HORIZON-CL3-2021-FCT-01-08

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

GA 101073932

Deliverable 7.1

Report on the legal framework

WP7 – Ethical, Societal and Legal Issues

Authors: Patricia Faraldo Cabana, Silvia Rodríguez López, María Ángeles Fuentes Loureiro, David José Soto Díaz (UDC)
Lead participant: UDC
Delivery date: 31 May 2023
Dissemination level: Public
Type: Report

Revision History

Author Name, Partner short name	Description	Date
Patricia Faraldo Cabana, María Ángeles Fuentes Loureiro, Silvia Rodríguez López, David José Soto Díaz (UDC)	Draft deliverable	10/05/2023
Michela De Bernardin (IIT), Alessandro Guarino (IIT)	Revision	30/05/2023
Arianna Traviglia (IIT)	Final version	31/05/2023

Contents

Executive Summary

The present document is a deliverable of the RITHMS project. It provides an integrated analysis of the legal aspects concerning the technologies developed in WP3 and WP4, both in the research and development phase itself and in the testing and validation phase (carried out in WP5). The deliverable consists of five sections after the introduction. Section 2 describes the European legal framework regarding research and development for the RITHMS Project, which mainly concerns the General Data Protection Regulation, but also other issues, such as copyright. Section 3 describes the national legal framework in the industry partners' countries concerning data protection issues for research and development purposes. Section 4 describes the European legal framework concerning the testing and validation phase, mainly related to the Law Enforcement Directive. Section 5 details the national implementation in the case-study countries, three of which are not members of the European Union.

List of abbreviations

AEPD	Spanish DPA
ANSPDCP	Romanian DPA
AZOP	Croatian DPA
BfDI	German DPA
CDSM	Copyright in the Digital Single Market
CJEU	Court of Justice of the European Union
CPDP	Bulgarian DPA
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSM	Digital Single Market
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EPPO	European Public Prosecutor's Office
EU	European Union
FADP	Swiss Federal Act on Data Protection
FDPIC	Swiss DPA
LEA	Law Enforcement Agency
LfDI	DPA of Baden-Württemberg
PDPA	Personal Data Protection Act of the Republic of Bulgaria
SCC	Standard Contractual Clause
TDM	Text and Data Mining
UN	United Nations
US	United States of America
WP	Work Package

List of tables

1 Introduction

1.1 Scope

The main focus of Task 7.1 is to 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 (henceforth, 'GDPR')[1] and the Law Enforcement Directive ('LED'),[2] as well as the national instruments envisaged by each country in the Consortium with regards to data protection and the gathering of criminal intelligence. This deliverable will elaborate upon the distinction between the development of the RITHMS platform by the research Consortium, on the one hand, and the end-users of this Platform (namely Law Enforcement Agencies), on the other hand. It also provides an introduction into the applicability of legal norms to open-source and publicly available information. RITHMS is a research and innovation project that – as such - aims at exploiting the research results. The Platform is developed in view of its future use by LEAs. The development of the Platform, including testing of the prototype modules, is aimed at proving functionality and is carried out by private parties. Pilots and demonstrations of the complete prototype will be carried out by public bodies, i.e., Law Enforcement Agencies who are part of RITHMS Consortium. This distinction is important, as different legal standards apply. Some legitimate processing grounds are reserved for public authorities in the field of law enforcement, creating more leeway for them than it is the case regarding private companies.

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 describes the European legal framework regarding research and development for the RITHMS Project, which mainly concerns the GDPR. Section 3 describes the national legal framework in the industry partners' countries concerning data protection issues for research and development purposes. Section 4 describes the European legal framework with regard to the testing and validation phase, mainly related to the LED. Section 5 details the national implementation in the case-study countries. Section 6 builds on the above sections, outlining the conclusions of the study. In addition, the appendix to this report presents a list of relevant European and domestic legislation.

1.3 Methodology

The methodology used for this report comprises comparative and legal analysis techniques to investigate the qualitative data collected through the following means:

[1] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

[2] 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.

- Country reports covering the six countries of industry partners, five of which are EU Member States, and one is not, and the six countries of the Consortium partners that are law enforcement agencies (LEAs), three of which are EU Member States and the other three are not.
- Desk research assessing information published at the EU level, internationally and in the case-study countries.

1.4 Relation with other deliverables

The scientific research within RITHMS should safeguard principles of research ethics as well as legal requirements. In many ways, though, legal requirements and research ethics overlap. The analysis of the legal framework is the objective of Task 7.1, which provides an integrated analysis of the legal aspects concerning the technologies developed in WP3-WP4. UDC will map the European and national legal framework regarding RITHMS technological outputs and the implied methodology, including an extensive exploration of the GDPR and the LED, as well as the national instruments envisaged by each country in the Consortium (D7.1 - Report on the legal framework, UDC, PU, M8). In particular, this document considers existing legal norms and requirements that the Consortium must comply with when researching and developing the RITHMS platform, as well as the ones that the final product must comply with in order to be deployed for law enforcement. Most of them have already been mentioned in D1.1 - Initial Legal Requirements (UDC, SEN, M6). The Ethics Protocol (D7.2, UDC, SEN, 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 requirements that should be complied with 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 (IIT, 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.

2 In research and development. The European legal framework

2.1 Introduction

This section's aim is two-fold. First, it seeks to map the trajectory of relevant legal instruments (regulations, directives, and international conventions) around the legality of data scraping for profit in the EU. Second, it assesses the legal risks surrounding industry partners' scraping activity, with examples extracted from pertinent jurisdictions. In the context of data scraping, the most important legal issue is related to data protection law. The most important legal instrument at the EU level is the General Data Protection Regulation ('GDPR').[3] However, also copyright creates specific restrictions in view of the research and development of the RITHMS Platform.

[3] 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

2.2 Data protection law

2.2.1 Rules on the processing of non-personal data

The EU allows companies and public administrations to store and process non-personal data wherever they choose. Such data still needs to be available to regulatory authorities. Nevertheless, the Non-Personal Data Regulation's[4] main obligations relate to Member States rather than corporations, and these obligations are considerably more lenient than those imposed by the GDPR. The Non-Personal Data Regulation does not define 'non-personal data'. It uses this term as equivalent to 'electronic data other than personal data' (Article 2(1)). In datasets in which personal and non-personal data are inextricably linked, its provisions shall not prejudice the application of the GDPR (Article 2(2)). According to the European Commission's Guidance on the interaction between this Regulation and the GDPR,[5] the notion of 'non-personal data' in the Regulation must be defined by opposition to personal data as laid down by the GDPR (see section 2.2.2.2).

The key principle of the Regulation on the Free Flow of Non-Personal Data is that such non-personal data must flow freely in the EU. Data localisation requirements, referring to Member States imposing the processing of data in their territory or hindering the processing of data in another Member State, are in principle not permitted, unless justified on the grounds of public security (encompassing the need to facilitate the investigation, detection and prosecution of criminal offences) in compliance with the principle of proportionality. Regardless of the localisation of data, persons subject to obligations to provide data to competent authorities shall comply with such obligations by providing and guaranteeing effective and timely electronic access to the data to competent authorities (Recital 25 of the Non-Personal Data Regulation). If said persons would fail to comply, national competent authorities shall provide assistance to each other, if appropriate under instruments in the area of police cooperation and criminal justice such as the Council Framework Decision 2006/960/JHA,[6] Directive 2014/41/EU on the European Investigation Order ('EIO'),[7] and the Cybercrime Convention,[8] together with its Additional Protocols.[9]

[4] 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.

[5] Communication from the Commission to the European Parliament and the Council 'Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union' (COM/2019/250 final).

[6] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

[7] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

[8] Council of Europe's Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001. Available in English at: https://rm.coe.int/1680081561.

[9] In particular, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), Strasbourg, 12 May 2022. Available in English at: https://rm.coe.int/1680a49dab.

2.2.2 Rules on the processing of personal data

2.2.2.1 Relevant texts

Data protection is a fundamental right, both under EU and Member State law. This implies that any breach of data protection rights will be granted special judicial procedures. Though, even before any claim is submitted before courts, the national data protection authorities will verify the compliance of any collection and processing of personal data with data protection law.

There is a constellation of legal instruments that govern data protection. Some of them have a national scope of application, while others are applied at the EU level or even at the wider level of the Council of Europe. This report tackles the EU law on data protection, since it plays a core role in the data protection system within EU and non-EU countries, as well as for national regulations.

