HORIZON-CL3-2021-FCT-01-08

RITHMS – Research, Intelligence and Technology for Heritage and Market Security

GA 101073932

Deliverable 1.1

Initial Legal Requirements

WP1 – Requirements and definition of users' needs

Authors: Patricia Faraldo Cabana, Xulio Ferreiro Baamonde, Luz María Puente Aba, Ana Neira Pena, María Ángeles Fuentes Loureiro, Silvia Rodríguez López, Amara García Adán (UDC)

Lead participant: UDC

Delivery date: 31 March 2023

Dissemination level: Public

Type: Report

Revision History

Author Name, Partner short name	Description	Date
Patricia Faraldo Cabana, Xulio Ferreiro Baamonde, Luz María Puente Aba, Ana Neira Pena, María Ángeles Fuentes Loureiro, Silvia Rodríguez López, Amara García Adán (UDC)	Draft deliverable	05/03/2023
Michela De Bernardin (IIT), Alessandro Guarino (StAG)	Revision	30/03/2023
Arianna Traviglia (IIT)	Final version	31/03/2023

Contents

Executive Summary

The present document is a deliverable of the RITHMS project. It presents the results of RITHMS research on legal requirements related to the end-user stage at the EU and national level (six countries, four EU Member States and two non-EU Member States). The report analyses relevant EU and national laws regarding the protection of data processed for the purposes of the prevention, investigation, and detection of criminal offences, and other pressing issues not related to data protection, such as accessibility or dual-use export. It summarises the results of the country studies on these topics, whose full version will be available at Deliverable 7.1 – Report on the legal framework (UDC, PU, M8). This report supports partners in monitoring and complying with the ethical and legal requirements of the project, taking into account LEAs' needs and counterbalancing them with the need to respect fundamental rights and ethical principles, data protection regulations, and European and national legal regimes. This report will also inform the technical development of RITHMS platform, which will be carried out in Work Package 3 and Work Package 4.

In the next pages, Section 1 outlines the approach followed regarding the methodology and research questions. Section 2 describes the initial legal requirements stemming from the EU legal framework, as well as the national particularities that are relevant for using the RITHMS Platform. Finally, Section 3 outlines the legal modifications that will follow the enactment of the Artificial Intelligence Act, at the moment only a draft.

List of abbreviations

AEPD	Agencia Española de Protección de Datos (Spanish DPA)
BG	Bulgaria
BiH	Bosnia and Herzegovina
CPDP	Commission for Personal Data Protection (Bulgarian DPA)
DCCP	Dutch Code of Criminal Procedure
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
ECHR	European Charter of Human Rights
EDPB	European Data Protection Board
ES	Spain
EU	European Union
GDPR	General Data Protection Regulation
IT	Italy
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
LPDP	Law on Personal Data Protection
LPPD	Law on the Protection of Personal Data
MD	Moldova
NL	The Netherlands
NPCDP	National Center for Personal Data Protection (Moldovan DPA)
SNA	Social Network Analysis
WP	Work Package

Annexes

Annex 1. List of laws

1 Introduction

1.1 Scope

The main focus of Task 1.1 – Legal and Security requirements (M1-M6, StAG) is to analyse the legal and security framework – both at national and international levels – with an impact on the RITHMS SNA ecosystem. Within this task, the primary legal requirements to which the development of RITHMS Platform will conform are collected and reviewed. Pieces of legislation relevant to the project are identified and the specific requirements extracted, in particular those stemming from the General Data Protection Regulation (2016/679), the Law Enforcement Directive (2016/680) and its national implementations in the countries where RITHMS will conduct its testing and validation. Initial legal requirements are issued in D1.1. They will provide relevant inputs for WP3 and WP4. These initial requirements will be subject to review and updates in WP7.

1.2 Structure

Section 1 of the report (this section) sets out the context, scope, structure, and methodology of the report, explaining its relation to other deliverables. Section 2 presents an analysis of the initial legal requirements, at both European and domestic levels, regarding the use of the RITHMS platform by LEAs. Section 3 outlines the legal modifications that will follow the enactment of the Artificial Intelligence Act, at the moment merely a draft. In addition, the appendices to this report present a reference list of relevant European and domestic legislation.

1.3 Methodology

The requirement definition process is a critical goal in system development, since one generally accepted cause of a system failure is a poor requirement identification. The process of determining requirements usually has three stages (Pitts and Browne 2007):

- information gathering
- representation, and
- verification

A search and analysis of all the useful sources (laws, opinions, studies, best practices etc.) are required in order to identify the elements that have to guide the system development from its design phase.
There are at least two different perspectives for requirements identification:

- On the one hand, the locating perspective, applicable to legal issues, which assumes that the requirements are something that actually exists and merely must be found. That perspective implies that requirements are stable and recognisable.
- On the other hand, the constructing view aims at creating something new by combining identified elements in new ways.

Following both approaches, the requirements' fulfilment will be monitored for the entire duration of the project through other deliverables (such as D7.1 – Report on the legal framework, M8, UDC), which will follow the requirements evolution. Hence, most requirements presented in this deliverable are design-principle oriented and based on the need to respect both human values (rights and freedoms) and legal provisions (obligations and duties for the controller, rights of data subjects).

As specified in the proposal, pieces of legislation relevant to the project have to be identified and the specific requirements extracted, in particular those stemming from the General Data Protection Regulation (henceforth, GDPR) and the Law Enforcement Directive (LED), plus national implementations in the member states where RITHMS will conduct its pilots (Bulgaria, Italy, the Netherlands, Spain), as well as the national legal framework of the two countries which are not members of the EU (Bosnia and Herzegovina and Moldova).

The detailed methods and approaches for analysing the EU and national legal frameworks were as follows:

A) Approach to analysing EU legal framework

In this phase of the analysis, using desktop research we studied relevant EU law. The analysis followed the above-outlined approach applied to the international law, but also took into account distinct features of the legal system of the EU. In particular, in the light of principle of conferral, we explored the extent to which addressing the identified legal issues, including human rights challenges, lies within the EU competences. We also bore in mind that EU law uses terminology and legal concepts that are often peculiar to it.

B) Approach to national legal frameworks

This research also analysed the six EU and non-EU countries' legislations pertinent to the use of the RITHMS platform at the end-user stage. The LEAs engaged in the consortium were identified in order to balance the following criteria: i) country participation (6 countries: Bulgaria, Bosnia and Herzegovina, Spain, Italy, Moldova, the Netherlands); ii) presence of both police forces (4) and border authorities (2); iii) countries' relevance and role in illicit trafficking of cultural goods; iv) presence of experienced partners (front-runners) with specialised units and early-stage ones.

The last step was to take inputs and expertise from the Consortium partners and individuals involved in the project, to develop the initial version of the system requirements. An online questionnaire was used for attaining information from the LEAs that will be concerned with the usage of the system. Legal requirements were then extracted from the information sent by the Consortium's legal experts. The results were contrasted with LEAs during the workshop in Munich (31 January-2 February 2023), after which they have been tailored to the project's platform and architecture by taking into consideration:

- The discussions held within the Consortium amongst LEAs, legal and industry partners, starting from the project's kick-off meeting held in Venice in October 2022, and continued in subsequent workshop in Munich in January 2023, and emails exchanges;
- The definition of the initial system and architecture's features, which resulted in the identification of necessary technical and user requirements by the relevant partners, on which legal requirements were devised.

Since the specific features of the multifaceted RITHMS platform and components cannot be entirely known in advance now the requirements are drafted, two corrective measures have been deployed to prevent the risk of outdated or impertinent requirements:

- The first measure is ensuring a close interaction between partners with different expertise within the Consortium, in order 1) for legal experts to be constantly aligned with technology's developments within the project, and 2) for industry partners to be fully instructed on the practical consequences of changes in the legal framework or in the technological environment considered.
- The second corrective measure consists of involvement of end-users into creation of the system. This exercise is part of WP1 and 5, with the test and demonstration of the platform prototype being part of WP5. End-users' feedback, concerning what are their expectations in terms of both project's outcomes and platform's functioning will be carefully considered for the whole duration of the project. During the co-creation phase, feedback will be collected from the LEAs involved in the project.

1.4 Relation to other deliverables

The scientific research and outputs within RITHMS should safeguard principles of research ethics as well as legal and ethical requirements. In many ways, though, legal and ethical requirements overlap. The analysis of the initial legal requirements concerning the technologies being developed in WP3-4 is the objective of this D1.1. A number of legally binding rules at European, national and international level already apply or are relevant to the development, deployment and use of technologies such as the RITHMS platform today. This document considers in particular existing legal norms and requirements that the RITHMS platform must comply with in order to be deployed for Law Enforcement. It also pays attention to future developments. In D7.1 - Report on the legal framework (UDC, PU, M8), UDC will map the European and national legal framework regarding RITHMS technological outputs and the implied methodology, including an extensive exploration of the General Data Protection Regulation and the Law Enforcement Directive (LED),[1] as well as the national

[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, OJ L 119, 4.5.2016, p. 89–131.

instruments envisaged by each country in the Consortium. The Ethics Protocol (D7.2, UDC, M6) provides an overview of all planned data collection and processing operations (Section 3); the identification and analysis of the ethics issues that these operations raise (Section 4); and an explanation of the mitigation measures that should be applied to reduce risks (Section 5). A detailed explanation of the technical and non-technical implementation of mitigation measures and methods to realise Trustworthy AI is contained in D9.3 (ITT, M6). Together, these deliverables consider the legality and ethics of using open-source and publicly available data in research, as well as of using the RITHMS platform by LEAs. They articulate a framework for achieving Trustworthy AI based on fundamental rights. The present document (D1.1), together with the Security Requirements (D1.2), the Use Case Scenarios presented in D1.3, and the technical requirements presented in D1.4, constitutes comprehensive input for the development of the RITHMS technical ecosystem.

2 Requirements description

2.1 Requirements analysis and classification

In this section, an initial set of requirements has been compiled. They indicate a property or a service of the system, which may be of interest either for the LEAs perspective or for the Consortium as a whole. Each requirement will be revised during the project, considering the development of the platform and the suggestions of the research community. The whole work on requirements is reported in a table like the following:

Requirement title	…
Level of criticality	…
Legal basis	…
Description	…
Explanation	
National particularities	…

Table 1. *Requirements table sample.*

Therefore, each requirement will have:

- A title;
- A level of criticality from 1 to 3. Requirements marked with:
  - Level 3 are described as 'critical' because they stem from legal obligations directly applicable to the system and the project;

- Level 2 requirements are 'important', which means that failure to implement them would result in legal non-compliance;
- Level 1 requirements are those that functionally are 'optional' and if embedded into the system will align it with non-binding legal recommendations (optional).

- Indication of the legal basis, be it international law or EU law.
- A synthetic description, based on applicable legislation;
- Some complementary explanations, which can further detail the presented requirement, its rationale, and eventually refer to any relevant normative basis, etc.
- National particularities, if any, with indication of the legal basis.

The following list of legal requirements consider only the LEAs' perspective (final-product usage).

2.2 Legal requirements at the end-user phase

2.2.1 Introduction

Legal requirements at the end-user phase have been identified only for Italy, Spain, Bulgaria, Bosnia and Herzegovina, Moldova and the Netherlands. They are the countries that provide the user-case scenarios and pilots, acting as a driver for the development of RITHMS Platform. Requirements are divided in two categories: the ones related to personal data protection and the ones related to other issues, such as accessibility or dual-use export control. As we will see, the law provides both positive and negative obligations: it should not only be interpreted with reference to what cannot be done, but also with reference to what should be done and what would be merely recommendable to do.

2.2.2 Personal data protection

The rights to privacy and to data protection are recognised throughout the world. Distinctions are made between the public sphere and the private sphere, and case law has evolved to facilitate the differentiation. It is generally held that in the public sphere, a suspect in a criminal investigation has less of a reasonable expectation of privacy. The LED seeks to remedy shortcomings from the previous framework and balance the free flow of personal data between competent authorities with a consistent and high level of protection of personal data and individuals' rights and freedoms. In that vein, the new framework is adapted to accommodate the special characteristics and needs of police and criminal justice personal data processing. It has further been praised for broadening the scope of data protection rules beyond the cross-border setting and to domestic processing activities, and for providing stronger safeguards for data subjects. The level of protection provided, though, differs from country to country, which explains why we have carefully explored the national particularities of the six countries of origin of the LEAs that are going to deploy the platform. In fact, prompted by the fragmented legal landscape on data protection within criminal justice, the LED constitutes an instrument of minimum harmonisation. The choice of a directive, and consequently the broad

discretion afforded to Member States, which may also apply higher standards of protection (see Article 1(3) LED), risk the perpetuation of divergent implementations at national level. Apart from legal uncertainty for controllers and data subjects, differences on data protection rules hinder the effective co-operation between authorities of different Member States.
The LED applies to processing activities when two cumulative conditions are met:

1) The processing pursues any of the purposes stipulated under Article 1(1) LED, and
2) it is carried out by competent authorities as defined under Article 3(7) LED.

