi.lv/ta/en/en/id/62324
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	In Latvia we don't have separate regulations for it.

8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	According to point (d) of Article 2 (2) the General Data Protection Regulation directly does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. At the same time, the GDPR has increased overall awareness of data protection in all data processing activities, and the amount of data shared between institutions has been reduced.

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	Criminal Procedure Law Chapter 82 *Assistance to a Foreign Country in the Performance of Procedural Actions* - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law CONVENTION ON CYBERCRIME Article 35 - 24/7 Network Regarding to Section 6 of "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" the responsible organisation is International Cooperation Department of the Central Criminal Police Department of the State Police of Latvia.
2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	Criminal Procedure Law Chapter 82 *Assistance to a Foreign Country in the Performance of Procedural Actions* - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law CONVENTION ON CYBERCRIME Article 35 - 24/7 Network

	Regarding to Section 6 of "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" the responsible organisation is International Cooperation Department of the Central Criminal Police Department of the State Police of Latvia.
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain.	
3a. Ireland	Cybercrime Convention,
3b. Estonia	1) Cybercrime Convention 2) European Investigation Order (EIO) 3) Agreement of 11 November 1992 between the Republic of Latvia, the Republic of Estonia and the Republic of Lithuania on legal assistance and legal relations https://likumi.lv/ta/lv/starptautiskie-ligumi/id/804
3c. France	Cybercrime Convention, European Investigation Order (EIO)
3d. Belgium	1) Cybercrime Convention 2) European Investigation Order (EIO) 3) AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF LATVIA AND THE GOVERNMENT OF THE KINGDOM OF BELGIUM ON POLICE COOPERATION https://likumi.lv/ta/id/106359-par-starptautisko-ligumu-speka-stasanos
3e. Latvia	
3f. Romania	Cybercrime Convention, European Investigation Order (EIO)
3g. Northern Ireland	Cybercrime Convention, European Investigation Order (EIO)
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the	If the cloud service provider is located in a foreign country then the CONVENTION ON CYBERCRIME Article 22 and Article 31 are applied.

cloud service provider, the data centre and/or the suspect are located in a foreign country or when the physical storage location is unknown and may be abroad?	
5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	Republic of Latvia adopted The CONVENTION ON CYBERCRIME on 23.11.2001., but joined on 14.04.2007 and the Parliament of Latvia (Saeima) ratiefied this convention.
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	Yes, EIO Directive is implemented into national law – see Chapter 82.[1] Recognition and Execution of a European Investigation Order and Chapter 83.[1] Taking a European Investigation Order and Transfer for Execution Thereof (https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law).
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	The provisions of Part C of the Criminal Procedure Law, the Law "On the Processing of Personal Data in Criminal Proceedings and Administrative Violation Proceedings", as well as international agreements that may provide for data protection rules are applicable (Latvia is currently negotiating bilateral agreements with several countries to ensure judicial co-operation criminal matters, and these agreements are intended to include data protection clauses).
8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	We have no information about such procedures.

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	In Latvia we don't have separate regulations for it.
2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	In Latvia we don't have separate regulations for it.
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	In Latvia we don't have separate regulations for it.
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	In Latvia we don't have separate regulations for it.
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	In Latvia we don't have separate regulations for it.
6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	In Latvia we don't have separate regulations for it.

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	Law on the Security of Information Technologies. https://likumi.lv/ta/en/en/id/220962

2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	We have no information about such actions.
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	**Electronic Communications Law** https://likumi.lv/ta/en/en/id/96611-electronic-communications-law
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	Within the framework of criminal proceedings, the provisions of Part C of the Criminal Procedure Law shall apply. Direct contact with service providers outside the jurisdiction of Latvia is not envisaged.
5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	Criminal Procedure Law - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law Section 190. Submission of Objects and Documents Requested by the Person Directing the Proceedings (1) The person directing the proceedings, without conducting the withdrawal provided for in Section 186 of this Law, is entitled to request from natural or legal persons, in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems. (2) If natural or legal persons do not submit the objects and documents requested by the person directing the proceedings during the term specified by such person directing the proceedings, the person directing the proceedings shall conduct a withdrawal or search in accordance with the procedures laid down in this Law. (3) The heads of legal persons have a duty to perform a documentary audit, inventory, or departmental or service examination within the framework of the competence thereof and upon a request of the person directing the proceedings, and to submit documents, within a specific term, together with the relevant additions regarding the fulfilled request.