As already indicated, the most important legal instrument at the EU level is the GDPR. As stated in Article 1(1), this Regulation lays down rules regarding the protection of natural persons - i.e., people - in relation to the processing of personal data and rules relating to the free movement of personal data. But the EU legal framework on data protection is also composed of other instruments:

- The LED, which applies generally 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, but only when these authorities process personal data for such purposes (but does not apply to personal data processing by EU institutions, bodies, offices and agencies). It will be analysed in Section 4.
- Regulation (EU) 2018/1725, or 'EU-DPR',[10] which is generally applicable to the processing of personal data by EU institutions, bodies, offices and agencies, but includes special rules for the processing of 'operational personal data', for instance by Eurojust, and leaves out of its scope Europol and the European Public Prosecutor's Office ('EPPO').
- Directive 2002/58/EC,[11] or e-Privacy Directive, applying to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

In addition to such instruments, other legal instruments also include particularly important data protection rules applying to specific data processing activities in this field, such as, for instance:

[10] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 39–98.

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

- Regulation (EU) 2016/794,[12] or the Europol Regulation, on the EU Agency for Law Enforcement Cooperation (Europol), which has its own data protection provisions.
- Council Regulation (EU) 2017/1939,[13] or EPPO Regulation, which equally has its own data protection provisions.
- Regulation (EU) 2018/1727,[14] or the Eurojust Regulation, on the European Union Agency for Criminal Justice Cooperation (Eurojust), which has data protection rules to be regarded as lex specialis to the relevant provisions of the EU-DPR.

Contrary to what this list might imply, the landscape of EU data protection law is considerably complicated. Even if the establishment of a harmonised framework for all data processing activities by has been a major, recurrent concern of the European Parliament for many years (see the European Parliament Resolution of 12 March 2014, 15), EU law does not provide a homogenous treatment of the subject. The present approach, notably enshrined by the LED in conjunction with the GDPR, whereby certain EU agencies processing data for law enforcement purposes are exempt from the application of general provisions in the area, has been described as leading 'level data protection regime where different legal instruments, and therefore different standards affecting individuals in exercising their data protection rights, apply' (Belfiore, 2013: 367). There exist also several specific provisions on the protection of personal data in certain EU instruments that remained unaffected by the entry into force of the LED and have not been revised since specific provisions for the protection of personal data that had entered into force before May 2016 in the field of judicial cooperation in criminal matters and police cooperation. In June 2020, the European Commission announced its action plan to progressively align with the LED the provisions still requiring alignment, a total of 10 according to its assessment.[15] Two of them have been already modified.

The general standards of the GDPR are the central element of the current legal framework applicable to industry partners, if not the only element worth being reviewed (AlgorithmWatch, 2019).

2.2.2.2 Key notions

'Personal data' is then one of the key notions of data protection law determining the material scope of the GDPR. Personal data is any information that relates to an identified or identifiable natural person (Article 4(1) GDPR). In this respect, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social

[12] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

[13] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1–71.

[14] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138–183.

[15] Communication from the Commission to the European Parliament and the Council Way forward on aligning the former third pillar acquis with data protection rules (COM/2020/262 final).

identity of that natural person. Different pieces of information which collected can lead to the identification of an individual also constitute personal data. It is worth noting that the Court of Justice of the European Union ('CJEU') has stated that for information to be treated as 'personal data', there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person.[16] Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Examples of personal data: a name and surname; a home address; an email address such as name.surname@company.com; an identification card number; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; the advertising identifier of a phone.

Examples of non-personal data: a company registration number; an email address such as info@company.com; anonymised data; numerical data, metrics, classifiers, or other types of data related to technical functionalities; internal categorizations of specific pieces of content or metrics regarding the enforcement of specific violations of terms of service.

Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymization must be irreversible.

To be considered personal data, the nature of information is of no significance: It can be accurate or unreliable, objective or subjective, and include judgments and opinions. The information content is not subject to any specific standards. Information need not be related to personal or family matters. It might be relevant to the individual's personal, professional, and other aspects of life. Additionally, the GDPR safeguards personal data independent of the technology used to process it. It is technology neutral and applies to both automatic and manual processing, providing the data are organized in line with pre-established standards (for example, alphabetical order). Personal data must adhere to the GDPR's protection obligations regardless of how it is stored, including on paper, in an IT system, or through video surveillance.

The individual whose personal information is used is called a 'data subject' – an 'identified or identifiable natural person' (Article 4(1) GDPR). Another relevant concept is 'data processing'. It refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR). The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system. This material scope of application has very few exceptions, this is, legal fields in which data protection law is not enforceable. Such exceptions are related to criminal investigations, domestic use, and the common and foreign security policy. In general, exceptions do not concern data scraping with commercial purposes.

[16] Judgment of the Court (Second Chamber) of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, para. 43-44.

Another key notion of data protection law determining the material scope of the GDPR is whether the personal data belongs to EU/EEA[17] citizens or residents. Only when personal data from EU/EEA citizens or residents are processed do the data protection principles, rights and obligations apply (Article 2(1) GDPR). In relation to this, Article 3 of the GDPR establishes that the GDPR applies in the context of the activities of a controller established in the EU/EEA, regardless of whether the processing takes place in the EU/EEA or not, but it is also of application where personal data of data subjects who are in the EU/EEA, regardless of their nationality, are processed by someone not established in the EU/EEA, where the processing activities are related to the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the EU/EEA. In the case of an EU/EEA-based company with servers and operations in a non-EU/EEA country, the GDPR applies. As the European Data Protection Board ('EDPB') says in the Guidelines 3/2018 on the territorial scope of the GDPR (Article 3),[18] 'The text of the GDPR specifies that the Regulation applies to processing in the context of the activities of an establishment in the EU 'regardless of whether the processing takes place in the Union or not.' It is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.

2.2.2.3 Principles

The GDPR establishes certain principles relating to the processing of data (Article 5 GDPR), which any processor must comply with. These principles are enlisted below:

- Lawfulness, fairness, and transparency principle requires that personal data be processed in a lawfully, fairly, and transparent manner.
- Purpose limitation principle, according to which personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation principle, meaning that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy principle requires that personal data shall be accurate and, where necessary, kept up to date. Therefore, 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.

[17] EEA stands for the European Economic Area, which is a European territory consisting of 30 countries, established as a result of the Treaty of 1992. The EEA consists of 27 EU member states plus Iceland, Liechtenstein, and Norway. The GDPR applies to all of them.

[18] Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

- Storage limitation principle indicates that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Integrity and confidentiality principle calls for the processing of personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, by using appropriate technical or organizational measures.

The only principle which is fully developed in the GDPR is the lawfulness principle. Indeed, Article 6 of the GDPR states that the processing will be lawful when:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes. Such consent must be given in accordance with the legal requirements established in Article 7(2) of the GDPR, i.e., in an intelligible and easily accessible form, using clear and plain language, but also ensuring the data subject their right to withdraw their consent at any time (Article 7(3) GDPR); or
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary to protect the vital interests of the data subject or of another natural person; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It is worth noting that when a processing is made with a purpose different from the original purpose for which data were collected and such further processing is neither based on data subject consent nor in a legal obligation, then the controller shall take into account certain criteria in order to ascertain the compatibility of such processing. Such criteria are, among others, the following (Article 6(4) GDPR): Any connection between the purposes for which the personal data have been collected and the purposes of the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; the nature of the personal data, in particular whether special categories of personal data are processed; the possible –negative- consequences of the intended further processing for data subjects; the existence of appropriate safeguards, which may include encryption or pseudonymisation.

In relation to the processing of sensitive personal data, Article 9 of the GDPR prohibits the 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. Nevertheless, such prohibition is tempered by several exceptions, being the processing of

personal data, which have been manifestly made public by the data subject, the only one applicable to text and data mining for private reasons. Below we will study the application of this regulation to private companies that scrape publicly available data for profit.

2.2.2.4 *Data subject rights*

The legal safeguards established in the principles and the limitations and prohibitions enshrined in the GDPR are supplemented by the rights of data subjects, laid down in Articles 12 to 22. In this regard, data subjects bear, among others, the following rights: right to receive transparent information, right of access, right to rectification, right to erasure, right to restriction of processing, right to object, and right not to be subject to a decision based solely on automated processing.