If either of these conditions is not met, then the GDPR applies. The scope is delimited by Article 2(3) LED, according to which the LED does not cover processing operations that fall outside the scope of EU law, and by EU institutions, bodies, offices and agencies. These positive and negative conditions of application may prove challenging in the implementation of the LED. Relevant to these aspects are the occasionally blurred lines between the LED and the GDPR, as the LED lacks a dedicated provision clarifying its delineation from the GDPR.

Requirement 1	***Lawfulness of personal data processing***
Level of criticality	3
Legal basis	Articles 8 and 9 LED, Recital 12 LED, Article 10 GDPR, Principle 2 of Recommendation No. R (87) 15, Article 8(2) ECHR
Description	Processing of personal data will be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority 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, and that it is based on Union or Member State law.
Explanation	LEAs can only process personal data 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, and these purposes must be based on Union or Member State law. Recital 12 LED specifies that these purposes under Article 1 LED concern 'police activities without prior knowledge if an incident is a criminal offence or not … such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence.' The definitions of prosecution and execution of criminal penalties, which are undertaken by a broad range of competent authorities and may differ

significantly at a national level depending on criminal procedural laws, are not further clarified. Recital 20 merely notes that LED 'does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.'.

Personal data collected by competent authorities for the above-mentioned purposes shall not be processed for other purposes unless such processing is authorised by Union or Member State law. This is relatively easy to fulfil given the broad range of aims listed in EU regulation, but national laws must clearly indicate the scope of the discretion conferred on the public authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

As established in Recital 13 LED, a criminal offence 'should be an autonomous concept of Union law' as interpreted by the CJEU. The lack of more concrete harmonisation may result in offences being considered as criminal within some national legal orders and as administrative in others.

National particularities

The expansive approach followed by the following Member States demonstrates how any national law can designate entities as competent authorities within the meaning of the LED, without a requirement of public authority and power, thereby widening the LED scope of application:

BiH Article 4 of the Bosnian LPPD simply states that the controller shall be required to process personal data fairly and lawfully. Regarding competent authorities, it establishes that any public authority, in the capacity of the controller, shall be required to issue, within the scope of legal competencies, a regulation aimed at enforcing this Law. No further reference has been found in 2011 amendment nor in the Draft Law.

BG Article 42 of the Bulgarian PDPA indicates that competent authorities shall be the public authorities vested with powers to prevent, investigate, detect or prosecute criminal offences or to execute criminal penalties, including to safeguard against and prevent threats to public security.

IT Article 5 of Decree 51 reproduces Article 8 LED, but allows, where provided for by law, the use not only of a law, but of a regulation which identifies the personal data and the purposes of processing. The Italian legislator made explicit that competent authorities may be Italian, European or third-country ones, while the Italian transposition of Article 3(7)(b) LED refers to any other entity or organization tasked by the national legal system with law enforcement activities, allowing for a broad interpretation of competent authorities.

MD	Article 8(1) of the Moldovan LPDP only states that 'processing of personal data relating to criminal convictions, coercive procedural measures or administrative sanctions may be carried out only by or under the control of public authorities, within the limits of their competences and on the conditions set by laws regulating these areas.' Article 8(2) adds that 'the Registry of Criminals and Criminological Data is kept by the Ministry of Internal Affairs'. Article 16(1) of Law no. 320/2012 regarding the Police activity and the status of the policeman states that for the efficient execution of its duties, the Police has the right to collect, process and keep information about people who have committed illegal or harmful acts, to create and use their own databases, to use the databases of other authorities, with compliance with the provisions of the legislation regarding the protection of personal data. Article 5(1) of Law no. 59/2012 regarding the special investigation activity states that the persons who have access to the personal data of the person subject of the special investigation measure are obliged to keep the respective data confidential in accordance with the provisions of Moldovan LPDP.
NL	Article 1 of the Dutch Police Data Act states that the competent authorities to process personal data in the context of the performance of the police task can be any government agency with due competences or any other body or entity authorized to exercise public authority and powers with a view to the police tasks. Besides, Article 3 of the Police Data Act establishes that police data will only be processed insofar as this is proper and lawful, the data has been obtained lawfully and the data, in view of the purposes for which they are processed, are sufficient, relevant and not excessive.
ES	Articles 11 and 12 of Organic Law 7/2021 simply reproduce Articles 8 and 9 LED. The Spanish list of competent authorities includes LEAs, prison system authorities, the Deputy Directorate of the Customs Surveillance Service, the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses, and the Commission for the Surveillance of Terrorism Financing Activities, as well as criminal judges and public prosecutors.

Requirement 2	***Purpose limitation and processing for secondary purposes***
Level of criticality	2
Legal basis	Articles 1 and 4(1)-(2) LED, 5(1)(b) GDPR; Principle 4 of Recommendation No. R (87) 15
Description	A key data protection principle is that of purpose limitation. The purposes for which data can be processed must be determined prior to collection. The original purpose serves as a binding guideline requiring all future processing activities to be compatible with these objectives. The proper documentation of the

	purpose is a requirement, as well as a necessary tool serving the assessment of the requirements of lawfulness and transparency.
Explanation	Police seizure of a person registered in civil databases for the purpose of subjecting that person to increased surveillance or detention does implicate the right to privacy. Only Union or Member State law can authorise it, since using data beyond what data subjects could reasonably expect infringes the purpose limitation principle. In order to do so, the proportionality test applies: Processing should be necessary and proportionate to any of the purposes set out in Article 1(1) LED.
National particularities	EU Member States simply reproduce the LED, while the two non-Member States also align with it.
BiH	Article 4 of the Bosnian LPPD establishes that the controller shall be required to process personal data only for special, explicit and lawful purposes, and in no manner contrary to the specified purpose, like Article 4 LED. Article 25 of the Ministry of the Interior Act allows the processing of personal data for the protection of national security, protection of public order and countering crime carried out under the terms and conditions of the GDPR and the LPPD.
BG	The Bulgarian PDPA includes provisions implementing the LED that permit secondary processing in certain circumstances (Article 45(2) PDPA).
IT	Article 3 of Decree 51 simply reproduces Article 4 LED.
MD	The Moldovan LPDP establishes that personal data must be 'collected for specific, explicit and legitimate purposes, and subsequently not to be processed in a manner incompatible with these purposes', like Article 4 LED. Moreover, Article 15 of the Moldovan LPDP states that this provision shall not apply where the processing of personal data is carried out in the context of actions of prevention and investigation of criminal offences, enforcement of convictions and other activities within criminal or administrative procedures, in terms of the law. Besides, it clarifies that 'the further processing of personal data for statistical, historical or scientific research purposes is not considered incompatible with the purpose of collection' if it is carried out in accordance with the law. Article 16(1) of Law no. 320/2012 regarding the Police activity and the status of the policeman states that for the efficient execution of its duties, the Police has the right to collect, process and keep information about people who have committed illegal or harmful acts, to create and use their own databases, to use the databases of other authorities, with compliance with the provisions of the legislation regarding the protection of personal data.
NL	Article 3(3) of the Dutch Police Data Act allows using police data for secondary purposes in certain circumstances.
ES	Article 6 of Organic Law 7/2021 simply reproduces Article 4 LED.

Requirement 3	Data minimization
Level of criticality	2
Legal basis	Articles 4(1)(c) LED, 5(1)(c) GDPR, Principle 2 of Recommendation No. R (87) 15
Description	Collected data will be adequate, relevant and not excessive.
Explanation	Under Article 4(1)(c) LED, personal data should be 'adequate, relevant and not excessive', instead of 'adequate, relevant and limited to what is necessary', as stipulated under Article 5(1)(c) GDPR. This wording reflects the need for flexibility and for safeguarding criminal procedures, such as an investigation, whereby it is not immediately evident what sort of data are necessary. It seems that LED controllers can operate with less precision, insofar as they do not process excessive datasets.
National particularities	All studied countries align with the LED, with no relevant national particularities.
BiH	Article 4(c) of the Bosnian LPPD requires that the process of personal data is only done to the extent and scope necessary for the fulfilment of the specified purpose.
BG	Article 45 of the Bulgarian PDPA simply reproduces Article 4(1)(c) LED.
IT	Article 3(1)(c) of Decree 51 simply reproduces Article 4(1)(c) LED.
MD	Article 4(1)(c) of the Moldovan LPDP simply reproduces Article 4(1) (c) LED. The same article at the letter (c) states that the personal data subject to processing must be accurate and, if necessary, updated. Inaccurate or incomplete data from the point of view of the purpose for which they are collected and subsequently processed are deleted or rectified. Article 5(2) of Law No. 59/2012 states that the access to the special file or to the materials in the file of persons other than those investigating the special file is prohibited, with the exception of the head of the specialized subdivision of the respective body, within the limits of competence, and the prosecutor who authorized the special investigative measure or requested its authorization by to the investigating judge, as well as with the exception of the investigating judge who authorized the special investigative measure.
NL	Article 3(2) of the Dutch Police Data Act establishes that police data will only be processed insofar as this is necessary for the purposes formulated by or pursuant to this law.
ES	Article 6 (1)(c) of Organic Law 7/2021 simply reproduces Article 4(1)(c) LED.

Requirement 4	*Accuracy*
Level of criticality	3
Legal basis	Articles 4(1)(d) and 7 LED, 5(1)(d) GDPR, Principle 3 of Recommendation No. R (87) 15
Description	Another key principle of data protection is that of data accuracy. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16 LED.
Explanation	The principle of accuracy requires every reasonable step to be taken to keep data up to date and accurate.
National particularities	There are no significant differences in the national implementation of the accuracy principle.
BiH	Article 4(d) of the Bosnian LPPD requires controllers to process only authentic and accurate personal data, and update such data, when necessary, similarly to what is foreseen in Article 4(1)(d) LED. Article 7 LPPD adds that, if the incomplete and inaccurate data cannot be corrected or amended, and so taking into account the purpose for which they are collected or further processed, the controller must destroy them without delay.
BG	Articles 45(3) and 48(2) of the Bulgarian PDPA simply reproduce Articles 4(1)(d) and 7 LED.
IT	Articles 3(1)(d) and 4 of Decree 51 simply reproduce Article 4(1)(d) and 7 LED.

MD	Article 4 (1)(d) of the Moldovan LPDP simply reproduces Article 4(1)(d) LED. In letter (c), it states that the personal data subject to processing must be accurate and, if necessary, updated. Inaccurate or incomplete data from the point of view of the purpose for which they are collected and subsequently processed are deleted or rectified. Article 14(a) of the LPDP states that any subject of personal data has the right to obtain from the operator or the person authorized by it, upon request and free of charge rectification, updating, blocking or deletion of personal data whose processing contravenes this law, especially due to the incompleteness or inaccuracy of the data.
NL	Article 4 of the Dutch Police Data Act simply reproduces Articles 4(1)(d) and 7 LED.
ES	Articles 6(1)(d) and 10 of Organic Law 7/2021 simply reproduce Articles 4(1)(d) and 7 LED.

Requirement 5	***Storage limitation***
Level of criticality	2
Legal basis	Articles 5 LED, 5(1)(e) and 89(1) GDPR, Principle 7 of Recommendation No. R (87) 15
Description	Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.
Explanation	In principle, long-term storage of non-anonymized personal data is impossible from the legal point of view, with exceptions concerning, inter alia, scientific or historical research purposes. Procedures must be in place to support the timely assessment and deletion of data which is either no longer considered relevant and necessary or has been stored for the maximum period allowed for by law. This period of retention may vary based on the type of crime, database, category of data subject, police force processing the information and the purpose of the processing. In the event that data is no longer considered necessary, it can be stored when fully anonymized. Should the controller fail to conduct a periodic review of whether further processing is necessary, then data should be automatically deleted or pseudonymised.
National particularities	According to WP29, national laws transposing Article 5 LED should establish clear and transparent criteria for the assessment of the necessity to further keep personal data, as well as procedural requirements, including the involvement of the DPO. National approaches to transposing the LED's time limits for the storage and review of personal data vary widely.
BiH	

	Article 4 of the Bosnian LPPD establishes that the process of personal data shall take place only within the period of time necessary for the fulfilment of the purpose of their processing.
BG	Article 46 of the Bulgarian PDPA establishes that: (1) Where the time limits for the erasure of personal data or for a periodic review of the need for the storage are not statutorily established, the said time limits shall be established by the controller. (2) The carrying out of a periodic review under Paragraph (1) shall be documented, and the decision to extend the storage of the data shall be reasoned. Regarding data for law enforcement, according to Article 25(a) of the Ministry of Interior Act, the data storage terms are determined by the Minister of the Interior. These data can be also deleted in compliance with a court decision or a decision of the Commission for the Protection of Personal Data.
IT	No variations from the GDPR regarding storage limitation are provided by Italian data protection laws.
MD	Article 4(1)(e) of the Moldovan LPDP establishes that personal data undergoing processing must be kept for no longer than is necessary for the purposes for which the data were collected and further processed. It adds that storage of personal data for longer period for purposes of statistical, historical or scientific research, shall be performed in compliance with law regulating these fields. Article 11(1) adds that the conditions and time periods of personal data storage shall be set by law. Upon expiration of the storage time limit, the personal data shall be destroyed as established by law. The Instructions on the Processing of Personal Data in the Police Sector (Order of May 2013) establish that data should not be stored "for a term that exceeds achieving the proposed goals" (17). Art. 15(2) of LPDP states that processing of personal data for the purposes of national defence, of state security and the maintenance of public order, of the protection of the rights and freedoms of the subject of personal data or of other persons, if by their application the efficiency of the action or the objective pursued in the exercise of the legal powers of the public authority is prejudiced, cannot exceed the period necessary to achieve the objective pursued.
NL	The Dutch implementation of the LED foresees that personal data may be stored by the police for one year, a period which can be extended to five years if the data are necessary for the police tasks (Article 8).
ES	In Spain, Article 8(1) of Organic Law 7/2021 establishes the obligation of data controller to conduct a periodic review of whether conservation is necessary every three years. If possible, it will be done automatically. In (3), a maximum time limit of 20 years for deletion is provided, unless there are factors such as

	the existence of open investigations or offences for which the statute of limitations has not expired, the non-completion of the execution of the sentence, recidivism, the need to protect victims or other justified circumstances making the processing of the data necessary for law enforcement purposes.