	(5) If a document or object significant to criminal proceedings is located in any administrative case, civil case or another criminal case, the person directing the proceedings shall request it from the holder of the relevant case. The original of a document or object shall be issued only temporarily for conducting of an expert-examination, but in other cases a certified copy of a document or image of an object shall be issued.
6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	Criminal Procedure Law Chapter 11 Special Investigative Actions regulating the lawful interception for investigative purposes in a digital environment - https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	These actions could be subject to a number of special investigative actions: "**Section 215. Types of Special Investigative Actions** (1) The following special investigative actions shall be performed in accordance with the provisions of this Chapter: 1) control of legal correspondence; 2) control of means of communication; 3) control of data in an automated data processing system; 4) control of the content of transmitted data; 5) audio-control of a site or a person; 6) video-control of a site; 7) surveillance and tracking of a person; 8) surveillance of an object; 9) a special investigative experiment; 10) the acquisition in a special manner of the samples necessary for a comparative study; 11) control of a criminal activity." The general rules applicable to searches and seizures, as set out in point 13 of Part 1 of the questionnaire.

8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	We have no information about such regulations.

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

LEGAL ACTS OF THE REPUBLIC OF LATVIA - https://likumi.lv/

Legislation of the Republic of Latvia (in English) - https://vvc.gov.lv/index.php?route=product/category&path=60_109_111

Thank you!

Romania

INSPECTr

QUESTIONNAIRE FOR THE COLLECTION OF INFORMATION

WP2 INSPECTr Reference Framework for the standardisation of Evidence Representation and Exchange

Task 2.1 Initial legislative compliance relating to law enforcement powers and evidence requirements

Introduction

This questionnaire was sent to you because you are Law Enforcement Agency (LEA) involved in the INSPECTr project. The INSPECTr project aims to develop a shared intelligent platform and novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime support of LEAs at local, national and international level. In the Living Labs (LL), which are part of the INSPECTr project, you will test this platform, together with your colleagues from Ireland, Estonia, France, Belgium, Latvia, Romania and Northern Ireland. For the development of this platform it is necessary to understand certain international and national legal requirements as regards digital evidence and privacy and data protection. The goal of the task 2.1 is therefore to understand and assess the legal framework relating to law enforcement powers and evidence requirements. This legal analysis will feed into task 3.4.1.a, the EU Legislation Management Tool, which transforms the legal requirements into automated validation queries within the INSPECTr platform.

In order to understand the national laws, codes of conduct and other relevant document within your country, we kindly ask you to answer the questions in this questionnaire. Please be as detailed as possible in your explanation, support your answer with the corresponding legal references (articles of primary or secondary laws/ regulations/ codes of conduct/ guidelines/ case law/ etc.) and – if possible – kindly attach or paste relevant (legal) texts. The questionnaire can be answered by more than one person, such as a police officer, legal officer and/or the Data Protection Officer within your organisation.

Many thanks for your cooperation. Should you have any questions, please don't hesitate to contact us.

Melania Tudorica (m.tudorica@step-rug.nl)

Jeanne Mifsud Bonnici (g.p.mifsud.bonnici@step-rug.nl)

Information about the respondent

Contact person:	
Organisation, country and position:	Ministry of Internal Affairs / General Inspectorate of Romanian Police / National Forensic Institute, Romania, police officer

Section 1

General questions concerning national law

In this section, we would like to get a first impression of your national legal framework. For the INSPECTr project it is relevant not only to consider EU regulations as regards digital evidence and privacy and data protection, but also national laws. This section will give us an understanding of the legal structure and general principles as regards digital evidence in your country.