The right to receive transparent information (Articles 12, 14 GDPR) entitles data subjects to request the controller information relative to the identity and the contact details of the controller and the data protection officer; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the categories of personal data concerned; the recipients or categories of recipients of the personal data, if any; and the intention of the controller to transfer the data subject's personal data to a third country. The information provided shall be written in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The right of access (Article 15 GDPR) implies that the data subject has the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed. If this is the case, the data subject shall have granted access to the personal data and the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries; the envisaged period for which the personal data will be stored; the existence of the right to request from the controller both rectification or erasure of personal data or the processing restriction, as well as the right to object to such processing; the right to lodge a complaint with a supervisory authority; the source of the personal data, where it has not been collected from the data subject; and, if personal data are to be transferred to a third country, the appropriate safeguards relating to such transfer.

The right to rectification (Article 16 GDPR) allows the data subject to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Close to this right, the right to erasure (Article 17 GDPR) grants the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay, where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected; the data subject objects to the processing and there are no overriding legitimate grounds for the processing; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation. It must be taken into account that where the controller has made the personal data public and is obliged to erase the personal data, he or she shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The right to the restriction of processing (Article 18 GDPR) authorises the data subject to restrict the processing of his or her data, this is that the processing will be subject to limitations.

This right may be exercised by the data subject if the accuracy of the personal data is being contested by him or her – in this context, the restriction cannot last more than the necessary time for enabling the controller to verify the accuracy of the personal data – ; or if the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or if the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the exercise or defence of legal claims; and, finally, if the data subject has objected to processing, and while the verification whether the legitimate grounds of the controller override those of the data subject is pending.

Finally, the right to object (Article 21 GDPR) empowers data subjects to express opposition, because of his or her particular situation, and at any time, to processing of personal data concerning him or her. This right might be exercised, inter alia, when such processing is based on the necessity of processing for the purposes of the legitimate interests pursued by the controller or by a third party (see Article 6 GDPR). In this case, the controller shall no longer process the personal data unless compelling legitimate grounds for the processing which override the rights of the data subject concur.

The GDPR also regulates the right of data subjects not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22 GDPR).

These rights mean obligations for the processors which must be borne in mind all throughout the processing.

2.2.2.5 *Controller and processor obligations*

In correlation with the rights of data subjects, many substantial obligations fall on data controllers and processors.

- According to Article 5(1)(b) of the GDPR, personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.' This means that, in principle, data collected for one purpose cannot be re-used for another purpose, unless this other purpose is compatible with the original one. In assessing compatibility of purposes account should be taken of the data subject's reasonable expectations.
- According to Article 5(1)(c) of the GDPR, collected personal data must be adequate, relevant, and necessary. This principle needs careful consideration by companies scraping websites, because their software usually gathers data in bulk.
- According to Article 5(1)(e) of the GDPR, personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.' Therefore, in principle, long-term storage of non-anonymized personal data is impossible from the legal point of view, with exceptions concerning archiving in public interest.
- According to Article 5(1)(f) of the GDPR, personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.' Arguably, if personal data are publicly available on the internet, the threshold of 'appropriate security' required in their processing is rather low.

- According to Article 5(2) of the GDPR, the controller shall be responsible for, and be able to demonstrate compliance with the abovementioned principles. This means that in case of a dispute between the data subject and the data controller, the burden of proof is on the latter. In other words, the data controller must prove that he or she respected the law.

As we can see, controllers are in charge of implementing appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR, such as maintaining a record of processing activities under his or her responsibility (Article 30 GDPR). Such record shall contain the identification of the controller, any controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data to be processed; the categories of recipients to whom the personal data have been or will be disclosed, including third countries' recipients; the time limits for erasure of data; and, if possible, a general description of the technical and organisational security measures adopted by the controller.

If the processing takes place outside the EU/EEA, then the controller must appoint a representative of him or her in the EU/EEA, which is the so-called processor. According to the GDPR, processors are responsible for a number of tasks, such as: processing the personal data on documented instructions from the controller; ensuring that persons authorised to process the personal data have committed themselves to confidentiality; taking all measures required pursuant to the security of processing; assisting the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights; assisting the controller in ensuring compliance with the obligations enacted in the GDPR related to ensuring the security of the processing and the assessment of the data protection impact; and, at the choice of the controller, deleting or returning all the personal data to the controller after the end of the provision of services relating to processing. As to the security of processing, this matter is regulated in a more complete way in Articles 32 to 36 of the GDPR, which explain which are the areas that need to be covered when assessing the security of processing, the notification of data breaches and the data protection impact assessment ('DPIA').

Apart from the controller and the processor, the GDPR foresees the appointment of data protection officers ('DPOs'). These are independent agents of the controllers in charge of tasks such as informing and advising the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR; monitoring the compliance with the GDPR, with other data protection provisions and with the policies of the controller or processor in relation to the protection of personal data; cooperating with the supervisory authority; and acting as the contact point for the supervisory authority.

2.2.3 Open-source and publicly available data scraping: privacy interference?

The mere fact that data are publicly available does not imply an absence of restrictions to collecting and processing them. 'Publicly available data' does not mean publicly 'owned' data. Individuals' contact details published in online public spaces, names, and affiliations of people, are still personal data, even if data are publicly available. As such, a data scraping company may not freely re-use the data and may not further process it without the individuals' consent. Restrictions imposed by the GDPR do not apply to data about companies. However, data about companies often includes users' data, such as, for example, comments on social media posts. If the non-personal data and the personal data are 'inextricably linked,' the data protection rights and

obligations arising under the GDPR apply fully to the whole mixed dataset, even if the personal data only represents a small part of the set.

Moreover, 'data scraping' and 'data mining' are likely to be classified as 'data processing' whenever related to personal data (according to the broad definition of Article 4(2) GDPR). In the view of the CJEU, in fact, certain activities currently at the core of data scraping companies' business model, such as the act of referring, on an internet page, to various persons and identifying them by name or by other means,[19] as well as the activity of a search engine consisting in finding information published on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference,[20] are indeed data processing actions.

2.2.3.1 *The requirement of a legal ground for personal data processing*

Industry partners that cannot justify a legal ground for collecting and processing personal data should not engage in the practice. As already seen in section 2.2.2, there are six lawful bases available under the GDPR for the collection and processing of personal data: consent; contract with the data subject; compliance with a legal obligation; vital interest; public interest; legitimate interest (Article 6(1) GDPR). Consent is only one of several legal grounds to process personal data, rather than the main ground. It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the industry partner's or from the data subject's perspective, but the availability of some of the other options described above may be limited. This is not because the GDPR makes a distinction about such bases being available for only public sector bodies. It has more to do with the practical realities of facilitating the use of these legal bases. In most cases, the only potentially fitting lawful grounds for industry partners are consent, contract, and legitimate interest.

a) Consent[21] and the impracticability exception

If an industry partner wants to scrape the personal data of EU/EEA citizens and residents it needs to demonstrate that it has the explicit consent of the individual before scraping their personal data. Such consent must be freely given, related to a specific purpose, informed, and unambiguous. This means that a certain amount of information about the processing must be provided to the data subject so that they can validly consent; moreover, consent cannot be blank, but it must be limited to a specific (narrowly defined) purpose. It can be argued that if a data subject publishes personal information about themselves on a publicly accessible website, they are implicitly giving their consent for that information to be processed by anyone with internet access. However, that implied consent must be understood as a consent for the information to be used for website-related purposes, not as a blanket consent for anyone to use that information for any purpose. It is important to think about what a typical user may reasonably expect. Moreover, when it comes to processing of

[19] Judgment of the Court (Grand Chamber), 6 November 2003, Lindqvist, Case C-101/01; paragraphs 43-48.

[20] Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12; paragraph 30.

[21] Consent as a legal ground has been analysed in Opinion 15/2011 of the Article 29 Data Protection Working Party on the definition of consent, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

sensitive data (i.e., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, data concerning health, sex life or sexual orientation), consent needs to be explicit.

Therefore, in many cases a company's scraping may need to adhere to the notice-and-consent requirement. In fact, under Article 14 of the GDPR, companies that indirectly collect personal information, even from publicly accessible sources, need to provide notice unless doing so 'proves impossible or would involve a disproportionate effort' (the impracticability exception).