Requirement 6	***Accountability***
Level of criticality	2
Legal basis	Articles 7(2) LED, 5(2) GDPR, Recital 74 GDPR, Principle 5 of Recommendation No. R (87) 15
Description	Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.
Explanation	For the purpose of improving accountability and data accuracy by guaranteeing a sufficient manner of traceability, the LED implements a strict requirement of logging practices.
National particularities BiH	Article 7(2) of the Bosnian LPPD establishes that if the incomplete and inaccurate data cannot be corrected or amended, and so taking into account the purpose for which they are collected or further processed, the controller must destroy them without delay. According to Article 40, the Agency for Personal Data Protection in Bosnia and Herzegovina has the competence to supervise the implementation of this law, including the supervision of the transfer of personal data out from Bosnia and Herzegovina.
BG	Article 48 of the Bulgarian PDPA simply reproduces Article 7 LED.
IT	Article 4(2) of Legislative Decree 51 of 2018 simply reproduces Article 7(2) LED.
MD	Article 26 of the Moldovan LPDP regulates how the National Centre for Personal Data Protection should control the lawfulness of personal data processing. According to Article 20(2)(d), the Centre has the competence to request from controllers the rectification, blocking or destruction of personal data which are inaccurate or obtained unlawfully. Besides, Article 33 establishes that for violations of this law, the convicted persons are liable under the civil, administrative or criminal law. On the 22nd of April 2022, Moldova approved the Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection. According to this

	instrument, the National Centre for Personal Data Protection can order the suspension or cessation of the cross-border transfer of personal data, if the national law of the controller or processor does not ensure an adequate level of personal data protection or does not comply with the Standard Contract. However, this does not apply if data protection is motivated by reasons related to national defence, national security, public order or the prevention, investigation and prosecution of criminal offences, etc.
NL	Article 4 of the Dutch Police Data Act establishes that the controller shall take all necessary measures to ensure that police data are correct and accurate in view of the purpose for which they are processed. The controller must ensure the immediate destruction or rectification of police data if it appears that these are incorrect in view of the purposes for which they are processed. The competent authority shall, as far as practicable, check the quality of police data before the data is provided. Besides, if it is established that incorrect police information has been provided, or that the police information has been provided in an unlawful manner, the recipient will be notified without delay. In that case, the data must be rectified or destroyed, or the processing must be limited.
ES	Article 10(2) of Organic Law 7/2021 simply reproduces Article 7(2) LED.

Requirement 7	***Distinction between categories of data subjects in law enforcement activities***
Level of criticality	3
Legal basis	Article 6 LED
Description	Article 6 LED distinguishes between different categories of data subjects: suspect, perpetrator, victim, witness, informant, contact and accomplice. Such a distinction is also necessary to ensure proper implementation of the principles relating to data processing (e.g., transparency and information to be given to the data subject). The crucial importance of updating those data at the end of the investigation/judicial proceeding can also affect the data accuracy and updating requirement.
Explanation	The purpose of this requirement is to avoid the misinterpretation of data by connecting identifiable persons with criminal acts without specifying the extent of their involvement. The distinction between different data subjects affects the application of many of the previous mentioned requirements such as: Lawfulness of the processing, Purpose limitation, Data minimization, Data accuracy and updating, Information to data subject in LEAs investigation

	activities. However, during a criminal investigation there is a certain fluidity in the categorisation of individuals linked with a crime, until the evidence that emerges leads to a concrete determination of the capacities of the individuals involved.
National particularities	The LED obliges Member States to require a data controller to draw a distinction, where applicable and as far as possible, between the data of different categories of data subjects, and to provide examples of those categories. There is no unanimity. Moreover, the non-Member States do not distinguish different categories of data subjects.
BiH	No information regarding different categories of data subjects is to be found in the Bosnian LPPD, nor in the amendments to this law adopted in 2011.
BG	Article 47 of the Bulgarian PDPA simply reproduces Article 6 LED.
IT	Article 4(1) of Decree 51 only refers to persons under investigation; accused persons; persons subject to investigation or accused in related or connected proceedings; persons convicted by a final judgment; persons aggrieved by the offence; civil parties; persons informed of the facts; witnesses.
MD	Article 3 of the Moldovan LPDP defines special categories of personal data which are the data that reveal the racial or ethnic origin of the person, his political, religious or philosophical beliefs, social affiliation, data regarding the state of health or sex life, as well as those related to criminal convictions, coercive procedural measures or contraventional sanctions. In this case, Article 23 LPDP imposes a DPIA.
NL	Article 6(b) of the Dutch Police Data Act simply reproduces Article 6 LED.
ES	Article 9 of Organic Law 7/2021 simply reproduces Article 6 LED.

Requirement 8	***Information to data subjects in law enforcement activities***
Level of criticality	2
Legal basis	Articles 6 and 13 LED, Articles 12 to 22, 34, 5, 89 GDPR, Principle 6 of Recommendation No. R (87) 15
Description	When processing personal data for the purposes of the LED, in order to enable the data subject to challenge the legality of the processing of personal data concerning them, the data subject has the right to be informed as a principle, particularly where the data are collected without their knowledge. This principle is exempted when such information would jeopardize ongoing investigations, expose a person to a danger or harm the rights and freedoms of others. Article 6 LED distinguishes between different categories of data subjects: suspect, perpetrator, victims, witnesses, informants, contacts and accomplices. Such a distinction is necessary to ensure proper implementation of the principles

	relating to data processing. So, when and if possible, the data subject will receive accurate and full information about the processing, including: (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended; (d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority; (e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject. Article 13 LED also envisages the opportunity to share information about the legal basis for the processing, the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period, the categories of recipients of the personal data, including in third countries or international organisations and further information, in particular where the personal data are collected without the knowledge of the data subject. However, these kinds of information may be excluded from the information provided to the data subject if there is a Member state law that delays, restricts or imposes to omit them in order to avoid obstructing official or legal inquiries, investigations or procedures, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protect public security, protect national security or protect the rights and freedoms of others.
Explanation	Criminal analysis requires the processing of different categories of persons with different degrees of involvement in heritage crime. The processing of personal data in this context must consider the role of the data subject in the crime. In practice, this means that personal data relating to a victim or a witness cannot be treated as if it concerned a suspect or a convict. The qualification as suspect, contact, victim or witness warrants a different treatment of their data, with different consequences for their fundamental rights.
National particularities BiH	Articles 22 and following of the Bosnian LPPD regulate the data subject's right to information. Article 24(1) establishes that the data controller shall notify the data subject on the progress of processing of his/her personal data performed either by the data controller or by a data processor, the purpose of the data processing, legal grounds for and duration of processing, if the data were collected from the data subject or a third party, the right to access personal data, as well as who has received or will receive data and for what purpose. As a general rule, on the basis of a written request of the data subject, the controller shall be obliged to provide the data subject with this information once per calendar year and free of charge (Article 25(1)). However, Article 28

	establishes that the data controller is exempt from this obligation if providing such information could cause significant damage to legitimate interests of Bosnia and Herzegovina, specifically including the prevention, investigation, detection of crimes and prosecution of perpetrators.
BG	Following Article 23 of the GDPR, the Bulgarian Act provides that the controller or processor may refuse fully or partially the exercise of data subjects' rights under Articles 12 to 22 of the GDPR, and is allowed not to fulfil their obligation under Article 34 of the GDPR, where their exercise would create a risk for example towards the national security, defence, public order, and security, the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties. The terms and conditions for application of this provision should be further regulated by a specific law.
IT	Article 10 of Decree 51 simply reproduces Article 13(1)-(2) LED. Article 14 of Decree 51 adopts legislative measures delaying, restricting or omitting the provision of the information to the data subject, as allowed, under certain conditions, by Article 13(3) LED.
MD	Article 12 of the Moldovan LPDP includes all the information the data subject must be provided with, distinguishing between those cases in which personal data are collected directly form the personal data controller or processor and those cases in which the personal data were not directly collected from them. However, article 15 of the Moldovan LPDP states that this provision shall not apply where the processing of personal data is carried out in the context of actions of prevention and investigation of criminal offences, enforcement of convictions and other activities within criminal or administrative procedures, in terms of the law.
NL	Articles 24(b) and 27 of the Dutch Police Data Act reproduces Article 13 LED. Article 24(b) does not make reference to a data subject's right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning him or her. The Dutch DPA has issued guidelines on the processing of personal data by the police, in the judicial system, and during private investigations.[2]
ES	Article 21 of Organic Law 7/2021 simply reproduces Article 13(1)-(2) LED. Article 24 allows the data controller to delay, restrict or omit the provision of the information to the data subject pursuant to Article 21(2), and to deny partially or fully the rights to access and to rectification or erasure of personal data and restriction of processing.

[2] Available in Dutch at Politie en justitie | Autoriteit Persoonsgegevens.

Requirement 9	Processing of special categories of personal data (sensitive data)
Level of criticality	3
Legal basis	Article 10 LED, Recital 37 LED, Article 9 GDPR, Recitals 51, 52, 53 and 54 GDPR, Principle 2(4) of Recommendation No. R (87) 15
Description	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject.
Explanation	Some personal data are by their nature particularly sensitive, because their processing involves significant risks to data subjects' fundamental rights and freedoms. For this reason, processing of these sensitive data is, as a general rule, prohibited. However, it can be allowed if it is explicitly foreseen by the law (both EU and national legislation), to protect the vital interests of the data subject or of another natural person, or when such processing relates to data which are manifestly made public by the data subject. According to the GDPR, States can authorise the processing of sensitive data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The derogation from the prohibition on processing special categories of data should also be allowed when it is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. In any case, the processing of sensitive data must always be subject to special safeguards. These safeguards can include the possibility to collect them only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, the establishment of stricter rules on the access of staff of the competent authority to the data or the prohibition of transmission of those data. The collection of certain sensitive data can be sometimes necessary for police purposes. According to Recommendation No. R (87) 15, it should only be authorised if 'absolutely necessary for the purposes of a particular inquiry'.