1. Does the legal system of your country provide for a strict distinction between measures for preventive purposes and measures for purposes of investigation and prosecution? If yes, could that prevent using digital data retrieved for preventive purposes as digital evidence in prosecution, for example due to divergent safeguards?	There is a distinction between measures for preventive purposes and measures for purposes of investigation and prosecution. Digital data retrieved for preventive purposes can be used as digital evidence in prosecution.
2. Which are the codes or laws in your national legal framework governing preventive measures (such as a Police Code or Criminal Code) and investigative measures (such as a Criminal Procedure Code)?	The law within the national framework that regulates preventive measures is Law no. 286/2009, regarding Criminal Code, and the investigation measures are regulated by Law no. 135/2010 regarding Criminal Procedure Code (Title V Preventive measures and other process measures, Chapter I Preventive measures, Section 1 General provisions, art. 202 Purpose, general application conditions and categories of preventive measures; art. 203 Judicial bodies of competent jurisdiction and the document ordering preventive measures; art. 204 Avenue of appeal against court resolutions ordering preventive measures during the criminal investigation)

3. Does the legal system of your country require a legal basis (such as a warrant) for all investigative measures (such as search and seizure)?	Yes. The legal basis for investigative measure is stipulated in the Law no. 135/2010 regarding Code of Criminal Procedure. For example: the art. 158 in this law stipulates the procedure for the issuance of a home search warrant.
4. Does your national legal framework make a distinction between physical evidence and digital evidence as regards gathering, analysing and sharing evidence? i.e. does your national legal framework apply general evidence rules designed for physical evidence also to digital evidence and/or are there separate rules for digital evidence?	Yes, our national legal framework (Law no. 135/2010 regarding Code of Criminal Procedure) makes a distinction between physical evidence and digital evidence in terms of collecting and analysing evidence.
5. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by competent authorities (such as police, prosecution, etc.)?	The law that covers gathering, analysing and sharing digital evidence by competent authorities is Law no. 135/2010 regarding Criminal Procedure Code
6. Which codes, laws or regulations cover sharing (i.e. transferring or exchanging) digital evidence between competent authorities, Security and Intelligence Agencies, CSIRTs and third-party data owners? Kindly list them.	The Law no. 14/1992 regarding the organization and functioning of the Romanian Intelligence Service. art 11 If from the verifications and specific activities provided in art. 9 and 10 result data and information that indicate the preparation or commission of an act provided by the criminal law, these are transmitted to the criminal investigation bodies under the conditions provided by art. 61 of the Code of Criminal Procedure.
7. Does your national legal framework provide definitions or concepts regarding the collection of digital evidence that are relevant for criminal investigations? If yes where can they be found?	The legal framework is represented by Law no. 135/2010 regarding Criminal Procedure Code. Concepts or definitions regarding the collection of digital evidence that are relevant for criminal investigations can be found Chapter IV Surveillance or investigative special methods at art. 138 General provisions and art. 168 Computer search.
8. What are the legal procedures or codes of conduct regulating the gathering of data for crime prevention?	Law no. 218/2002 on the organization and functioning of the Romanian Police, Provision S 126/2003 regarding the activity carried out by the Romanian Police for the Prevention of Crime, Strategy for the modernization of the Romanian Police 2004-2007 and Recommendation R 19/1987 of the Committee of Ministers of the Member States of the Council of Europe.
9. What are the legal procedures or codes of conduct regulating the collection of digital evidence in criminal investigations?	Law no. 135/2010 regarding Criminal Procedure Code