The EDPB, in its Guidelines on transparency under Regulation 2016/679,[22] states that 'you should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information.' In the context of personal data, if it is not possible for a data scraping company to adhere to Article 14 GDPR (consent), and as the data are not collected directly from the individuals, data scraping will be considered 'invisible' processing and classified as 'high risk'. Article 35(1) of the GDPR requires controllers to conduct a 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) of the 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. Other processing activities may require DPIAs. 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). Moreover, the EDPB's Guidelines on Data Protection Impact Assessment[23] provide an example of 'the gathering of public social media for generating profiles' as requiring a DPIA. The reason being, this processing includes evaluating or scoring, processing data on a large scale, matching and combining datasets and sensitive data or data of a highly personal nature as possible relevant criteria. Accordingly, many national data protection authorities consider this to be 'high risk' processing for which a DPIA is required.

In **Bulgaria**, the national Data Protection Authority ('DPA') adopted a List of processing operations requiring a DPIA pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/67924 of the processing activities where a 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 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; also in case of regular and systematic

[22] Available at: https://ec.europa.eu/newsroom/article29/items/622227.

[23] Available at: https://ec.europa.eu/newsroom/article29/items/611236.

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

processing for which the provision of information pursuant to Article 19 of the GDPR by the controller to the data subject is impossible or requires disproportionate efforts.

In **Italy**, the national data protection authority simply adopted the same list contained in the EDPB's Guidelines on Data Protection Impact Assessment.

In **Spain**, the national DPA has issued a list of activities which require a DPIA ('Blacklist').[25] The Blacklist includes, among others: processing that involves the use of data on a large scale; processing that involves the association, combination, or linking of records in databases from two or more data-processing events with different aims or by different controllers; processing that prevents interested parties from exercising their rights, using a service, or executing a contract, such as for example processing where data have been compiled by a controller distinct from the controller who is to process them, and any of the exceptions regarding the information that ought to be provided to the interested parties under Article 14(5)(b), (c), (d) of the GDPR apply.

Another way to demonstrate compliance for both controllers and processors is the adherence to an 'approved' code of conduct (Article 32 GDPR). Not only the GDPR encourages it, also Member States, supervisory authorities and the EDPB do it.[26]

b) Contract

The provision covers situations where processing is necessary for the performance of the contract to which the data subject is a party. Most companies store the name, email, password, and other personal data from their clients, which is a normal procedure. The provision regarding contractual obligations, though, must be interpreted strictly. It does not include circumstances in which the processing was imposed on the data subject by the controller unilaterally rather than being really required for the fulfilment of a contract. For instance, if a business keeps detailed records of its customers' queries, along with a history of the documents and queries they have accessed as well as their preferences and processes these data to improve suggestions and deliver better service, these processing activities should be specifically mentioned in the contract. Because this fact alone does not make them 'necessary' for the performance of the contract, the exact rationale of the contract, i.e., its substance and fundamental objective must be clear, as it is against this that it will be tested whether the data processing is necessary for its performance. Given the ease and availability of the collection and processing of personal data online, the EDPB[27] asserts that the purpose of data collection must be 'clearly and specifically identified' and as such, 'a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research', without more detail, usually do not meet the criteria of being 'specific'.

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

[26] Most approved codes are national. In May 2021, with the blessing from the EDPB and the approval from the Belgian DPA, the EU Cloud Code of Conduct became the first approved transactional code under the GDPR.

[27] Article 29 Working Party Opinion 03/2013 on Purpose Limitation (WP203 2013), at 15–16. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

c) Legitimate interest

A third lawful reason available to industry partners is if they can demonstrate they have a legitimate interest in scraping/storing/using these personal data. Legitimate interest is, in fact, the most flexible lawful basis for processing. The GDPR does not specify what exactly the legitimate interest of a data controller means. However, Recital 47 gives certain clues, stating that such legitimate interest may be a ground for processing provided that 'the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.' Legitimate interest should not be treated as 'a last resort' for rare or unexpected situations where other grounds for legitimate processing are deemed not to apply.

Since for private companies it may be difficult to demonstrate that they have a legitimate interest in scraping someone's personal data, it is worth noting that some national laws have defined broadly that processing of certain data is necessary for the purposes of the legitimate interest pursued by a data controller.

Article 19 of the **Spanish Data Protection Law** allows the processing of contact data and individual entrepreneur and liberal professional data, that is, data relating to the function or position held by natural persons providing services in a legal person. In absence of a proof to the contrary, it is considered a processing 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data' (as indicated in Article 6(1)(f) GDPR). Some requirements must be met:

(a) the processing relates solely to data necessary for their professional location;

(b) the purpose of the processing is solely to maintain relations of any kind with the legal person in which the data subject provides his or her services.

The underlying assumption is that if data subjects make their personal data (name, email, affiliation) publicly visible on websites such as an open-access journal, they somehow invite people to contact them. Therefore, it seems possible to assume data subjects, by making certain data public, expect that these data may be used to identify and, in some cases, to contact them.

The same presumption of necessity applies to the processing of data relating to sole entrepreneurs and liberal professionals, when it relates to them solely in that capacity and is not processed for the purpose of establishing a relationship with them as natural persons.

The allegation of a legitimate interest requires weighing the interests of the business against those of the individual and the latter's reasonable expectations, which must be addressed by national legislation. However, a good evaluation in this case goes beyond a simple balancing test that involves just comparing and weighing two easily quantifiable and equivalent 'weights.' In order to ensure that the interests and fundamental rights of data subjects are properly considered, the test instead calls for careful assessment of several elements. It is scalable since it can range from easy to very complex. At the same time, it does not have to be overly difficult.

To make this assessment, the elements and circumstances of the specific case must be considered. One of those elements that can be assessed, and which may play in favour of assessing this legitimate interest, is the fact that the data were accessible to the public, as recalled in EDPB Opinion 06/2014 on legitimate interests of the

data controller,[28] which cites as one of the key factors to be considered when carrying out the 'balancing test' whether the data are held in sources accessible to the public or whether the data have been disclosed to the public or otherwise made available to a large number of persons. Anyway, disclosure must be weighed against the other concurrent circumstances. In no case it exempts compliance with the other principles of personal data protection law.

According to what has been said, factors to consider when carrying out the balancing test include:

- The nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned. The promotion of technological innovation for law enforcement purposes through the business activity of the data scraping company could be argued in this regard. Data scraping is increasingly being deployed for the gathering of criminal intelligence because it provides investigators with access to both data that are hypothetically available using traditional methods, but data subjects or data controllers are unresponsive to police's request (Luscombe and Walby, 2017: 382), and data that are otherwise difficult or impossible to obtain. Moreover, data scraping has the potential to capture phenomena as they occur in real time in their natural environment (Marres and Weltevrede, 2013: 315), with only a minimal risk that investigators will influence criminal behaviour as it is observed (Holt and Bossler, 2015: 183). Web scrapers are used to collect data from personal websites and blogs, social media, chat rooms, web forums, online marketplaces, video streaming platforms and peer-to-peer networks that can be found in the Surface Web, the Deep Web and the Dark Web to gain knowledge and understanding in support of preventing crime and pursuing offenders. Open-source and publicly available data are a particularly interesting data source in this regard. Analysing the textual and relational content on publicly available websites and extracting innovation-related information from them has the potential to provide LEAs with a cost-effective way to survey millions of pieces of information, gain insights into criminal activities, and understand links between individuals within complex, rapidly evolving interactive criminal networks. Data scraping companies that work in this sector offer a better way of gathering criminal intelligence. In the fight against organized crime, big data analytics is applied to automatically process information sources, extract frequent patterns, detect anomalies and predict trend evolution, in order to build a richer context that helps LEAs: 1) to understand the broader socio-economic scenario in which illegal activities happen, in order to forecast the evolution of a certain type of crime in a concrete region (Larsen et al., 2017); 2) to analyse digital marketplaces where illicit goods and services are being bought and sold (Soska and Christin, 2015; Barrera et al., 2019; Frank and Mikhaylov, 2020): 3) less frequently criminal acts and perpetrators (Décary-Hétu et al., 2014; McAlister, 2015), 4) as well as possible victims (Perry et al., 2013). In this case, the private business interest of a company coincides with a public interest. As the EDPB Opinion 06/2014 on legitimate interests of the data controller puts it, 'In general, the fact that a controller acts not only in its own legitimate (e.g., business) interest, but also in the interests of the wider community, can give more 'weight' to that interest. The more compelling the public interest or the interest of the wider community,

[28] See Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

and the more clearly acknowledged and expected it is in the community and by data subjects that the controller act and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance.'