	Such an inquiry should be based on strong grounds for believing that serious criminal offences have been or may be committed. The collection of sensitive data in such circumstances should, moreover, be 'absolutely necessary' for the needs of such inquiries. In no circumstances should such data be collected simply in order to allow the police to compile a file on certain minority groups whose behaviour or conduct is within the law. The reference to sexual behaviour does not apply where an offence has been committed.
National particularities BiH	Bosnian LPPD slightly modifies the definition of special categories of data: it adds 'criminal convictions', as well as 'nationality' or 'national origin' and [political] 'party affiliation'. However, it does not expressly mention genetic data, biometric data or sexual orientation. Article 11 of the Bosnian LPPD establishes that data processing of special categories of data shall be examined by the Data Protection Commission following receipt of a notification from the controller that such data is to be processed. Such processing operations must only be started after the Data Protection Commission has completed its examination or two months have passed since the Commission has been notified.
BG	Article 45 of the Bulgarian PDPA establishes that the processing of sensitive data (same categories as Articles 10 LED and 9 GDPR) shall be allowed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject and is provided for in Union law or in the legislation of the Republic of Bulgaria. When processing of such data is not provided for in EU or Bulgarian law, these data can still be processed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject, and: 1. the processing is necessary to protect the vital interests of the data subject or of another natural person, or 2. if the processing relates to data which are manifestly made public by the data subject. This article adds that suitable measures and safeguards for non-discrimination against natural persons shall be put in place where sensitive data are processed.
IT	Article 7 of Decree 51 indicates that processing of sensitive data referred to in Articles 10 LED and 9 GDPR is authorised only if it is strictly necessary, in the cases specified in EU law and assisted by adequate safeguards of the rights and freedoms of the data subject and specifically provided for by EU law or by Italian regulation. Specific safeguards are still to be developed by Italian competent authorities.
MD	Article 6 of the Moldovan LPDP establishes that the processing of special categories of personal data shall be prohibited, except for a list of cases, which are substantially the same as those included in article 9 GDPR. However, the Moldovan LPDP slightly modifies the categories of data that can be considered

	sensitive. It adds "data relating to criminal convictions, administrative sanctions or coercive procedural measures". Besides, it mentions "social belonging" instead of "trade union membership", and it does not explicitly include genetic or biometric data. The Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection (Order no. 33, 22nd April 2022) establishes that, when such transfer involves sensitive data, the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data only for staff having followed specialised training, keeping a record of access to the data, strict purpose limitation, as well as additional security measures (such as pseudonymisation) and restrictions with respect to further disclosure.
NL	Section 22 of the Dutch GDPR Implementation Act refers to the same categories of sensitive data as Articles 10 LED and 9 GDPR. It indicates that, as a general rule, their processing is prohibited. However, a number of cases are established in which these sensitive data may be processed. These cases are those already mentioned in Article 10 LED and other cases provided for in national law. In fact, Section 22 of the Dutch GDPR Implementation Act specifies that the prohibition on processing special categories of personal data does not apply if the data subject has given explicit consent; processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim in the course of its legitimate activities and with appropriate safeguards, and on condition that the processing relates solely to the members or ex members; when processing relates to personal data which are manifestly made public by the data subject; or when processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity. According to Section 23, the prohibition on processing special categories of personal data does not apply if it is necessary to comply with an obligation under international law; the data are processed by the Dutch DPA or an ombudsman and in so far as processing is necessary for the performance of the tasks entrusted to them by law, provided specific safeguards; or when processing is necessary relating to criminal law matters. Section 24 permits the processing of special categories of personal data if it is necessary for scientific or historical research purposes or statistical purposes; the research referred to in a. serves a public interest; when it is impossible or would involve a disproportionate effort to request express consent; and when safeguards have been put in place for the processing

such that the data subject's privacy is not disproportionately compromised. Section 25 accepts the processing of personal data revealing racial or ethnic origin to identify the data subject and only in so far as such processing is unavoidable for that purpose; or with the purpose of conferring a preferential position on persons of a certain ethnic or cultural minority group in order to eliminate or reduce the actual disadvantages connected with race or ethnicity, only if processing is necessary for that purpose; the data relate to the country of birth of the data subject, his or her parents or grandparents, or to other criteria set by law on the basis of which it can objectively be determined whether a person belongs to a certain ethnic or cultural minority group; and the data subject has not objected to the processing in writing. Section 26 establishes that the prohibition on processing personal data revealing political opinions does not apply if the processing is carried out with a view to requirements on political opinions that may reasonably be imposed in connection with the performance of duties in administrative bodies and on advisory boards. Section 27 accepts the processing of personal data revealing religious or philosophical beliefs for spiritual care if the processing is carried out by specific institutions, and in so far as the processing is necessary for the purpose of providing spiritual care to the data subject, unless he or she has objected to this in writing. According to Section 28, the prohibition on processing genetic data does not apply if such processing is carried out in relation to the data subject from whom the data concerned have been collected and: (a) a substantial medical interest prevails; (b) the processing is needed for scientific research that serves a public interest or for statistical purposes, with specific safeguards for the processing such that the data subject's privacy is not disproportionately compromised. The consent is not required if it proves impossible or would involve a disproportionate effort to request express consent. According to the Section 29, the prohibition of processing of biometric data for the purpose of uniquely identifying a natural person does not apply if the processing is necessary for authentication or security purposes. Section 30 accepts the processing data concerning health if it is carried out by administrative bodies, pension funds, employers or institutions that perform activities on their behalf in so far as this is necessary for proper compliance with legal requirements, pension schemes or collective employment contracts that provide entitlements which depend on the data subject's health status; or the reintegration or support of employees or recipients of welfare benefits in connection with illness or disability. Processing data concerning health is also permitted when made by schools, an institution of rehabilitation, a special probation officer, the Child Care and Protection Board, a certified body for those purposes, when it is necessary to give special support for pupils or making special arrangements in connection

	with their health status. The processing can also be made by the Minister and the Minister of Justice and Security in so far as the processing is necessary for the enforcement of measures involving the deprivation of liberty. The prohibition on processing data concerning health does not apply if the processing is carried out by healthcare providers, institutions or health care or social services facilities in so far as the processing is necessary for the proper treatment or care of the data subject or for the management of the institution or professional practice concerned. It is also permitted when made by specific insurers of the Financial Supervision Act or financial service providers who provide insurance brokerage services as referred to in Section 1(1) of that Act, in so far as the processing is necessary to assess the risk to be insured if the data subject has not made any objection and to perform the insurance agreement or to assist in the management and implementation of the insurance.
ES	Article 13 of Organic Law 7/2021 refers to the same categories of sensitive data as Articles 10 LED and 9 GDPR and allows their processing, with the corresponding legal safeguards, in the cases indicated in Article 10 LED. Article 13 of Organic Law 7/2021 specifically allows competent authorities to process biometric data intended to uniquely identify a natural person for the purposes of prevention, investigation, detection of criminal offences, including the protection and prevention of threats to public security. Lastly, if the data concerned are of minors (under 18 years of age) or persons with legally modified capacity, they shall be processed in their best interest and with an appropriate level of security.

Requirement 10	***Automated decision-making, including profiling***
Level of criticality	3
Legal basis	Articles 11 LED, 22 and 23 GDPR, EDPB Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679[3]
Description	In Article 11(1) LED, there is a reference for Member States having to establish that decisions based solely on automated processing, including profiling, which produce an adverse legal effect concerning the data subject or significantly affects them, shall be prohibited unless authorised by an EU or Member State law to which the controller is subject and which provides appropriate safeguards to the rights and freedoms of the data subject, at least to obtain human intervention on the part of the controller.
Explanation	Automated decisions producing adverse legal effects are thus not fully prohibited under the LED but conditioned to the existence of a legal provision

[3] Available in English at https://ec-europa-eu.accedys.udc.es/newsroom/article29/items/612053.

	providing for some safeguards. In relation to these safeguards, the Guidelines noted that any processing likely to result in a high risk to data subjects requires the controller to carry out a DPIA, which might be particularly useful for controllers who are unsure whether their proposed activities will fall within the Article 22(1) definition, and, if allowed by an identified exception, what safeguarding measures must be applied (ibid., 20).
National particularities BiH	Article 29 of the Bosnian LPPD establishes the following: (1) The controller shall not issue a decision producing legal effects in regard of the data subject or a decision which may considerably affect the data subject while being aimed at evaluating certain personal characteristic of the data subject, solely on the basis of automatic data processing. (2) Notwithstanding the provision of Paragraph 1 hereof, the decision issued solely based on automated data processing shall generate legal effects for the data subject in the following cases: a) in a procedure of entry into a contract or implementation of the contract, provided that the request of the data subject is fulfilled or that there are appropriate protection measures of his lawful interests such as a procedure that allows him/her to protect his/her position; or b) if the controller is authorised by a law, which also defines protection measures relevant to lawful interests of the data subject, to issue such a decision.
BG	Article 52 of the Bulgarian PDPA simply reproduces Article 11 LED.
IT	Article 8 of Decree 51 simply reproduces Article 11 LED.
MD	Article 23 of the Moldovan LPDP establishes that systematic and comprehensive assessment of personal matters relating to natural persons, which are based on automatic processing, including profiling, and which are based on automated decisions which produce legal effects on the natural person, require the controller to seek the opinion of the data protection officer and carry out a DPIA before processing. Article 13(1)(c) of LPDP states that any data subject has the right to obtain from the operator, upon request, without delay and free of charge information on the principles of operation of the mechanism through which the automated processing of data is carried out that concerns the subject of personal data. Article 17 of the LPDP stipulates that any person has the right to request the cancellation, in whole or in part, of any individual decision that produces legal effects on his rights and freedoms, being based exclusively on the automated processing of personal data intended to evaluate some aspects of his personality, such as competence professional, credibility, behaviour and the like. The person may be subject to such a decision if the decision is authorized by a law that establishes the measures that guarantee the protection of the

	legitimate interest of the subject of personal data and the decision is taken within the framework of the conclusion or execution of a contract, provided that the request for the conclusion or execution of the contract submitted by the subject of personal data has been satisfied.
NL	Article 7(a) of the Dutch Police Data Act reproduces Article 11 LED, but allows automated decision-making based on special categories of data whenever the Dutch DPA has been consulted.
ES	Article 14 of Organic Law 7/2021 simply reproduces Article 11 LED.

Requirement 11	***Data protection by design and by default***
Level of criticality	2
Legal basis	Article 20 LED
Description	1. Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects. 2. Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
Explanation	Due to the nature of data stored in the system, which includes personal data, the system itself must be secured against any threat of intrusion, violation, breach or alteration. Data protection must be a default setting. Moreover, privacy and ethical values must be embedded into the design, as an essential component of the system. In order to ensure the privacy-by-design approach, the system will use privacy friendly principles as default options.
National particularities BiH	Data protection by design or by default are concepts used by EU Member States, but not by Bosnia and Herzegovina and Moldova.

	There is no reference to DP by design or by default in the Bosnian LPPD or the Law on Amendments to the LPPD.
BG	Article 59(3) of the Bulgarian PDPA simply reproduces Article 20 LED.
IT	Article 16 of Decree 51 simply reproduces Article 20 LED.
MD	Article 23 of the Moldovan LPDP stipulates that the DPIA should contain risk prevention measures, including guarantees, security measures and mechanisms designed to ensure the protection of personal data and demonstrate compliance with the provisions of this law, taking into account the rights and legitimate interests of data subjects and other interested persons. Also, Article 30(1) of the LPDP obliges the operator to take the necessary organizational and technical measures for the protection of personal data against destruction, modification, blocking, copying, distribution, as well as against other illegal actions, measures aimed at ensuring an adequate level of security in terms of the risks presented by the processing and the character processed data.
NL	Article 4(a) of the Dutch Police Data Act regulates the data protection by design principle. The controller and the processor shall take appropriate technical and organisational measures: a. to ensure and to be able to demonstrate that the processing of police data is carried out in accordance with what is provided for by or pursuant to this Act; b. data protection policies and principles on an effective carry out or apply the manner; c. the necessary safeguards for the determination of the means of processing and the processing itself, such as pseudonymisation, to be incorporated into the processing in order to comply with what is or is determined under this Law and to protect the rights of the data subjects. 2. The controller and the processor shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular with regard to the processing of the special categories of police data, referred to in Article 5, and in such a way that police data is protected against unauthorised or unlawful processing and against intentional loss, destruction or damage. 3. When taking the measures referred to in the first and second paragraphs, the controller and processor take into account the nature, scope, the context and purposes of the processing, as well as the probability of and seriousness of varying risks to the rights and freedoms of natural persons. 4. In addition to the third paragraph, the controller and the processor with regard to the first paragraph, under c, and the second paragraph, take into account the position of the technology and the implementation costs.

	5. The measures referred to in the first and second paragraphs shall be periodically evaluated. and, if necessary, updated. 6. By or pursuant to a general administrative order, further rules are laid down on the measures referred to in the first and second paragraphs. Article 4(b) of the Dutch Police Data Act simply reproduces Article 20(2) LED.
ES	Article 28 of Organic Law 7/2021 simply reproduces Article 20 LED. The Spanish DPA has issued Guidelines for Data Protection by Default.[4]

Requirement 12	***Record and logging of processing activities***
Level of criticality	3
Legal basis	Articles 24 and 25 LED
Description	The former provision mirrors the correspondent Article 30 GDPR and provides that controllers keep record of various information related to their data processing, to be made available to DPAs upon request. The latter is instead a peculiarity of the LED and requires that, for each processing operation, the time, the identification of the operator accessing the data, the possible recipients, and the justification for the processing operation itself are registered.
Explanation	As law enforcement databases contain high volumes of information on a large number of individuals, a lot of which are sensitive data, records and logs play a central role in ensuring that such databases are not being abused and are only accessed by persons with proper authorization and with valid reasons to access retained data. Overall, this improves the transparency of data processing activities, the accountability of controllers and the effective capability for supervisory authorities to oversee data processing.
National particularities BiH	Article 11 of the Bosnian LPPD requires the controller and the processor to take measures against unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transfer, other forms of illegal data processing, as well as measures against misuse of personal data. Article 13 lists the information that shall be recorded by controllers, but this list does not include keeping record of accesses to the data.
BG	Articles 62 and 63 of the Bulgarian PDPA simply reproduce Articles 24 and 25 LED.
IT	Articles 20 and 21 of Decree 51 simply reproduce Articles 24 and 25 LED.
MD	In Moldovan LPDP it is not expressly stipulated about the record and logging of processing as it is in Articles 24 and 25 LED, but still has the provision regarding the presence of personal data record system which are any structured series of personal data accessible according to specific criteria, whether it is centralized,

[4] Available in English at Guidelines for Data Protection by Default (aepd.es).

	decentralized or distributed according to functional or geographical criteria. For example, Article 15(1) of the Law 320/2012 stipulates that for the efficient execution of its duties, the Police has the right to collect, process and keep information about people who have committed illegal or harmful acts, to create and use their own databases, to use the databases of other authorities, with compliance with the provisions of the legislation regarding the protection of personal data. Article 4(1)(e) states that personal data that are the subject of processing must be stored in a form that allows the identification of the subjects of personal data for a period that will not exceed the duration necessary to achieve the purposes for which they are collected and subsequently processed. The storage of personal data for a longer period, for statistical, historical or scientific research purposes, will be done in compliance with the guarantees regarding the processing of personal data, provided by the rules governing these fields, and only for the period necessary to achieve these purposes. Also, at the national level there are State Registers with personal data. Article 11(2) of the LPDP states that the personal data from the state registers, from the date of termination of their use, may remain in storage receiving the status of an archive document.
NL	Articles 31(d) and 32(a) of the Dutch Police Data Act simply reproduce Articles 24 and 25 LED.
ES	Articles 32 and 33 of Organic Law 7/2021 simply reproduce Articles 24 and 25 LED.