10. Is there a specific legal provision in your national legal framework covering lawful interception for investigative purposes in a digital environment (such as the internet), and if yes, which?	The legal framework is represented by Law no. 135/2010 regarding Criminal Procedure Code. Concepts or definitions regarding the collection of digital evidence that are relevant for criminal investigations can be found Chapter IV Surveillance or investigative special methods
11. Is there a specific legal provision in your national legal framework explicitly covering lawful interception on terminal devices for investigative purposes, and if yes, which?	The legal framework is represented by Law no. 135/2010 regarding Criminal Procedure Code, Chapter IV Surveillance or investigation special methods at art. 138 General provisions (2) Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device.
12. Is there a specific legal provision in your national legal framework explicitly covering computer-assisted search for investigative purposes, and if yes, which?	The legal framework is represented by Law no. 135/2010 regarding Criminal Procedure Code art. 138 General provisions (3) Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialized programs or through a network, for the purpose of identifying evidence and art. 267 Access to electronic databases
13. Is there a specific legal provision in your national legal framework explicitly covering the seizure of digital evidence (data itself and/or media carrying the data), and if yes, which?	Law no. 135/2010 regarding Criminal Procedure Code, Section 3 Seizure of objects and documents art. 169 Seizure of objects and documents and art. 168 Computer search

Section 2

Legal requirements for privacy and data protection

This section is aimed at giving us an understanding of fundamental rights and legal requirements concerning privacy and data protection in your country. The Data Protection Officer within your organisation could answer this section.

1. Does the system of fundamental rights in your country provide for a distinct (codified or uncodified) fundamental right to (telecommunications) privacy and data protection? If yes, does this impact the necessary safeguards to be taken when gathering and analysing digital data in the prevention or	The Romanian Constitution provides for 2 fundamental rights on data protection and confidentiality. It is: - paragraph 26 Intimate, family and private life:

investigation of crimes? i.e. could lack of safeguards prevent or hinder gathering and analysing digital evidence?	"(1) Public authorities respect and protect intimate, family and private life. 2. The natural person shall have the right to dispose of himself, unless he infringes the rights and freedoms of others, public order or good morals." –paragraph 28 The secret of correspondence: "The secret of letters, telegrams, other postal items, telephone calls and other legal means of communication is inviolable."
2. Has Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Police Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant points that stand out in the implemented national law, such as higher safeguards than those established in the Police Directive?	Yes, it was translated into national legal framework by Law No. 363/2018, regarding protection of individuals to processing of personal data by the competent authorities for the purpose of preventing, discovering, investigating, prosecuting and combating criminal offences or the execution of penalties, educational and safety measures, and on the free movement of such data. No greater guarantees are provided than those of Directive EU 2016/680
3. Does your national legal framework or operational guidelines determine who is authorised to process digital evidence?	Yes, national legal framework requires competent authorities to carry out activities for the purpose of preventing, discovering, investigating, prosecuting and combating crime according to law No. 218/2002 regarding the organisation and functioning of the Romanian Police. In criminal investigations evidence is gathered and processed by police authorities and prosecutors. The general rules for evidence management also apply to digital evidence, even though digital evidence analysis has a distinct procedure set forth in the Criminal Procedure Code.
4. Does your national legal framework require standard operating procedures or codes of conduct for the preservation of digital evidence?	The legal framework doesn't require SOP's/COC's for the preservation or examination of digital evidence.
5. Does your national legal framework provide any specifications on the preservation of digital evidence, i.e. how, how long and where digital evidence must be stored?	National legal framework and the Criminal Procedure Code lay down rules on evidence in criminal cases. Depending on the crimes investigated, there are also special provisions in other normative acts. There are no special provisions for the preservation of digital evidence.