- The impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed. 'Impact' as used here covers any possible (potential or actual) consequences of the data processing. The concept encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data, considering that the purpose of Article 7(f) of the GDPR balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact, as highlighted by the EDPB Opinion.

The Spanish DPA (**Agencia Española de Protección de Datos**, AEPD) issued on April 26, 2021, a decision in proceeding PS/00240/2019,29 fining **Equifax Ibérica, SL** €1.000.000, following 96 complaints against the same, for the inclusion of personal data of individuals associated with alleged debts in the File of Judicial Claims and Public Bodies ('FIJ'), without their consent, and in some cases without such data being accurate. In particular, the decision highlights that these data were publicly available, originally disclosed in documents of public administrators and public law entities, and published through newsletters or newspapers, with the purpose of making effective the notification of an administrative or judicial resolution. These individuals' publicly available data were scraped by Equifax to use them in credit reports. The decision outlines that Equifax violated Article 6(1) in relation to Article 5(1)(a), (c), and (d) of the GDPR. Furthermore, the decision highlights that Equifax also violated Article 14 of the GDPR by failing to comply with the transparency regime under the GDPR, obliging data controllers to provide data subjects with information about their personal data, where such data has not been obtained from the data subjects themselves. Lastly, the decision highlights that the legitimate interests of Equifax - an interest (from the controller and the third parties to be recipients of the data) linked to the assessment of the financial solvency of the data subjects, and an interest linked to fraud prevention- could not be established as a valid legal basis for the processing of personal data in the FIJ. In this case, there was no connection between one purpose (a public notification that constitutes a guarantee to preserve a fundamental right of the data subject, and that therefore overrides their right to data protection) and Equifax's purpose (providing potential harmful or negative information about the data subjects to different businesses). There could not have been any reasonable expectation of the data subjects for their data to be processed in such a way, given the context.

In this evaluation, facts such as whether the personal data are disclosed to the general public or only to a restricted number of people, whether data are combined with other information from different sources or whether the processing involves sensitive data or not are important,[30] once guaranteed that they will not be

[29] Available in Spanish at https://www.aepd.es/es/documento/ps-00406-2020.pdf.

[30] Even in case data were sensitive, one controversial ground for processing sensitive data relates to sensitive data that have been 'manifestly made public'. The European Data Protection Supervisor, in its Preliminary Opinion on data protection and scientific research, has recently provided guidance on when this base can be used stating: 'Special categories of data may be processed if the data subject has manifestly made them public. EU data protection authorities have argued that this provision has to be 'interpreted to imply that the data subject was aware that the respective data will be publicly available

combined with other data in such a way that they may lead to inferences about sensitive data nor can lead to uncanny, unexpected or inaccurate predictions. Furthermore, it is relevant to consider the terms and conditions of the website on which data were made public: users may have specific expectations based on such terms and conditions as to how their data will be processed. If such reasonable expectations conflict with the operation of the data scraping company, the processing of the data may become unlawful. The more particular and limiting the context of collecting, the more restrictions there are on use.

Additional safeguards which could limit undue impact on the data subject are data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability. In fact, even when assessing the existence of a legitimate interest, the principles of data protection regulations must be respected. This includes the provision of information to data subjects even in instances where consent is not used as the legal basis for processing, in so far as this obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In many cases, only governments, universities, LEAs, etc., will have what would be deemed a legitimate interest in scraping the personal data of citizens as they will typically be scraping people's personal data for the public good. But the same can be said about RITHMS industry partners. They carry out scientific research in the pursue of a legitimate interest that strongly correlates with a public interest. Recital 159 of the GDPR admits the relevance of scientific research as a lawful ground for data processing. According to this Recital, where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area. Furthermore, there is enough literature on the many advantages that companies scraping open-source and publicly available data offer in producing technological innovation for law enforcement when compared with other traditional invasive and unobtrusive investigative methods, such as the interception of communications or hacking, particularly in terms of a wide range of data quality dimensions, including accuracy, completeness, currency, quantity, flexibility, and accessibility. Such exploration is likely to open new ways to generate complex innovation processes that help to promote law enforcement.

The GDPR, even as a regulation protecting personal data, aims to offer a flexible regime when data are used for scientific research. Nevertheless, the GDPR requires, as a counterbalance, the implementation of solid safeguard measures that must be implemented by researchers when processing personal data. The European Data Protection Supervisor ('EDPS') expressly refers to this question in the document 'A preliminary opinion on data protection and scientific research' (6 January 2020):[31] 'the special regime cannot be applied in such a way that the essence of the right to data protection is emptied out, and this includes data subject rights, appropriate organisational and technical measures against accidental or unlawful destruction, loss or alteration, and the

which means to everyone' including, in this case, researchers, and that, 'In case of doubt, a narrow interpretation should be applied, as the assumption is that the data subject has voluntarily given up the special protection for sensitive data by making them available to the public including authorities'. Publishing personal data in a biography or an article in the press is not the same as posting a message on a social media page.' (EDPS 2020: 19).

[31] Available at: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

supervision of an independent authority. There is also a specific reference to open data: Personal data which are 'publicly available' - such as those collected from social media sites - are still personal data.'

Also, according to Article 6(3) of the GDPR, the basis for the processing referred to in point (e) of paragraph 1 shall be laid down by Union law or Member State law to which the controller is subject. The EDPS highlights the need of a regulated access across the EU to personal data for research purposes that serve a public interest (e.g., to improve healthcare provision), noting the uncertainty around what counts as 'scientific research'. In any case, being in the frame of a research project within Horizon Europe, the admissibility of an activity of scientific research presenting public interest can be undoubtedly stated. As the EDPS also points out, 'building on the considerable harmonisation efforts of the European Commission in the research area with Horizon 2020 and Horizon Europe, the next European Research and Innovation framework programme, can also support convergence across the Member States.' Even taking such public interest as a lawful ground for processing these data, it must be noted that many website hosts have sought to inhibit automated access via data scraping requiring users to agree to terms and conditions or terms of use that explicitly prohibit data scraping. In these specific cases, consent will not apply as a lawful ground, but all provisions in Article 6(1) of the GDPR have the same legal status: consequently, public interest can be alleged as a lawful ground for processing in absence of consent.

Finally, it must be noted that the GDPR establishes restrictions for the processing of special categories of personal data. Article 9 of the GDPR refers to 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. The processing of these data is prohibited (Article 9(1)), unless any of the conditions of Article 9(2) are met: specifically, point (e) allows the processing of personal data which are manifestly made public by the data subject, while point (g) admits the processing of these special data 'when processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;' moreover, point (j) refers to the case when 'processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

Notwithstanding these provisions, the EDPS highlights in the above-mentioned document that 'such laws have yet to be adopted. It is therefore difficult at present, if not impossible, to view a 'substantial public interest' as a basis for processing sensitive data for scientific research purposes.' More clearly, the EDPS also states: 'Special categories of data may be processed if the data subject has manifestly made them public. EU data protection authorities have argued that this provision has to be 'interpreted to imply that the data subject was aware that the respective data will be publicly available which means to everyone' including, in this case, researchers, and that, 'In case of doubt, a narrow interpretation should be applied, as the assumption is that the data subject has voluntarily given up the special protection for sensitive data by making them available to the public including authorities'. Publishing personal data in a biography or an article in the press is not the same

as posting a message on a social media page.' In fact, it should be guaranteed that the processing activity is directly connected to those personal data that have been manifestly made public by the data subject; that there is evidence of a deliberate, affirmative act by the data subject themself to make their data available, and that the data are public such that any hypothetical interested member of the public could access them; and that the data have been made manifestly public by the data subject themself or the data subject has given a clear indication to an intermediary to make their data public (as proposed by Dove and Chen, 2021: 122).

Furthermore, regarding certain categories of data in the hands of public bodies, recent legislative developments in the EU in the field of data governance (the Open Data Directive[32] and the Data Governance Act[33]) aim to make more data available by regulating the re-use of publicly available information held by the public sector. The public sector also holds protected data (e.g., personal data and commercially confidential data) that cannot be re-used as open data but that could be re-used under specific EU or national legislation. The new legislative instruments show that data sharing, including personal data, is for the EU a crucial tool to enable new products and services based on novel technologies, make production more efficient, and provide tools for combatting societal challenges.