Requirement 13	***Security of processing***
Level of criticality	2
Legal basis	Article 29 LED, Principle 8 of Recommendation No. R (87) 15
Description	Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to: (a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

	(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control'); (c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control'); (d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control'); (e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control'); (f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control'); (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control'); (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control'); (i) ensure that installed systems may, in the case of interruption, be restored ('recovery'); (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').
Explanation	One of the core obligations for all data controllers or data processors is that of the security of personal data processing. Technical and organisational measures must be put in place to ensure that data are protected with an appropriate level of security. Appropriate security includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
National particularities BiH	Article 11 of the Bosnian LPPD establishes that the data controller and processor shall take care of data security and shall take all technical and organisational measures and develop rules of procedure required to implement this law. This article adds that the controller and, within the scope of its competencies, the processor shall be required to develop the data security plan, which shall specify technical and organizational measures for security of personal data. The Council of Ministers of Bosnia and Herzegovina shall, upon obtaining the prior opinion from the Agency, prescribe the methodology of safekeeping and special measures of technical protection. Still in force, there are Rules on the manner of keeping and special measures of personal data technical protection,[5] 2 July 2009.

[5] Available in English (official translation) at: http://azlp.ba/propisi/default.aspx?id=1322&langTag=bs-BA.

BG	Article 66 of the Bulgarian PDPA simply reproduces Article 29 LED.
IT	Article 25 of Decree 51 simply reproduces Article 29 LED.
MD	Article 30 of the Moldovan LPDP establishes that the controller must implement appropriate technical and organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risk represented by the processing and nature of the data. Besides, the controller must choose a processor that shall ensure sufficient guarantees in respect to the technical security measures and organizational measures governing the processing to be carried out. Article 16(2) of Law No. 320/2012 states that the police ensure the protection of information, including personal data, against destruction, loss, unauthorized access. Article 5(1) of Law No. 59/2012 provides that the persons who have access to the personal data of the person subject to the special investigation measure are obliged to maintain the confidentiality of the respective data in accordance with the provisions of LPDP.
NL	Article 36(c) of the Dutch Police Data Act establishes that the controller shall take appropriate technical and organisational measures to protect police data against accidental or unlawful destruction, modification, unauthorised communication or access, in particular if the processing is transmitted over a network or made available through direct automated access and against all other forms of unlawful processing, in particular: the risks of the processing and the nature of the protection to be protected are taken into account. It should ensure these measures, taking into account the state of the art and the cost of implementation, an appropriate level of security, having regard to the risks of processing and the nature of police data.
ES	Article 37 of Organic Law 7/2021 simply reproduces Article 29 LED.

Requirement 14	***Communication of personal data breaches to supervisory authorities***
Level of criticality	2
Legal basis	Articles 30 LED, 34 GDPR, Recitals 85-88 GDPR, EDPB Guidelines on Personal data breach notification under Regulation 2016/679
Description	1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

	2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article. 6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.
Explanation	Supervisory authorities will be informed of any occurred breach of the security of the servers leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, as well as about any possible remedies.
National particularities BiH	In Bosnia and Herzegovina, the applicable data protection legislation does not impose data security breach notification duties on the controller. However, a duty on the database's administrator, processor or other person handling the data is to inform the controller of any attempt of unauthorized access to information system for the database's management. Pursuant to the Draft Data Protection Law in case of a personal data breach the controller is obliged to undue delay and where feasible not later than 72 hours after having become aware of it, which fully corresponds to the obligation prescribed by GDPR.
BG	The Bulgarian Act does not implement exemptions or variations from the GDPR on breach notification to the supervisory authority.
IT	

MD	Article 26 of Decree 51 does not introduce substantive changes in this obligation. The Garante has issued guidelines and templates concerning data breaches, providing a dedicated email address for due notification. In Moldova, data controllers shall submit to the NCPDP an annual report on any security incidents involving information systems during that year. According to Article 20(1)(m) of the LPDP, the NCPDP notifies the law authorities in the event of the existence of indications regarding the commission of crimes related to the violation of the rights of the subjects of personal data.
NL	Article 33(a)(1)-(4) of the Dutch Police Data Act simply reproduces Article 30 LED.
ES	Article 38 of Organic Law 7/2021 simply reproduces Article 30 LED.

Requirement 15	***Communication of personal data breaches to data subjects***
Level of criticality	2
Legal basis	Article 31 LED, 33 GDPR, Recitals 85-88 GDPR, EDPB Guidelines on Personal data breach notification under Regulation 2016/679
Description	Data subjects will be informed only where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.
Explanation	According to Article 13(3) LED, Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

	(c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others.
National particularities BiH	In Bosnia and Herzegovina, the applicable data protection legislation does not impose data security breach notification duties on the controller. However, a duty on the database's administrator, processor or other person handling the data is to inform the controller of any attempt of unauthorized access to information system for the database's management.
BG	Regarding communication of a personal data breach to the data subject, the Bulgarian Act contains exemptions for cases where there is a risk for the national security, defence, public order and security, the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, etc., where the terms and conditions should be governed by a specific law (Article 37(a) of the Act). The Act does not establish specific sectoral obligations with respect to data breach notification, besides processing activities performed by courts and prosecution authorities where notifications should be filed with the Inspectorate to the Supreme Judicial Council instead of the CPDP.
IT	Article 27 of Decree 51 does not introduce substantive changes in this obligation.
MD	Article 14 of the Moldovan LPDP establishes that any personal data subject has the right to obtain from the controller, free of charge, a rectification, update, blocking or erasure of personal data, the processing of which does not comply with this law. However, article 15 foresees that this provision shall not apply if the processing of personal data is carried out in the context of actions of prevention and investigation of criminal offences, enforcement of convictions and other activities within criminal or administrative procedures.
NL	Article 33(a)(5)-(7) of the Dutch Police Data Act simply reproduces Article 31 LED, not including, though, Article 31(4) LED.
ES	Article 39 of Organic Law 7/2021 simply reproduces Article 31 LED. The AEPD has stated in its updated Guide on personal data breach notification[6] that when data subject notification may compromise the outcome of an ongoing investigation, the controller may delay notification under the AEPD's supervision.

[6] AEPD, Guía para la notificación de brechas de datos personales.

Requirement 16	*Data Protection Impact Assessment*
Level of criticality	3
Legal basis	Articles 27 LED, 9, 10 and 35 GDPR
Description	Article 35(1) GDPR requires controllers to conduct a data protection impact assessment (DPIA) before processing when the data processing activity is likely to result in a high risk to data subjects' rights and freedoms. Article 35(3) GDPR specifically requires DPIAs when the controller engages in: • Automated processing, including profiling, that produces legal or other significant effects for a data subject. • Large-scale processing of special categories of personal data (Article 9 GDPR) and criminal conviction and offense data (Article 10 GDPR). • Large-scale systematic monitoring of a publicly accessible area. The list is not exhaustive, and other processing activities may require DPIAs. The general requirements for a DPIA in the police sector are laid down in Article 27 LED. The minimum elements are the following: a general description of the envisaged processing operations; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address those risks; the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with LED, while taking into account the rights and legitimate interests of data subjects and other persons concerned.
Explanation	The DPIA is a tool for helping decision-making and design strategy concerning data processing, including the choice of the appropriate security measures to put into place to ensure the protection of personal data and safeguard the rights and freedoms of natural persons.
National particularities BiH	The GDPR permits supervisory authorities to establish lists of the types of processing activities requiring a DPIA and the types of processing activities that do not require a DPIA (Article 35(4)-(5) GDPR). In Bosnia and Herzegovina, no DPIA needs to be carried out in certain circumstances.
BG	In Bulgaria, the CPDP adopted a List of processing operations requiring data protection impact assessment pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679[7] of the processing activities where DPIA is mandatory. Pursuant to the List, data controllers whose main or only place of establishment is in the territory of Bulgaria will be required to conduct a DPIA when carrying out the following types of processing operations: • large scale processing of biometric data for the unique identification of the individual which is not sporadic;

[7] Available in English at https://www.cpdp.bg/en/index.php?p=element&aid=1186.

- processing of genetic data for profiling purposes which produces legal effects for the data subject or similarly significantly affects them;
- processing of location data for profiling purposes which produces legal effects for the data subject or similarly significantly affects them;
- processing operations for which the provision of information to the data subject pursuant to Article 14 of the GDPR is impossible or would involve disproportionate effort or is likely to render impossible or seriously impair the achievement of the objectives of that processing, when they are linked to large scale processing;
- personal data processing by controller with main place of establishment outside the EU when its designated representative for the EU is located on the territory of the Republic of Bulgaria;
- regular and systematic processing for which the provision of information pursuant to Article 19 of GDPR by the controller to the data subject is impossible or requires disproportionate efforts;
- processing of personal data of children in relation to the offer of information society services directly to a child; and
- migration of data from existing to new technologies when this is linked to large scale data processing.

IT

In Italy, Article 23 of Decree simply reproduces Article 27 LED. The Garante adopted the same list contained in the Guidelines on DPIA (wp248rev.01).[8]

MD

In Moldova, controllers have the obligation to perform a DPIA, taking into account the nature, scope, context, and purposes of the processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons. Prior to the processing, the controller shall carry out an DPIA of the envisaged processing operations on the protection of personal data. The DPO must issue an opinion on the performed DPIA. The DPIA is required upon:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences referred to a natural person; and
- a systematic monitoring of a publicly accessible area on a large scale.

[8] Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018, available in Italian at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979.

The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

According the NCPDP's Order 27 of 31 March 2022, the types of processing operations that are subject to a DPIA are:

1. The processing of personal data in order to carry out a systematic and comprehensive evaluation of the personal aspects related to natural persons, which is based on automatic processing, including the creation of profiles, and which is the basis of automated decisions that produce legal effects regarding the natural person or which affects it, similarly, to a significant extent.

2. The processing, on a large scale, of some categories of data that refer to the disclosure of racial or ethnic origin, political opinions, religious confession or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for unique identification of a natural person, data on health or data on sex life or sexual orientation, on criminal convictions and offenses of a natural person.

3. Processing of personal data with the aim of systematic monitoring, on a large scale, of an area accessible to the public.

4. Large-scale processing of personal data of vulnerable persons (such as asylum seekers, elderly persons, patients, minors, persons in respect of whom the judicial protection measure was instituted and employees), through automatic means of monitoring and/ or systematic recording of behaviour, including in order to carry out advertising, marketing and advertising activities.

5. Large-scale processing of personal data through the innovative use or implementation of new technologies, especially if the respective operations limit the ability of natural persons to exercise their rights.

6. Large-scale processing of data generated by sensor devices that transmit data via the Internet or other means.

NL	7. Large-scale and/or systematic processing of traffic and/or location data of natural persons, when the processing is not necessary for the provision of a service requested by the data subject. Article 4(c) of the Dutch Police Data Act simply reproduces Article 27 LED. Paragraph 3 allows the controller to carry out a review to assess whether the processing is carried out in accordance with the DPIA. The Dutch AP has published an overview of types of processing activities that require a DPIA.[9] This includes processing activities related to large-scale or systematic monitoring in convert investigations; of location data; of communications data; blacklists of personal data concerning criminal convictions and offences, wrongful conduct, obstinate behaviour, and payment performance; systematic and extensive assessment of personal traits by means of automated processing (profiling), such as the assessment of professional performance; etc.
ES	In Spain, Article 35 of Organic Law 7/2021 reproduces Article 27 LED. Moreover, it authorizes the DPA to establish a list of activities that require or do not require a DPIA. The AEPD has issued lists of activities which require ('Blacklist')[10] or do not require ('Whitelist')[11] a DPIA. The Blacklist contains activities such as processing that involves: profiling or the evaluation of subjects; automated-decision making or that makes a significant contribution to such decision-making; the observation, monitoring, supervision, geo-location, or control of the interested party in a systematic and extensive manner, including the collection of data and metadata via networks, applications, or in publicly accessible areas, as well as the processing of unique identifiers that allow the identification of users of services of the information society, such as web services, interactive TV, mobile applications, etc.; the use of special categories of data as referred to in Article 9(1) GDPR; data concerning criminal convictions and offences as referred to in Article 10 GDPR; the use of data on a large scale; the use of new technologies or an innovative use of consolidated technologies, including the use of technologies on a new scale, for a new purpose, or in combination with others, in a manner that entails new forms of data collection and usage that represents a risk to people's rights and freedoms, etc.