6. Does your national legal framework impose specific restrictions to LEAs for access to digital evidence databases, such as a strong authentication system for authorised access?	National legislation grants access to databases specific to each authority. Depending on their responsibilities and competences, some authorities have access to databases created by other authorities. Access is clearly established in normative acts. At the individual level, a person's access to a database is strictly subject to authorisation, subject to several conditions for ensuring data security.
7. Does your national legal framework provide any safeguards aiming at the protection of individuals against function creep, i.e. when digital evidence collected for a certain purpose ends up being used for a different purpose (such as a different case)?	Yes. Personal data collected for the purpose of preventing, discovering, investigating, prosecuting and combating criminal offences may not be processed for any other purpose, except in cases expressly provided for by law.
8. Does the entry into force of the General Data Protection Regulation GDPR impact the gathering, analysing and sharing of data for the prevention, investigation and prosecution of crimes?	No. Activities carried out for the purpose of preventing, discovering, investigating, prosecuting and combating criminal offences or the execution of punishments, educational and safety measures, as well as on the free movement of such data, shall be subject to the provisions of Law no. 1/2002 and Law no. 363/2018, transposing into national law EU Directive 2016/680

Section 3

Legal framework for cross-border cooperation

Considering the goal of the INSPECTr project to develop a platform for sharing investigative data and the variety of international and national regulations as regards transfer, this section aims at mapping the applicable legislation on all levels in detail in order to build this into the automated validation of LEA queries within the platform. The countries in questions 2 – 8 in this section are specifically mentioned as they are part of the Living Labs in the INSPECTr project.

1. Which codes, laws, or regulations cover cross-border cases, in which authorities from your country are requested/obliged to collect and/or transfer case data or digital evidence to authorities of another country and vice versa?	The Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters has been Transposed by Romania by Law no. 302/2004 on international judicial cooperation in criminal matters, as amended and supplemented by Law no. 224/2006, Law no. 222/2008, Law no. 300/2013 and Law no. 236/2017, published in the Official Journal of Romania no. 993/14 December 2017.

	Law no. 56/2018 on the cooperation of the Romanian public authorities with the European Agency for Law Enforcement Cooperation (Europol). Government Emergency Ordinance No. 103 of 13 December 2006 on the measures for facilitating the international police cooperation
2. Who is responsible for approving and making requests for transferring case data or digital evidence, according to the national rules or regulations in your country, i.e. which department, level or position within the LEA organisation is responsible for this.	The investigative officers under the supervision of case prosecutors are entitled to such requests.
3. Are competent authorities in your county allowed to share digital evidence with the following countries (under a – g)? If yes, based on which law, agreement, treaty, etc. (such as Mutual Legal Assistance (MLA), Cybercrime Convention, European Investigation Order (EIO)) are you allowed to do this and are there any restrictions? Please list and explain.	
3a. Ireland	Mutual Legal Assistance (MLA with referrer The Convention on Cybercrime, 23.11.2001; EUROJUST
3b. Estonia	European Investigation Order with referrer The Convention on Cybercrime, 23.11.2001; EUROJUST, Law no. 302/2004
3c. France	European Investigation Order with referrer The Convention on Cybercrime, 23.11.2001; EUROJUST, Law no. 302/2004
3d. Belgium	European Investigation Order with referrer The Convention on Cybercrime, 23.11.2001; EUROJUST, Law no. 302/2004
3e. Latvia	European Investigation Order with referrer The Convention on Cybercrime, 23.11.2001; EUROJUST, Law no. 302/2004
3f. Romania	
3g. Northern Ireland	Mutual Legal Assistance (MLA with referrer The Convention on Cybercrime.
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence out of a cloud service, in particular when the cloud service provider, the data centre and/or the suspect are located in a	There are no codes, laws or regulations that explicitly cover the collection of digital evidence from a cloud service