2.2.3.2 *Purpose limitation, data minimisation and other principles, rights and obligations related to data protection*

Even if a valid basis for processing personal data is found, subsequent processing must be made lawfully, fairly, and in a transparent manner in relation to the data subject (Article 5(1)(a) GDPR). For an industry partner that does not adhere to consent as the legal ground for processing, it may be hard to prove that invisible scraping is fair and transparent. A DPIA and the adherence to an approved code of conduct will help. Anyway, as already shown in section 2.2.2, many other conditions apply.

2.3.4 Cross-border data transfers

The EU allows companies and public administrations to store and process non-personal data wherever they choose. Such data still needs to be available to regulatory authorities. Nevertheless, the Non-Personal Data Regulation's main obligations relate to Member States rather than corporations, and these obligations are considerably more lenient than those imposed by the GDPR.

One of the main goals of harmonization of EU data protection law was to allow free transfer of personal data within the EU. As a result, such data can be freely transferred within the EU, providing that all the requirements of the GDPR, including principles of lawfulness and purpose limitation, are met. This is not an easy task.

Following the Schrems I judgment, Facebook Ireland explained that it transferred much of the data to its US parent company based on standard contract clauses ('SCCs'). On 1 December 2015, Max Schrems reformulated his complaint lodged with the Irish DPA to the effect that the SCC Decision was not able to justify the transfer of personal data to the US, since US surveillance programmes interfered with his fundamental rights to privacy,

[32] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, p. 56–83.

[33] Proposal for a Regulation of the European Parliament and the Council on European Data Governance (Data Governance Act) (COM/2020/767 final).

to data protection, and to effective judicial protection. In a draft decision, the DPA shared Schrems' concerns and brought an action before the Irish High Court, which then referred to the Court for a preliminary hearing. In the meantime, another transfer mechanism, the Privacy Shield Decision, became pertinent to the case, which prompted the CJEU also to rule on the validity of this instrument.

In **Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems** ('Schrems II'), Case C-311/18, the CJEU held that the US does not provide for an essentially equivalent, and therefore sufficient, level of protection as guaranteed by the GDPR and the EU Charter of Fundamental Rights. Additionally, the court affirmed the validity of the SCC Decision and held that SCCs do not, per se, present lawful or unlawful grounds for data transfer (no panacea). The CJEU also stipulates that data controllers or operators that seek to transfer data based on SCCs, must ensure that the data subject is afforded a level of protection essentially equivalent to that guaranteed by the GDPR and EU Charter of Fundamental Rights – if necessary, with additional measures to compensate for lacunae in the protection of third-country legal systems. Failing that, operators must suspend the data transfer. Supervisory authorities must check transfers and are required to prohibit transfers where they find that data subjects are not afforded essentially equivalent protection. Implications for commercial data transfers are not clear.[34]

In many EU/EEA-based companies, data are processed by the web-node and stored in a Virtual Machine located outside the EU, for instance in the US. There must be an explicit consent from the data subject to this data transfer. When personal data is transferred outside the EU/EEA, special safeguards are foreseen in the EU to ensure that the protection travels with the data. The GDPR applies to any transfer of personal data undergoing processing or intended for processing after transfer to a third country or to an international organization. It restricts transfers of personal data outside the EU/EEA, unless the rights of the individuals in respect of their personal data are protected in another way, or one of a limited number of exceptions applies. These restrictions include:

- Sending of personal data from inside the EU/EEA – or making it accessible – to a receiver located in a country outside the EU/EEA. Consider even your 'read-only' support model and geography when thinking about 'making it accessible'.
- Personal data to be held on servers abroad. Consider your disaster recovery and archival plans too.
- Emails or attachments that contain personal data sent to recipients abroad.
- Transfers to another company within the same corporate group.

One does not actually have to 'send' the data to a non-EU/EEA country for these provisions to apply. If one of the partners or service providers is located outside the EU and can access the personal data one has collected, this amounts to a 'data transfer' in the context of the GDPR.

Certainly, the GDPR offers a variety of mechanisms to transfer personal data to third countries, provided that adequate safeguards are in place: explicit consent of the data subject, after having been informed about

[34] See the opinion of the European Parliamentary Research Service, available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

potential risks – which are quite high in the case of data transfers to the US -, adequacy decisions,[35] standard contractual clauses,[36] binding corporate rules,[37] certification mechanism, codes of conduct,[38] so-called 'derogations',[39] etc. However, there remains a significant amount of uncertainty in this area. Nowadays, the US Government and the European Commission ('EC') are negotiating a new EU-US Data Privacy Framework that will allow the Commission to issue a new adequacy decision in the following months. Until then, any transfer of EU/EEA data subjects' personal data to the US needs that the controller sets appropriate safeguards before such transfer takes place.

2.3 Copyright law

In addition to limitations imposed by privacy and data protection laws, open-source and publicly available data may also be subject to intellectual property rights. Copyright and database rights are the most important intellectual property rights for OSINT. Much information that is accessible through open sources is protected. It is important to note that just because a work is freely accessible to the public or a copyright notice is absent, it cannot be inferred that the owner of the rights has renounced those rights. The same is true if content is not

[35] The European Commission has the power to determine, on the basis of Article 45 GDPR, whether a country outside the EU/EEA offers an adequate level of data protection. The adoption of an adequacy decision involves: a) a proposal from the European Commission; b) an opinion of the European Data Protection Board; c) an approval from representatives of EU countries; and d) the adoption of the decision by the European Commission. The effect of such a decision is that personal data can flow from the EEA/EU to that third country without any further safeguard being necessary. In other words, transfers to the country in question will be assimilated to intra-EU/EEA transmissions of data. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR, and Uruguay as providing adequate protection. The US is not included in the list.

[36] According to the GDPR, contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU/EEA to third countries. This includes model contract clauses – so-called standard contractual clauses ('SCCs') – that have been pre-approved by the European Commission. On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR). Until 27 December 2022, controllers and processors can continue to rely on earlier SCCs for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged.

[37] In the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules.

[38] Transfers are allowed if appropriate safeguards include adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.

[39] Derogations under Article 49 GDPR are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights to continue to benefit from their fundamental rights and safeguards.

technologically protected, a rights holder does not restrict access to the work, a rights holder does not show that he retains, exercises, or enforces his right, or for any other non-waivable reason.

2.3.1 Rules on copyright

The EU law governing copyright is scattered throughout several directives. These legal instruments provide for a high level of protection for rightsholders and create a framework in which the exploitation of protected works can take place.

Directive 2001/29/EC[40] ('**Copyright Directive**') must be borne in mind. This instrument was incepted in order to protect the copyright and related rights in the framework of the internal market, with particular emphasis on the information society (Article 1). It establishes certain rights for the copyright holders, one of them being the right to authorise or prohibit direct or indirect, temporary or permanent reproduction of their works by any means and in any form (Article 2). Nevertheless, in accordance with Article 4 of Directive 96/9/EC[41] ('**Database Directive**'), in the matter of text and data mining, no authorisation will be required in relation to the reproduction and extractions of lawfully accessible works. In this instrument, databases are conceived as collections of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means (Article 1(b)). The starting point is that databases are protected as intellectual property – i.e., copyright -, as long as the selection or the arrangement of the contents of the database is an author's own intellectual creation (Article 3).

The protection enshrined for authors sets up several acts that require their authorisation to be carried out by anyone. Such acts are enlisted in Article 5. They include:

- temporary or permanent reproduction by any means and in any form, in whole or in part;
- translation, adaptation, arrangement and any other alteration;
- any form of distribution to the public of the database or of copies thereof;
- any communication, display or performance to the public;
- any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).

Despite these restrictions, Directive (EU) 2019/79042 ('Digital Single Market' or '**DSM Directive**') establishes a limitation to the need for authorisation of temporary or permanent reproduction by any means and in any form, in whole or in part of a database, when it comes to carrying out text and data mining activities (the so-called Text and Data Mining or 'TDM' exception). As stated in Recital 18 of the DSM Directive, this limitation should only apply where the work or other subject matter is accessed lawfully by the beneficiary, including when it has

[40] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 0010-0019.

[41] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

[42] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.5.2019, p. 92–125.

been made available to the public online, and insofar as the rightsholders have not reserved in an appropriate manner the rights to make reproductions and extractions for text and data mining. In the case of content that has been made publicly available online, it should only be considered appropriate to reserve those rights using machine-readable means, including metadata and terms and conditions of a website or a service. In Section 3 we will study the application of this regulation to companies that scrape publicly available data for profit.