2.2.3 Other legal requirements related to the gathering of criminal intelligence

The RITHMS platform is intended as an investigative tool for LEAs gathering criminal intelligence. In this section we analyse what legal requirements for the deployment of online investigatory powers exist (or do not) at European level and in the countries of LEAs involved in the Consortium. Whenever

[9] Available in Dutch at: stcrt-2019-64418.pdf (autoriteitpersoonsgegevens.nl)-)

[10] Available in English at: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf.

[11] Available in English at: https://www.aepd.es/sites/default/files/2019-09/ListaDPIA-35-5-Ingles.pdf.

implemented for the criminal investigation of a concrete case in the context of a criminal proceeding, the use of the platform will be governed by criminal procedure laws. Requirements oriented to ensuring that information gathered through the RITHMS platform can be used in a judicial process will be studied in WP2, more concretely in Task 2.5 - Verification and validation of potential AI-based evidence in criminal cases. Guidelines and recommendations on validation planning and testing for evidential AI systems will be then provided: D2.6 - Report on validation requirements for AI-based evidence (StAG, R, SEN, M24).

In many EU Member States there is no specific regulation on intelligence-led policing (ILP), nor, therefore, on the limits or requirements of such activity, which is necessarily characterized by its secretive and preventive nature. Moreover, the use of new technologies, such as the one developed in RITHMS, is a relatively new phenomenon. It is therefore not surprising, considering the notion of 'law lag', that not even all Member States examined have specific legislative provisions. Furthermore, those EU and non-EU Member States that do have specific legislative provisions have, for the most part, enacted them, recently. In this regard, two of the countries examined do not have specific legal provisions that authorize and govern the use of a tool such as the RITHMS platform: Italy and Spain. Rather, its use must be included into the existing investigative powers.

Italy and Spain

Despite the lack of legal regulation, in order to ensure that concrete applications of the ILP paradigm comply with international human rights standards and do not have a negative impact on human rights, some fundamental principles must be observed in its design and implementation at the national level. According to the OSCE Guidance on Intelligence-led Policing, intelligence-led policing should comply with the following parameters:

- Firstly, ILP must be based on clear and precise legal and administrative provisions, setting out the conditions under which it is to be implemented and providing adequate safeguards to ensure that it does not jeopardise human rights (**principle of legality**).
- Secondly, interferences with fundamental rights implied by ILP should only be permissible if they are stipulated by law, if they are necessary to achieve a legitimate aim and are proportionate to the achievement of that aim (**proportionality**).
- To guarantee the rights to **equality and non-discrimination**, when collecting, processing and analysing information and intelligence, law enforcement officers should refrain from deploying controls or profiling that discriminate on the basis of birth, race, sex, religion, opinion or any other personal or social status or circumstance. A diversity and gender-sensitive approach should therefore be incorporated into all ILP activities and regularly reviewed for any discriminatory impact it may have on men or women, or on particular communities.

- International human rights law stipulates the right of any person whose rights or freedoms have been violated to an **effective remedy**, as well as the right to seek and obtain a remedy and to have it decided by the competent judicial, administrative or legislative authority. Since ILP can have far-reaching implications for a wide range of human rights - notably the right to privacy and the protection of personal data -, effective and accessible remedies for violations of these rights that may result from its implementation are essential.
- Finally, it is also necessary to establish mechanisms to hold those responsible for carrying out these activities accountable (**accountability**).

Moldova

Moldova, on the contrary, has a Law No. 59/2012 on Special Investigation Activity. It defines the special investigative activity as 'a procedure of a secret and/or public nature, undertaken by the competent authorities, with or without the use of special technical means, with the purpose to collect necessary information for the prevention and fight against crime, ensuring the security of the state, public order, protection of rights and legitimate interest of persons, discovery and investigation of crimes' (Article 1(1)). The law regulates the special investigative measures, their method of ordering and enforcement, as well as control over their legality (Article 1(2)). Moreover, the Criminal Procedure Code has provisions on special investigation activities and the use of technical means in such of activities (Articles 1321 to 1383). Article 164 of the Moldovan Criminal Procedure Code states that audio or video recordings, photographs, means of technical, electronic, magnetic, optical control and other carriers of technical-electronic information, obtained under the terms of this code, constitute means of evidence if they contain data or fundamental indications regarding the preparation or commission of a crime and if their content contributes to finding out the truth in that case.

Bulgaria

In Bulgaria there is no specific regulation on technological investigative techniques. However, a regulation on obtaining criminal information can be found in the Criminal Procedure Code, in its section VIII of chapter 14 'Special intelligence tools' from Article 172 to 177, and in the Special Intelligence Assets Act.

Special intelligence means are understood as technical means and operational methods for their application, which are used to prepare physical evidence - film recordings, video recordings, sound recordings, photographs and marked objects. Technical means are electronic and mechanical equipment, as well as substances that serve to document the activity of controlled persons and objects (Article 2 of the Special Intelligence Asset Act). In the Criminal Procedure Code, special intelligence means are defined as 'technical means - electronic and mechanical equipment and substances that serve to document the activity of controlled persons and objects, and operational methods - monitoring, eavesdropping, tracking, penetration, marking and inspection of correspondence and computer information, controlled delivery, trust transaction and investigation by undercover officer' (Article 172(1)).

The measures foreseen both in the Criminal Procedure Code and in the Special Intelligence Asset Act are: monitoring, eavesdropping, tracking, penetration, marking and verification of correspondence and computerized information, controlled delivery, confidential transaction and the investigation by an undercover officer. As there is no technological measure specifically foreseen, we must follow the general procedure regulated for intelligence means. Article 6 of the Special Intelligence Assets Act refers to communications by electronic means and Article 19b of the Special Law cites the control of data transmission and reception of information through wired means of communication, in which we could include communications through fibre optics.

Intelligence means are used when deemed necessary in the investigation of serious intentional crimes of Chapter One, Chapter Two, Sections I, II, IV, V, VIII and IX, Chapter Three, Section III, Chapter Five, Sections I - VII, Chapter Six, Sections II - IV, Chapter Eight, Chapter Eight 'a', Chapter Nine 'a', Chapter Eleven, Sections I - IV, Chapter Twelve, Chapter Thirteen and Chapter Fourteen, as well as for the crimes of Article 219, para. 4, second proposal, Article 220, para. 2, Article 253, Article 308, para. 2, 3 and 5, second sentence, Article 321, Article 321 bis, Article 356k and 393 of the special part of the Criminal Code, if the relevant circumstances cannot be established in any other way or their establishment is associated with extreme hardship (Articles 172(2) of the Code of Criminal Procedure and 3 of the Special Intelligence Assets Act).
These measures may be used only when this is necessary for the prevention and detection of serious intentional crimes according to the procedure established by the Code of Criminal Procedure and the required data cannot be collected in any other way. In other words, it has a subsidiary character if the information to be collected cannot be obtained by any other method. Article 12 of the Special Intelligence Assets Act specifies the scope of application of the special intelligence means regarding both persons and places. These are:

- persons in respect of whom information has been received and in respect of whom it may reasonably be presumed that they are about to commit, are committing or have committed serious offences;
- persons about whose actions data have been received and in respect of whom it can reasonably be presumed that they are used by persons in the previous group without being aware of the criminal nature of the activity carried out;
- sites for the establishment of the identity of persons belonging to the above-mentioned groups;
- persons and sites related to national security;
- persons who have given their written consent to the use of special intelligence means for the protection of their life or property.

In terms of procedure, the Special Intelligence Assets Act and the Code of Criminal Procedure make distinctions. On the one hand, Article 13 of the Special Intelligence Assets Act specifies which persons have the authority to request the use of special means of intelligence:

- General Directorate for Combating Organised Crime, General Directorate of the Judicial Police, General Directorate of the Security Police, General Directorate of the Border Police, Directorate of Internal Security, regional directorates of the Ministry of Interior, and specialised directorates (except for the Technical Operational Directorate), territorial directorates and autonomous territorial departments of the State Agency for National Security;
- Defence Information Service and Military Police Service under the Ministry of Defence;
- National Intelligence Service;
- the supervising public prosecutor, who shall submit a written and reasoned request to the court for to the court for the use of special intelligence means in a pre-trial procedure.

As for the procedure foreseen in Article 14 of the Special Intelligence Assets Act for requesting the use of these means, the information that must be included as mandatory in the request is reflected in greater detail than in the Code of Criminal Procedure. This information would be:

- a complete and exhaustive indication of the facts and circumstances which give rise to the presumption that a serious crime is being prepared, is being committed or has been committed which makes the use of special intelligence means necessary;
- a full description of the action taken so far and the results of the preliminary check or investigation;
- identification details of the persons or places in respect of whom or which the special intelligence means are to be used;
- period of use;
- operational techniques to be used;
- authorised official to be informed of the results of the use of special means of intelligence (Article 14(1)).

On the other hand, the Code of Criminal Procedure describes the application procedure in much less detail. Article 173 states that for the use of special intelligence tools in pre-trial proceedings the supervising prosecutor shall submit a written and reasoned request to the court. Before submitting the request, the supervising prosecutor shall notify the administrative head of the relevant prosecutor's office. In cases falling within the jurisdiction of the European Public Prosecutor's Office, the written and reasoned request to the court is submitted by the European Public Prosecutor or by a Deputy European Public Prosecutor. In this case, because only the supervising prosecutor can request the use of special means of intelligence in pre-trial proceedings, the mandatory elements of his or her request do not include data on the authorised official who is to be informed of the results of the use of special means of intelligence.

Authorisations to use special means of intelligence are granted in advance and the court is the only authority that can grant them. Generally, applications must be addressed to the president of the relevant district court or by a vice-president expressly authorised by him (Article 174(1) of the Code of Criminal Procedure).

There are authors, such as M. Yordanova [5], who consider that this difference in the framework between the Code of Criminal Procedure and the Law on Special Intelligence Means is due to the different application and objectives pursued by the two laws. The regime of the Code of Criminal Procedure serves the purpose of pre-trial proceedings and is applied by the pre-trial authorities. The investigating authorities also apply the regime provided for in the Special Intelligence Assets Act, but these one also serves a certain circle of special services, which apply it for preventive and other operational purposes.

This approach of the legislator, however, hardly merits uncritical acceptance. The risks discussed above materialise in the framework outside the Criminal Procedure Code. Regardless of whether and how far it serves its declared purpose: prevention and detection of serious offences, this framework not always can simultaneously serve the purposes of collecting evidence in a criminal proceeding.

As for the duration of the measures, we must consider both laws. Article 175 of the Code of Criminal Procedure and Article 21 of the Special Intelligence Assets Act provide for a maximum period of two months after the authorisation has been granted. If necessary, this time limit may be extended by a maximum of four months following the same procedure applicable for obtaining the initial authorisation. The total period may therefore not exceed six months.

The Netherlands

The Netherlands has incorporated into the Code of Criminal Procedure special investigative police powers, including the systematic gathering of intelligence. A duty of notification applies to the use of special investigative powers, which includes notifying a citizen if they have been deployed against him and, not having been involved in criminal proceedings, he has remained unaware of the fact. He needs not be notified if the interests of the investigation so require. In its regulation of 'exploratory investigation', the Act provides a legal basis for investigating specific sectors of society where crimes may be being committed or planned. At the same time, it introduces a new and broader concept of 'reasonable suspicion' (probable cause) for the benefit of investigations aimed at organised crime. In a criminal proceeding, police and prosecutors must account further for the conduct of the preliminary investigation if required to do so.

Moreover, the Computer Crime Act III provided law enforcement officials with a power to access computer systems remotely by stealth. The legislator deems the incorporation of such power in the

Act a necessity to tackle the ongoing challenges posed by advances in technology and the widespread use of computerised devices or systems for communication and the processing and storage of data. Subject to conditions, this power, in common parlance known as 'hacking power', allows designated investigative officials to access remotely and by stealth a computerised system ('a device or a system of inter-connected or related devices, which or any of which, pursuant to a program, performs automatic processing of computer data' (Section 80 DCCP) - such as a computer, smartphone or a server) in use by a suspect. Officials hack a system by breaking or circumventing the system's security or by applying software and technical tools. Gaining access is subject to stringent conditions: the officials are required to specify an investigative objective and the investigation is limited to serious crimes. Moreover, there must be an urgent investigation interest, an order from the prosecutor *and* a warrant from an investigative judge, the suspected offence must constitute a serious breach of legal order and for which the law prescribes a sentence of imprisonment of eight years or more, or it must concern an offence that has been designated by Order in Council (such as the dissemination or possession of child pornography (Section 240b DCCP), grooming (Section 248e DCCP), recruiting for terrorism (Sections 131 and 205 DCCP), participation in a criminal organisation (Section 140 DCCP), fraud offences (such as forgery of documents) and money laundering (Section 420bis DCCP).