foreign country or when the physical storage location is unknown and may be abroad?	Request for preservation of evidence by Convention on Cybercrime, to the prosecutor's office in the country. Request to make evidence available through the Mutual Legal Assistance /European Investigation Order
5. Has the Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) been implemented into national law in your country? If yes, to what extent and in which form?	The Council of Europe Convention on Cybercrime (2001 Cybercrime Convention) has been Transposed by Romania by Law no. 64/2004 published on 24 march 2004
6. Has Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) been implemented into national law in your country? If yes, to what extent and in which form? Are there any significant measures that stand out in the implemented national law? And in your expert opinion, is the EIO an effective tool or does it have the potential to be an effective tool? What could be improved?	The Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters has been Transposed by Romania by Law no. 302/2004 on international judicial cooperation in criminal matters, as amended and supplemented by Law no. 224/2006, Law no. 222/2008, Law no. 300/2013 and Law no.236/2017, published in the Official Journal of Romania no. 993/14 December 2017.
7. Does your national legal framework provide specific rules regarding the transfer of digital evidence or does your national legal framework provide general rules regarding transfer of evidence that are also applicable to digital evidence?	There are no specific rules regarding the transfer of digital evidence. The transfer of the digital evidence is done as for the other evidence.
8. Does your national legal framework provide for guidelines or procedures for cross-border exchange between national authorities of different countries, such as method of exchange, requirements, authorisation, etc.?	There are no guidelines or procedures for cross-border exchange between national authorities of different countries.

Section 4

Legal framework for LEA and Security and Intelligence Agencies interactions

With this section we would like to get an understanding of the legal framework for LEA and Agencies interactions in your country.

1. Does your national legal framework provide guidelines or procedures for exchange of digital evidence between national authorities, such as method of exchange, requirements, authorisation, etc.?	There are no specific regulations regarding the exchange of digital evidence among LEA's. Information and data is exchanged based on a case-to-case analysis and request.

2. Are LEAs and Security and Intelligence Agencies allowed to share information for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	Yes, information obtained legally
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Security and Intelligence Agencies?	The Law 14/1992 regarding the organization and functioning of the Romanian Intelligence Service, art 11 If from the verifications and specific activities provided in art. 9 and 10 result data and information that indicate the preparation or commission of an act provided by the criminal law, these are transmitted to the criminal investigation bodies under the conditions provided by art. 61 of the Code of Criminal Procedure.
4. Do Security and Intelligence Agencies have executive powers (such as arrest, search, seizure, etc.) in your country?	The Romanian Intelligence Service cannot carry out criminal investigation, cannot arrest or detain persons and does not have its own detention facilities. However, in case of catching somebody in the act of committing a crime punishable under the national security regime established by law, of an attack or terrorist act or of attempts or preparatory acts for such crimes, if they are punished by law, the officers of the Romanian Intelligence Service may detain the perpetrator, immediately handing it over to the competent judicial authorities together with the relevant evidence
5. Does your national legal framework provide any legislative acts that regulate the transfer of information from intelligence services to LEAs or prosecution authorities, and if yes, which?	The Law no. 14/1992 regarding the organization and functioning of the Romanian Intelligence Service, art 11 If from the verifications and specific activities provided in art. 9 and 10 result data and information that indicate the preparation or commission of an act provided by the criminal law, these are transmitted to the criminal investigation bodies under the conditions provided by art. 61 of the Code of Criminal Procedure.
6. Are there any restrictions for gathering, analysing and sharing of digital evidence (not only information) collected by intelligence services in criminal proceedings, and if yes, which?	Digital evidence to be obtained legally and it has to pertain to national security

Section 5

Legal framework for Computer Security Incident Response Team (CSIRTs) and third-party data owner interactions

With this section we would like to get an understanding of the legal framework for CSIRTs and other third-party data owner's interactions in your country.

1. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by Computer Security Incident Response Teams (CSIRTs)?	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union has been Transposed by Romania by Law no. 362/2018, was published in the Official Journal of Romania no 21, section 1 and came into force on 12th January 2019, with the aim of transposing the NIS Directive into national legislation. Law no. 362/2019 empowers The Romanian National Computer Security Incident Response Team (CERT-RO) as the competent national authority supervising OESs (Operators of Essential Services - acting in sectors that heavily rely on information and communications technology, such as water transport, energy, digital infrastructure, banking and financial market, healthcare or transport) and DSPs (Digital Service Providers – that normally provide their services for a cost, at a distance, by electronic means and at the individual request of the recipient of services) in implementing their responsibilities according to the law
2. Are LEAs and CSIRTs in your country allowed to share information or digital evidence for the prevention, investigation and prosecution of crimes? If yes, what are the requirements?	CERT-RO carries out its activity in accordance with the legislation and with its own organization and functioning regulation, in order to achieve prevention, analysis, identification and response to incidents in cyber infrastructures that provide public utility functionalities or provide information society services. Law no. 362/2019 art. 16 CERT-RO shall consult and cooperate, as appropriate, with: a) the criminal investigation bodies (the prosecutor; the criminal investigation bodies of the judicial police; special criminal investigation bodies)
3. Which codes, laws or regulations cover gathering, analysing and sharing digital evidence by third-party data owners (such as telecommunication service providers)?	Law no. 135/2010 on the Code of Criminal Procedure, art. 152 Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these; art. 170 Surrender of objects, documents or computer data
4. Are there any codes, laws or regulations in your country explicitly covering the collection of digital evidence from internet service providers, in particular when the service provider is located in a foreign country?	Law no. 135/2010 on the Code of Criminal Procedure, art. 154 Preservation of computer data

5. Does your national legal framework provide procedures that need to be followed by LEAs to access digital evidence databases of private companies, such as an authorisation or warrant?	There are no specific procedures regarding access digital evidence databases of private companies, but law no. 135/2010 regarding Criminal Procedure Code, art. 168 Computer search, provides the information required for the digital data search warrant.
6. Which law governs observation on the internet or other networks, infiltration online e.g. on social media or darknet platforms, rules for digital search and seizure? Are there differences in who may be authorised to carry each of these activities?	There are no special regulations in observing the internet or other networks, online infiltration e.g. on social media or darknet platforms, rules for digital search and confiscation, but law no. 135/2010 on the Code of Criminal Procedure provides according to art. 138 General provisions 1) The following are surveillance or investigation special methods a)wiretapping of communications or of any type of remote communication, b) accessing a computer system; g) use of undercover investigations and informants; art. 152 Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these; art. 154 Preservation of computer data; art. 170 Surrender of objects, documents or computer data (1) In the event that there is a reasonable suspicion in relation to the preparation or commission of an offense and there are reasons to believe that an object or document can serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender
7. Are there laws, operational procedures or codes in your national legal framework for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution?	There are no special regulations or operational procedures for LEA access of network operators infrastructure for observation on the internet, infiltration on social media, rules for digital search and seizure for prevention, investigation and prosecution, but law no. 135/2010 on the Code of Criminal Procedure provides according to art. 138 General provisions 1) The following are surveillance or investigation special methods a) wiretapping of communications or of any type of remote communication, b) accessing a computer system; g) use of undercover investigations and informants

8. Which laws, operational procedures or codes are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure?	There are no special operational procedures are used to allow network operators to assist LEAs in the observation on the internet, infiltration on social media, rules for digital search and seizure but law no. 135/2010 on the Code of Criminal Procedure provides according to art 142 Enforcement of electronic surveillance warrants (2) Providers of public electronic communication networks or providers of electronic communication services intended for the public or of communication or financial services are under an obligation to cooperate with the criminal investigation bodies, within the limits of their authority, for the enforcement of electronic surveillance warrants. Law no. 506 of 17 November 2004 on the processing of personal data and the protection of privacy in the electronic communications sector Article 12 ^ 1 Access to data of the authorities 1. At the request of the courts or at the request of criminal investigation bodies or state bodies with responsibilities in the field of defense and national security, with the prior authorization of the judge established by law, electronic communications to the public and providers of public electronic communications networks shall make available to them, immediately but not later than 48 hours, traffic data, equipment identification data and location data, in accordance with the provisions on the protection of personal data.

If you would like to inform us about any further issues which are relevant for understanding the legal framework of your country as regards law enforcement powers and evidence requirements, please feel free to make additional comments.

Thank you!