The Database Directive also enacts a '*sui generis*' right as core protection for databases' makers when such makers are EU nationals or have their residence in the EU. This right is set as follows: 'Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database' (Article 7). This sui generis right seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collecting the contents by protecting the database against certain acts by a user or competitor.

The sui generis right has limitations. So, firstly, the right might be transferred by contract or license; secondly, the maker of a database which is made available to the public in any manner cannot prevent a lawful user of the database from extracting and/or reutilizing insubstantial parts of its contents with independence of the purposes such lawful user is seeking. This right also has exceptions. The most relevant exception when it comes to data scraping is enshrined in the DSM Directive (Article 4) and essentially allows for extractions and reutilizations of the whole or a substantial part of the contents of the database for purposes of text and data mining.

Another relevant European legal instrument is Directive 2009/24/EC[43] ('**Software Directive**') on the legal protection of computer programs. The Software Directive protects computer programs by copyright (Article 1(1)). It states that computer programs shall be protected as literary works, this is, in accordance with the **Berne Convention for the Protection of Literary and Artistic Works**, enacted in 1979.

The Berne Convention sets up several rights that protect literary authors in relation to their works. In this regard, there are two types of intellectual property rights: economic rights and moral rights. Some of them may easily fit in the rights to be granted to computer programs developers, and to anyone who makes adaptations on those computer programs. The so-called 'moral rights' consist in the right to claim authorship of the work, and the right to object to any distortion, or modification of their work, which would be prejudicial to their reputation (Article 6 bis (1) of the Berne Convention). As economic rights, the Berne Convention enshrines the exclusive right of making and of authorizing the translation of their works (Article 8), the exclusive right of authorizing the reproduction of these works, in any manner or form – although such reproduction might be allowed as long as it does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author (Article 9 of the Berne Convention) -, and, finally, the exclusive right of authorizing adaptations, arrangements and other alterations of their works (Article 12 of the Berne Convention).

[43] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 5.5.2009, p. 16–22.

In the Software Directive, the expression 'computer programs' means 'programs in any form, including those which are incorporated into hardware' (according to Recital 7), and as long as it is original in the sense that it is the author's own intellectual creation (Article 1(3)). The latter requirement introduces a very interesting legal principle, known as the 'idea/expression doctrine' (Margonie and Kretschmer, 2022: 689), which basically means that 'ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright' (Article 1(2) of the Software Directive). So, as stated in Recital 11 of the Software Directive, 'only the expression of a computer program is protected, meanwhile ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright.' So, because logic, algorithms and programming languages comprise ideas and principles, such ideas and principles are not protected.

Be that as it may, Article 4 of the Software Directive restricts both the permanent or temporary reproduction of a computer program, as well as the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof. So, in principle, an authorisation must be issued by the copyright holder to carry out such actions. Still, Article 4 of the DSM Directive also establishes limitations to this restriction, by allowing the aforementioned reproductions when the access to the computer program was lawful and has taken place with the aim of text and data mining.

A mention must be made to Directive 2019/79044 (also known as the '**Directive on Copyright in the Digital Single Market**', or 'CDSM'). This directive explicitly tackles the legal regulation of data mining. In accordance with this instrument, there are two possible legal scenarios in relation to data mining. In the first one, data mining may be carried out in relation to acts protected, both through copyright and through the sui generis database right. It is also possible that both rights concur in the protection of a certain database. In these cases, where no exception or limitation applies, an authorisation to undertake such acts is required from rightsholders. In the second scenario, data mining may involve mere facts or data that are not protected by copyright and, therefore, data mining activities do not require any authorisation. Therefore, it must be understood that data mining is allowed where the work is accessed lawfully by the beneficiary, including when it has been made available to the public online, as insofar the rightsholders have not reserved the rights to make reproductions and extractions of text and data in an appropriate manner (Recital 18 CDSM).

Finally, Directive 2019/1024[45] on open data and the re-use of public sector information (the '**Open Data Directive**') must be borne in mind. This instrument indicates that documents stemming from public sector bodies of the Member States –i.e., public universities, governmental agencies, public research institutes, etc.- shall be re-usable for commercial and non-commercial purposes. In these cases, it may be possible that the institution in charge of the data requires that a request for re-use is submitted (Article 4) and may in certain cases charge a fee for such re-use (Article 6). The Open Data Directive excludes data which are not accessible due to commercial and statistical confidentiality and data that are included in works or other subject matter over which

[44] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.5.2019, p. 92–125.

[45] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, p. 56–83.

third parties have intellectual property rights. Commercially confidential data includes data protected by trade secrets, protected know-how, and any other information the undue disclosure of which would have an impact on the market position or financial health of the undertaking.

Some of the provisions established in this directive are broadened in Regulation 2022/868[46] on data governance, which has entered into force on 23 June 2022, 20 days after its publication in the Official Journal of the European Union but will only apply from 24 September 2023. The **Data Governance Act** establishes the right to re-use the aforementioned data, even when such data are protected by confidentiality or copyright law (Article 3).[47] The public institution in charge may impose certain limitations to the re-use of such data, e.g., with previous anonymization or deletion of confidential information, to access data in secure premises, and the like. The public institution may also be able to verify any results of processing of data undertaken by the re-user, as well as reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties (Article 5 of the Data Governance Act). This instrument has a specific focus on promoting access to such data by SMEs and start-ups (Recital 15). The intellectual property rights of third parties, though, should not be affected by this regulation. Moreover, such processing should be carried out in accordance with Union law on the protection of individuals regarding the processing of personal data (see section 2.2).

2.3.2 Copyright infringement

Because data scraping is essentially a form of copying using bots, it firmly falls within the subject matter of copyright laws (Ballon, 2020). Data scraping and web crawling are fundamentally tools for copying information, facts, and data online. A scraping bot accesses websites and makes copies of those websites, parses the websites' code, and stores information in a database. Copyrighted data, though, are not allowed to be replicated on other websites that scraped them from the source. Some exceptions to this rule include, e.g., official works or purely factual statements (such as product names, prices, features, train schedules, or data concerning web traffic), which are supposedly copyright-free. In the EU, in principle, copyright-protected content cannot be reproduced or communicated to the public without the permission of the rightsholders, unless the use is covered by a statutory exception. As the licensing of the single contributions proves to be unrealistic, our attention will be mostly directed to the legal permits. Below, we will refer to several aspects of that protection that may conflict with business models based on scraping publicly available data for profit. Brief descriptions of judicial cases illustrate the problems and the answers given by the legal system.

2.3.2.1 Scraping websites and social media sites

Scraping websites and social media sites and storing data in the data scraping company's system may entail an infringement of intellectual property. Rightsholders have an exclusive right to authorise communication of their work. Data scraping could violate the rights of the authors or other rightsholders of text contributions.

[46] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 152, 3.6.2022, p. 1–44.

[47] This regulation applies to personal data that fall outside the scope of the Open Data Directive insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules.

However, to consider the copyright infringed, it is necessary that the public being communicated to is a 'new public' in respect to the public originally targeted by the rightsholders. In short, rightsholders' authorisation is not required when the relevant act of communication to the public, such as providing a clickable link to protected works, targets the same public as the initial communication.

A case was brought to the CJEU following a Swedish litigation involving journalists and the owners of a website which provided visitors with links to the journalists' articles that were published on freely accessible newspapers' websites. The journalists sought compensation from the website owners claiming that the website owners infringed on their exclusive right to make their articles available to the public by providing the links on the website. In **Judgment of the Court (Fourth Chamber), 13 February 2014, Nils Svensson and Others v Retriever Sverige AB, Case C-466/12**, the court ruled that since the journalists published their articles on the internet, and the articles were accessible for free, the 'public' targeted by the website manager who provided the clickable links was the same public initially targeted by the authors. The court also decided that there is no distinction between cases where the protected work is shown after the client is redirected to another website and cases where it is not clear that the client is being redirected if the targeted 'public' is the same in both accounts.

There is no distinction to be drawn between cases where the protected work is shown after a click on another website and cases where such work is shown in a way that gives the impression that it is on the original website (i.e., 'framing').

In **Order of the Court (Ninth Chamber), 21 October 2014, BestWater International GmbH v Michael Mebes and Stefan Potsch, Case C-348/13**, the CJEU, accordingly with the Svensson case, ruled that embedding a copyright protected work on a website through framing or 'transclusion' technology cannot be considered communication to the public according to Article 3(1) of the Copyright Directive as long as the copyright protected work is neither communicated to a new public nor communicated by technical means that differ from the technical means of the initial communication. The court held that whenever and as long as a work is freely available on the site pointed to by an internet link, it must be considered that when the copyright holders authorised the communication, they considered all internet users as the public.