Any data that can be registered may be copied for evidence purposes in a criminal investigation. Therefore, the Dutch legislator has built in an additional safeguard: the requirement of 'logging' (recording data) during the investigation (Section 126e DCCP). However, the logged information will not be added (automatically) in the case file, the defence must expressly request for it. The controversial nature of the power has prompted the legislator to require the annual publication of statistics of the use of intrusion software as well as an assessment after two years.

Thus, the Computer Crime Act III provides law enforcement officials a power to access the (computer) systems of suspects, but the Minister of Security and Justice, who is charged with overseeing the execution of the law, has spoken out to take explicit account of the facts of every case and of a proportionality test when using this special investigative power, which may result in waiving the application of the power in a particular case.

2.2.4 Accessibility

Requirement 17	*Accessibility and Universal Design*
Level of criticality	1
Legal basis	Many international instruments inform the European position on accessibility and Universal Design. These are only some of the most relevant: Council of Europe Recommendation No. R (92) 6 on a coherent policy for people with disabilities; the UN Standard Rules on the Equalization of Opportunities for Persons with Disabilities; the Council of Europe Resolution ResAP(2001)1 on the

	introduction of the principles of universal design into the curricula of all occupations working on the built environment ('Tomar Resolution'); the Council of Europe Resolution ResAP(2001)3 'Towards full citizenship of persons with disabilities through inclusive new technologies'; the UN Convention on the Rights of Persons with Disabilities of 2007; the Council of Europe Resolution ResAP(2007)3 on 'Achieving full participation through Universal Design' of the same year; the Directive on web accessibility;[12] the European accessibility act,[13] etc.
Description	Accessibility is the quality of being easy to approach, reach, enter, use or understand. Universal Design is defined as the design and composition of an environment so that it may be accessed, understood and used to the greatest possible extent, in the most independent and natural manner possible, in the widest possible range of situations, without the need for adaptation, modification, assistive devices or specialised solutions, by any persons of any age or size or having any particular physical, sensory, mental health or intellectual ability or disability. It means, in relation to electronic systems, any electronics-based process of creating products, services or systems so that they may be used by any person.
Explanation	The way specific AI-based functionalities are implemented can exclude people with certain disabilities. Not only international regulations and national laws, but also many standards and recommendations have been developed in order to overcome biases against people with disabilities.
National particularities	Many countries have laws and policies regarding accessibility, so it is not possible to include here a comprehensive or definitive listing.

2.2.5 Dual-use export control requirements

Requirement 18	***Dual-use export control requirements***
Level of criticality	1
Legal basis	At the international level, dual-use exports are primarily regulated by the non-binding Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. It contributes to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.

[12] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Text with EEA relevance), OJ L 327, 2.12.2016, p. 1–15.

[13] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance), OJ L 151, 7.6.2019, p. 70–115.

	At the EU level, dual-use exports are governed by Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. It states several legal requirements with regard to dual-use items, as well as to strengthening the exchange of relevant information and greater transparency. It also gives a guidance to exporters, in particular to small and medium sized enterprises (SMEs), regarding responsible practices.
Description	The Wassenaar Arrangement includes technology under the following terms: 'intrusion software', 'mobile interception or jamming equipment' and 'Internet Protocol (IP) network surveillance systems.' Supporting guidance on the Wassenaar Arrangement[14] states that export licences should not be issued to a private company if their product may 'be used for the violation or suppression of human rights and fundamental freedoms.' Regulation (EU) 2021/821 applies to 'cyber-surveillance items'. In order to address the risk that technologies exported from the EU might be misused by persons complicit in or responsible for serious violations of human rights or international humanitarian law, the export of such items is under control. Specifics risks relate to items are specially designed to enable intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of persons by monitoring, extracting, collecting or analysing data, including biometrics data, from those systems. The RITHMS platform entails such risks. Article 2(1) of Regulation (EU) 2021/821 describes 'dual-use items' as means items, including software and technology, which can be used for both civil and military purposes. The RITHMS platform can be considered a dual-use item.
Explanation	Given the characteristics and risks involved in the technology developed on the RITHMS platform, if exported, the requirements and procedures of Regulation (EU) 2021/821 must be complied with. The export will be subject to a regime of registrations, authorisations and control by the competent authority. In fact, while export control regimes have historically been aimed at mitigating military risks, the EU's new rules on export of surveillance technologies take human rights considerations as a primary justification for control, marking a shift in its normative grounding as well.
National particularities	All EU Member States except Cyprus are party to the Wassenaar Arrangement and must therefore follow its guidelines. Moldova and Bosnia and Herzegovina are not parties. The guidelines of the Regulation (EU) 2021/821 should be complied with by all EU Member States.

[14] The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org/.

3 What's next? The Artificial Intelligence Act

The European Commission released a Proposal for a Regulation on Artificial Intelligence (the AI Act or the Draft AI Act) on 21 April 2021.[15] The Act is likely to be passed into law during the Spanish Council Presidency in the second half of 2023. This legislation aims to regulate the use of AI by the public sector and LEAs. Therefore, it is of great interest for RITHMS. This Section does not cover all the AI Act's facets. Many aspects are omitted, which will deserve further scrutiny in the next future. This is only a first approach, based on [1] and [2], to the next step in the regulatory framework concerning AI-based systems for Law Enforcement purposes.

3.1 Scope

The material scope of the Draft AI Act concerns 'harmonised rules for [...] the use of artificial intelligence systems' (Article 1(a)), and aims to prevent 'Member States from imposing restrictions on the [...] use of AI systems, unless explicitly authorised by this Regulation' (Recital 1). The scope of the Act is apparently very wide, covering systems developed with any of the approaches in Annex I (machine learning, logic and knowledge-based approaches, and statistical or Bayesian approaches) that can generate outputs such as content, predictions, recommendations, or decisions influencing 'environments they interact with' (Article 3(1) and Annex I). The operational impact of the Act is, though, quite narrow, the main thrust relating to 'high-risk AI', which is quite closely delimited (below).

Subject to obligations under the Draft AI Act will be providers of systems who develop an AI system with a view to placing it on the market or putting it into service under their own name or trademark (Article 3). obligations also, or alternatively, fall in different ways on 'users', defined here to mean any natural or legal person 'using an AI system under its authority', e.g., a local authority putting in a fraud detection scheme, or an employer putting in an automated hiring system. Obligations also fall on importers and distributors (Articles 26–28) in a way similar to the product safety regime, with the intent of stopping dangerous products built outside the EU from entering it. The primary actor on whom obligations are placed is nonetheless the provider.

3.2 Structure

The Act splits AI into four different bands of risk based on the intended use of a system. Although described as a 'risk based' scheme, there is no sliding scale of risk, merely one category ('high risk'), which is extensively regulated; some minor transparency provisions for a small number of systems

[15] European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 .

characterised as 'limited-risk' AI; and a number of 'red lines', which have rhetorical effect but in practice are likely to be of very limited application.

The Act distinguishes different risk levels regarding AI practices, which we adapt to analyse in four categories: i) unacceptable risks (Title II); ii) high risks (Title III); iii) limited risks (Title IV); iv) minimal risks (Title IX). The Project, in its activities, follows the principle of precaution. Therefore, of the four levels of risk currently present in the draft legislation, the Consortium will consider RITHMS Platform (or at least the elements of it which are within the scope of the AI Act) as fitting in the high-risk level. For this reason, this document will not cover all four categories. Furthermore, the Act is most concerned with 'high-risk AI'. High-risk AI systems are subject to a detailed certification regime (see below) but are not deemed so fundamentally objectionable that they should be banned. These include:

- In Annex II-A, AI systems intended to be used as a safety component of a product, or themselves a product, which are already regulated under the NLF (e.g., machinery, toys, medical devices) and, in Annex II-B, other categories of harmonised EU law (e.g., boats, rail, motor vehicles, aircrafts, etc.).
- In Annex III, an exhaustive list of eight 'new' high-risk AI systems, comprising, under f), law enforcement systems that may interfere with people's fundamental rights (e.g., automated risk scoring for bail; 'deepfake' law enforcement detection software; 'pre-crime' detection), while under g) migration, asylum and border control management (e.g., verification of authenticity of travel documents; visa processing). Under h), it also comprises Administration of justice and democratic processes (e.g., 'robojustice', automated sentencing assistance).

The European Commission can add new sub-areas to Annex III by delegated act if they pose an equivalent or greater risk than systems already covered but cannot add entirely new top-level categories.

3.3 'Essential requirements' for high-risk AI

The AI Act requires providers of high-risk AI systems to conduct a prior conformity assessment before placing them on to the market (Articles 16 and 43). Providers must ensure their systems are compliant with the 'essential requirements' set out in Title III, Chapter 2 of the AI Act. They can then attach a CE mark to conforming systems, which can be freely imported and distributed throughout the EU. These requirements relate to data and data governance; technical documentation; record keeping; transparency and provision of information to users; human oversight; and robustness, accuracy and security.

Providers must set up a risk-management system that documents and manages risks across the AI system's entire lifecycle, when used as intended, or, under conditions of 'reasonably foreseeable misuse' (Article 9). Risks may be added as a result of post-market surveillance (see below). The aim is to bring down the 'high risks' of the AI system to an acceptable residual level. 'Adequate mitigation and control measures' can be used when risks cannot be eliminated. Residual risks are to be communicated to users.

Four categories of requirements seem particularly germane to some of the ethical concerns identified in RITHMS Ethical Protocol, which are algorithmic error, bias and discrimination; automated decision-making as contrary to human dignity; and opacity/lack of explanations. They are applied to providers.

3.3.1 Data and data governance (Article 13)

This requirement aims to meet a set of concerns about the quality of the data used to build AI systems. It includes:

- Rules about how training sets (also validation and testing datasets) must be designed and used. Significantly for concerns about error and discrimination generated by partial, erroneous or historically biased data, datasets must be 'relevant, representative, free of errors and complete', taking into account the intended purpose (Article 10(3)). Despite these requirements seeming steep, datasets only need to meet them 'sufficiently' and 'in view of the intended purpose of the system' (Recital 44).
- Rules about data preparation, including 'annotation, labelling, cleaning, enrichment and aggregation'.
- Assessment of the 'formulation of relevant assumptions [about] the information that the data are supposed to measure and represent'; and 'examination in view of possible biases.'
- Exemption from GDPR rules restricting collection of sensitive personal data to de-bias algorithms.

3.3.2 Human oversight (Article 14)

Systems must be designed and developed in such a way that they can be 'effectively overseen by natural persons during the period in which the AI system is in use' (Article 14(1)). This is not simply a matter of transparency or explanation of how the AI system works, as discussed in the context of Articles 22 and 13–15 of the GDPR, but goes much further into terrain such as enabling the 'human overseer' to spot anomalies, become aware of 'automation bias', be able to correctly interpret the system's outputs and be able to override or disregard the system's results. Explicitly, one aim is to prevent or minimise risks to fundamental rights (Article 14(2)). If a high-risk system is operated by a 'user' rather than the original provider – e.g., a LEA buys and installs the platform from the RITHMS Consortium – then the allocation of responsibility is quite different in the Act than in the GDPR. Under the GDPR, the LEA would be the 'data controller' and the main focus of duties. In the Act, it remains the sole responsibility of the RITHMS Consortium to implement 'human oversight' in a way that is 'appropriate to be implemented by the user' (Article 14(3)(a)) and to obtain conformity assessment

before the system is put on the market (Article 14(3)(b)). Under Article 28, if the user substantially modifies the system, they become the new 'provider' with all corollary certification duties.
Under the AI Act, no obligations for human oversight flow directly from the Act to a user, e.g., a LEA. In relation to human oversight, LEAs must simply follow the instruction manual.

3.3.3 Conformity assessment (pre-marketing)

The Act requires providers to ensure before placing on market that their systems conform with the essential requirements listed above, as well as to comply with a number of other tasks including: registering AI systems on a database,[16] having an appropriate quality management system in place – 'appropriate' meaning in this regard complying with Article 17 –, recording the system's technical documentation and keeping automatically generated logs. The requirements regarding this technical documentation are extensive. We refer the reader to them. The Consortium will not have to publish the technical documentation or provide it except to organisations involved in regulation or conformity assessment. However, separate provisions indicate what information must be provided as a form of user transparency, and what information must be registered in a public database. Providers must facilitate logging to allow traceability appropriate to a system's risks. Providers must only keep logs for an appropriate amount of time 'to the extent such logs are under their control' (Article 20(1)), else the user must instead (Article 29(5)).

After doing all this, the system gets its CE mark, which enables distribution throughout the EU (Article 19). Providers in the main will only have to demonstrate conformity by an 'assessment based on internal control', i.e., self-certification (Article 43(1)(a)). Therefore, all the Consortium will need to do is self-assess that their quality management system, technical documentation, and post-market monitoring plan follow the essential requirements. The Consortium can do this either by their own bespoke plans for conformity, or by following a relevant harmonised technical standard. High-risk AI systems which self-certify as confirming with such standards are then presumed to have met the requirements of Chapter 2 (see Article 40). The European Commission anticipates that the Draft AI Act standards will first appear in the EU's Official Journal in 2024–2025, aligned with when the Draft AI Act would be applicable.[17] The Consortium, though, have also the possibility to ignore these standards, and instead justify that they have adopted technical solutions at least equivalent (Article 41(4)). Nevertheless, if existing, harmonized standards are both cheaper for the Consortium and a safer bet.

[16] The Draft AI Act proposes a new, central database, managed by the Commission, for the registration of 'standalone' high-risk AI systems, such as the RITHMS Platform.

[17] European Commission, 'Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021) 206 Final)' (2021) 57.

At present, only a subset of high-risk AI systems must make use of a third-party body – a 'notified body' – to externally audit their conformity. The systems in question are:

1. AI systems for biometric identification or categorisation of natural persons (Article 43(1)) but only if no technical harmonised standard is made, which is unlikely to result.
2. AI systems already regulated under existing legal framework or other EU laws, listed in Annex II, where that legislation already demands a notified body be involved (Article 43(3)).

3.3.4 Enforcement (post-market)

Providers are tasked to 'establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system' (Article 61(1)). This monitoring system will 'collect, document and analyse relevant data provided by users or collected… throughout their lifetime' (Article 61(2)). Users (i.e., deployers) are also tasked to monitor systems 'on the basis of the instructions of use' and report new risks, serious incident or 'malfunctioning' (Article 29(4)). Their intel goes to providers or distributors, not directly to the Market Surveillance Authority (MSA). Provider monitoring of accidents and malfunctions must go to the relevant MSA at least within 15 days of becoming aware of it (Article 62). Member States are to appoint national supervisory authorities, which by default act as MSAs (Article 59), though in some cases other bodies - such as Data Protection Authorities (DPAs) - will take the role. In relation to law enforcement users and Union bodies, DPAs will gain MSA roles (Article 65).

3.4 Future national implementation

The Draft AI Act aims to 'prevent unilateral Member States actions that risk to fragment [sic] the market and to impose even higher regulatory burdens on operators developing or using AI systems.' (EC, "AI Act Impact Assessment", 54). Where the Draft AI Act's provisions entail this 'maximum harmonisation', Member States' abilities to act in that area are disabled. Member States must disapply conflicting national rules and accept compliant products on their markets. If a provision is found to not maximally harmonise an area, or only harmonises certain areas, Member States retain competence to adopt more stringent standards.

References

[1] L. Edwards, “The EU AI Act: a summary of its significance and scope,” The Ada Lovelace Institute, 2022. Available at: www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf.

[2] M. Veale, M., and F. Z. Borgesius, “Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach,” *Computer Law Review International* Vol. 22(4), pp. 97-112, 2021.

[3] C. Brants, A. Jackson, and T. J. Wilson, “A Comparative Analysis of Anglo-Dutch Approaches to ‘Cyber Policing’: Checks and Balances Fit for Purpose?,” *The Journal of Criminal Law* Vol. 84(5), pp. 451-473, 2020.

[4] O. L. van Daalen, J. V. J. van Hoboken, and M. Rucz, “Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control,” *Computer Law & Security Review* Vol. 48, online first, 2023.

[5] M. Yordanova, “Special intelligence means for collecting evidence of organised crime in Bulgaria”, *Archivio Penale* n.3, pp. 1-31, 2012. Available at: https://archiviopenale.it/2012-3--maria-yordanova-special-intelligence-means-for-collecting-evidence-of-organized-criminal-activity-in-bulgaria/contenuti/1123.

[6] OSCE Guidebook Intelligence-Led Policing, June 2017. Available at: https://www.osce.org/files/f/documents/d/3/327476.pdf.

Annex 1. List of laws

European Union

Regulations

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance), OJ L 303, 28.11.2018, p. 59–68.

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), OJ L 206, 11.6.2021, p. 1–461.

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance), OJ L 170, 12.5.2021, p. 1–68.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final.

Directives

Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (Text with EEA relevance), OJ L 327, 2.12.2016, p. 1–15.

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122–137.

Decisions

Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, OJ L 72, 17.3.2015, p. 53–88.

Commission Decision (EU, Euratom) 2021/259 of 10 February 2021 laying down implementing rules on industrial security with regard to classified grants, OJ L 58, 19.2.2021, p. 55–97.

Council of Europe

Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector.

National regulations

Bosnia and Herzegovina[18]

Law on the Protection of Personal Data No. 49/06, available in English at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af037.

The amendment to the Law on the Protection of Personal Data carried out in 2011 is available in English at: http://azlp.ba/propisi/Default.aspx?id=5&langTag=en-US&template_id=149&pageIndex=1.

Law on the Protection of Secret Data No. 54/2005, available in English at: https://tuzilastvobih.gov.ba/files/docs/zakon_o_zastiti_tajnih_podataka_54_05_-_eng.pdf.

Instructions on criminal intelligence work of the Border Police

Regulation on the Manner of Keeping the Records of Personal Data Filing Systems and the Pertinent Records Form (14 May 2009), available in English at: http://azlp.ba/propisi/default.aspx?id=1321&langTag=en-US.

Agreement between Bosnia and Herzegovina and the European Union on security procedures for the exchange of classified information, signed on 5 October 2004, as attached to the Council Decision 2004/731/EC of 26 July 2004, as well as its implementing arrangements, available in English at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22004A1027(01).

Bulgaria

Law on the Protection of Personal Data,[19] available in English at: https://www.cpdp.bg/en/index.php?p=element&aid=1194. The Bulgarian LPPD includes provisions implementing the Law Enforcement Directive.

Criminal Procedure Code, available in Bulgarian at: https://lex.bg/bg/laws/ldoc/2135512224.

Special Intelligence Assets Act,[20] available in Bulgarian at: https://lex.bg/bg/laws/ldoc/2134163459.

Ministry of the Interior Act.[21]

Italy

Personal Data Protection Code. Containing provisions to adapt the national legislation to 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,[22] available in English at https://www.garanteprivacy.it/documents/10160/0/PERSONAL+DATA+PROTECTION+CODE.pdf/96672778-1138-7333-03b3-c72cbe5a2021?version=1.0.

[18] In the near future we expect the adoption of a new Law on Personal Data Protection which will transpose the provisions of the GDPR with some adjustments to Bosnian conditions. The draft is only available in Serbian. Bosnia and Herzegovina is not an EU Member State and European provisions on personal data protection are not directly applicable in Bosnia and Herzegovina.

[19] Zakon za zashtita na lichnite danni, DV no. 1, 4 January 2002 (ZZLD).

[20] ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА.

[21] Zakon sa Ministerstvo na vatreshnite raboti, DV no. 53, of 27 June 2014 (ZMVR).

[22] Text released on 22.12.2021, including the amendments made by way of decree-law No. 139 of 8 October 2021 as subsequently enacted via Law No. 205 of 3 December 2021, and the amendments made by way of decree-law No. 132 of 30 September 2021 as subsequently enacted via Law No. 178 of 23 November 2021.

Legislative Decree No. 51 of 2018, implementing Directive (EU) 2016/680 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,[23] available in Italian at https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

Legislative Decree No. 101 of 10 August 2018, containing provisions to adapt the national legislation to 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,[24] available In Italian at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

Legislative Decree No. 186 of 8 November 2021. Implementation of Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down provisions to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Decision 2000/642/JHA,[25] available in Italian at https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-11-29&atto.codiceRedazionale=21G00195&elenco30giorni=false

Italian Presidential Decree No. 54 of 2021, containing the regulation that defines the procedures, methods and terms of evaluation of the acquisitions of goods, systems and services by the individuals included in the information and communication technology cybersecurity perimeter (ICT),[26] available in Italian at: www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.

Italian Ministerial Decree No. 81 of 2021, containing the regulation governing the procedures for notifications in the event of incidents having an impact on networks, information systems and IT services, as well as measures aimed at guaranteeing high security models,[27] available in Italian at: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.

---

[23] Decreto Legislativo 15 maggio 2018, n. 51. Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[24] Decreto legislativo 10 agosto 2018, n. 101. Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[25] Decreto Legislativo 8 novembre 2021, n. 186. Attuazione della direttiva (UE) 2019/1153 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI.

[26] Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[27] Decreto del presidente del Consiglio dei Ministri 14 aprile 2021, n. 81, Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.

Moldova[28]

Law No. 133 of 8 July 2011 on Personal Data Protection, available in English (unofficial translation) at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fdatepersonale.md%2Fwp-content%2Fuploads%2F2022%2F02%2FLaw-on-personal-data-protection-2022-1.docx&wdOrigin=BROWSELINK.

Law No. 320/2021 regarding the activity of the Police and the status of the policeman, available in Romanian at: https://www.legis.md/cautare/getResults?doc_id=120699&lang=ro.

Criminal Procedure Code of the Republic of Moldova, available in Romanian at: https://www.legis.md/cautare/getResults?doc_id=135680&lang=ro#.

NCPDP's Order No. 27 of 31 March .2022 regarding the approval of the List of types of processing operations that are subject to the requirement to carry out an impact assessment on the protection of personal data, available in Romanian at: https://datepersonale.md/wp-content/uploads/2022/04/Ordinul-nr.-27-din-31.03.2022.pdf.

Governmental Decision No. 1123 of 14 December 2010 on the approval of the requirements for the assurance of personal data security and their processing within the information systems of personal data.

Law No. 59 of 29 March 2012 on Special Investigative Activity, available in English (unofficial translation) at: https://www.legis.md/cautare/getResults?doc_id=123543&lang=ro.

Agreement between the European Union and the Republic of Moldova on security procedures for exchanging and protecting classified information signed on 31 March 2017 as attached to the Council Decision 2017/718/CFSP of 27 March 2017, as well as its implementing arrangements, available in English at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22017A0422%2801%29. Not yet in force.

Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data information (Order no 33 of 22 April 2022), available in English at: https://datepersonale.md/wp-content/uploads/2022/07/Ordin-Eng-.pdf.

The Netherlands

General Data Protection Regulation Implementation Act,[29] available in English (unofficial translation) at: https://vertaalbureau-fiducia.nl/wp-content/uploads/2022/06/Vertaling-UAVG-EN.pdf.

Act of 17 October 2018 amending the Police Data Act and the Judicial and Criminal Records Act to implement European legislation on the processing of personal data for the prevention, investigation, detection or

---

[28] In the near future we expect the adoption of a new Law on Personal Data Protection which will transpose the provisions of the GDPR with some adjustments to Moldovan conditions. Moldova is not an EU Member State and European provisions on personal data protection are not directly applicable in Moldova.

[29] General Data Protection Regulation Implementation Act of 16 May 2018, containing rules on the implementation of 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) (OJEU 2016, L 119) (Dutch GDPR Act, Uitvoeringswet Algemene verordening gegevensbescherming).

prosecution of criminal offences or the execution of criminal penalties,[30] available in Dutch at: https://zoek.officielebekendmakingen.nl/stb-2018-401.html.

Decree of 14 June 2022 amending the Police Data Decree, implementing Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, establishing rules to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offenses and repealing Council Decision 2000/642/JHA),[31] available in Dutch at: https://zoek.officielebekendmakingen.nl/stcrt-2022-15876.html.

Code of Criminal Procedure (henceforth DCCP),[32] which incorporates the Special Powers of Investigation Act,[33] and the Computer Crime Act III 2018.[34]

Spain

Spanish Data Protection Law,[35] available in Spanish at: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673.

Organic Law 7/2021, of 26 May, on the Protection of Personal Data to prevention, detection, investigation and prosecution purposes of criminal offenses and execution of criminal sanctions,[36] available in Spanish at: https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806

Organic Law 9/2022 of 28 July, setting the rules for facilitating the use of financial information and other measures designed to prevent, detect, investigate or process criminal offences,[37] available in Spanish at: https://www.boe.es/buscar/act.php?id=BOE-A-2022-12644.

Royal Decree of 14 September 1882 approving the Criminal Procedure Act (LECrim),[38] available in English (official version, not updated) at: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.

[30] Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van de Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen

[31] Besluit van 14 juni 2022 tot wijziging van het Besluit politiegegevens ter implementatie van Richtlijn (EU) 2019/1153 van het Europees parlement en de Raad van 20 juni 2019 tot vaststelling van regels ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten, en tot intrekking van Besluit 2000/642/JBZ van de Raad.

[32] Wetboek van Strafvordering.

[33] Wet Bijzondere Opsporingsbevoegdheden.

[34] Wet Computercriminaliteit III.

[35] Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

[36] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

[37] Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que faciliten el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales, de modificación de la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas y otras disposiciones conexas y de modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[38] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

RITHMS

Research, Intelligence and Technology for Heritage and Market Security

Project Coordinator

Arianna Traviglia

arianna.traviglia@iit.it

Scientific Project Manager

Michela De Bernardin

michela.debernardin@iit.it