The authorisation of the rightsholder, though, is always required when the original access to the relevant contents is protected by means of technical measures[48] or when the relevant content is no longer accessible on the website where the communication commenced. In these cases, indeed, "it is arguable that the provision of the clickable link is targeted to a 'new public' than the one considered by the subject who made the initial communication" (Bellezza, 2014). Moreover, when the link leads to unlicensed content (i.e., a content that was uploaded without the authorisation from rightsholders), the knowledge of the unlicensed character of the content is presumed when the link is provided with a profit-making intention (Peguera, 2019). So, e.g., when a

[48] Here understood as any security measure aimed at protecting the scrapped content from being accessed, not only authentication and authorisation systems and paywalls, but also white lists of HTTP user agents, analysis of the cookie settings or the request format. Such technical measures can be avoided by altering the content of request headers, choosing suitable cookie settings, varying the sequence of requested URLs, varying the time intervals between requests, changing the IP address.

link to unlicensed content is on a website containing commercials, the owner of the website would have to prove that he or she was not aware of its unlicensed character.

In **Judgment of the Court (Second Chamber) of 8 September 2016, GS Media BV v Sanoma Media Netherlands BV and Others, Case C-160/15**, the CJEU ruled that in order to establish whether the fact of posting, on a website, hyperlinks to protected works, which are freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public', it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed.

EU law provides an explicit list of exceptions from copyrights granted to the rightsholders, each with a specific scope. One of them is related to databases (see 2.3.2.2), another one to screen and cached copies (see 2.3.2.3).

2.3.2.2 Sui generis database right and the Text and Data Mining exception

The Database Directive provides specific protection with regards to databases. A database is copyrighted if the structure of the database is an original intellectual creation. Computer code, which may be included in HTML,[1] in form of JavaScript code that executes in the web browser, at the user device, is explicitly classified as a type of work that may be protected by copyright. The ability of web scrapers (in themselves) to copy voluminous amounts of HTML content from multiple webpages immediately raise concerns of copyright infringement (Ang, 2021).

However, not all HTML content is protected by copyright, as copyright protection only extends to the creative efforts expended by the author of a work.

What 'work' means in this context has been clarified by the CJEU in **Judgment of the Court (Third Chamber), 12 September 2019, Cofemel - Sociedade de Vestuário SA, v G-Star Raw CV, Case C-683/17**. In accordance with the doctrine of the court, the concept of 'work' constitutes an autonomous concept of EU law. This concept requires two cumulative conditions to be satisfied. The first condition demands that there exists an original object that is the author's own intellectual creation –for this, it is both necessary and sufficient that the object reflects the personality of its author, as an expression of his or her free and creative choices. The second condition requires that the classification as a work is reserved to the elements that are the expression of such creation. So, if the process of creation of an object has been dictated by technical considerations or rules, which leave no room for creative freedom, that object cannot be conceived as possessing the originality required for it to constitute a 'work'. In this regard, the European Court, in **Judgment of the Court (Fifth Chamber), 11 June 2020, SI and Brompton Bicycle Ltd v Chedech / Get2Get, Case C-833/18**, has clarified that even though the existence of other possible ways to achieve the same technical result makes it possible to establish that there was a possibility of choice by the author, this is not decisive in assessing the factors which influenced the choice made by the creator and, thus, in these cases there is no originality in the sense of EU copyright law.

HTML code (way of writing text) is in most cases not original enough, but the content itself might be considered original. Therefore, when considering whether data scraping might result in copyright infringement, the real

question to be asked is generally whether the HTML content copied by web scrapers is 'original' enough to warrant copyright protection.

This turns out to be an extremely difficult question to answer. The CJEU[49] explains that the "criterion of originality is satisfied when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices [...] By contrast, that criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom". Holders' rights to their copyrighted text may be violated even by reproducing just one sentence if it is of special originality.

In the **Judgment of 16 July 2009, Infopaq International A/S v Danske Dagblades Forening, Case C-5/08**, the CJEU asserted that even an excerpt of 11 words might be protected (paragraph 47). In this case, the claimant, a professional association of Danish daily newspapers publishers, sued a corporation which operated a media monitoring which consisted primarily in drawing up summaries of selected articles from Danish daily newspapers. The respondent considered that it was not required to obtain the consent of the rightsholders for acts of reproduction of newspaper articles using an automated process consisting in the scanning and then conversion into digital files followed by electronic processing of that file. Contrarily, the European Court stated that 'an act occurring during a data capture process, which consists of storing an extract of a protected work comprising 11 words and printing out that extract, is such as to come within the concept of reproduction in part within the meaning of Article 2 of the Copyright Directive, if the elements thus reproduced are the expression of the intellectual creation of their author.' So, even if words as such do not constitute elements covered by the protection, given the requirement of a broad interpretation of the scope of the protection conferred by Article 2 of the Copyright Directive, the possibility may not be ruled out that certain isolated sentences, or even certain parts of sentences in the text in question, may be suitable for conveying to the reader the originality of a publication such as a newspaper article, by communicating to that reader an element which is, in itself, the expression of the intellectual creation of the author of that article. So, even if the data collected consists only in few words, it might be necessary to request the author's authorisation to collect such data, if the extracted sentence is an expression of the author's intellectual creation.

While just a very minimal amount of originality is necessary for a work to be protected by copyright, there are numerous aspects of HTML code that make even this minimal requirement challenging to meet (Ang, 2021: 6).

In **Judgment of the Court (Third Chamber), 1 March 2012, Football Dataco Ltd and Others v Yahoo! UK Ltd and Others, Case C-604/10**, the court found it is irrelevant to consider the intellectual effort and skill that went into creating the original data; the key tenant for protection is whether there is originality expressed in selecting or arranging the data.

In fact, it may be difficult to prove a copyright over such data since only a specific arrangement or a particular selection of data is legally protected. Moreover, although compilations of facts can be protected by copyright, authors may not copyright their ideas or the facts they narrate. Accordingly, if the data scraped are purely facts without a creative component, the code is seen as 'factual', rather than creative, in nature, or as being primarily dictated by functional purposes rather than authorial creativity, then there is no copyright claim. Databases are

[49] In the CJEU Judgment of 1 March 2012, Football Dataco Ltd and Others v Yahoo! UK Ltd and Others, Case C-604/10.

usually quite regular, technical, composed in a way to demonstrate in the clearest way possible ('dictated by technical considerations') specific data. Usually, they are not organized creatively. Many of them are not copyrighted. However, it is extremely difficult to guess what a domestic court would say about the work's originality. Therefore, it is safer to assume that most of the databases from which one is scraping are copyrighted (as advised by Szwed, 2021). As the copyright protects the structure and organization of the database (and not the data included therein), the scraping simply cannot lead to copying or republishing the original database's structure (or a substantial part of it).

Even if the database is not original, it still may be protected. The Database Directive grants a sui generis protection to the EU 'maker of a database[50] which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents.' The CJEU sets a very high threshold for the 'substantial investment' requirement.

In **Judgment of the Court (Grand Chamber) of 9 November 2004, The British Horseracing Board Ltd and Others v William Hill Organization Ltd, Case C-203/02**, the court ruled that 'the expression 'investment in... the obtaining... of the contents' of a database in Article 7(1) of Directive 96/9 on the legal protection of databases must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database. The expression 'investment in... the... verification... of the contents' of a database in Article 7(1) of Directive 96/9 must be understood to refer to the resources used, with a view to ensuring the reliability of the information contained in that database, to monitor the accuracy of the materials collected when the database was created and during its operation. The resources used for verification during the stage of creation of materials which are subsequently collected in a database do not fall within that definition.' Therefore, in the context of drawing up lists of horse races, the resources used to draw up a list of horses entered in a race constitute investment not in the obtaining of the contents of the database but in the creation of the data making up the lists relating to those races. The resources used for the checks prior to the entering of a horse on a list for a race relate to the stage of creating the data making up that list and thus do not constitute an investment in the verification of the contents of a database.

Whenever there was a substantial investment, the database maker is entitled to prevent extraction and/or re-utilization[51] of the whole or a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database (Article 7 of the mentioned Directive). Mining these databases qualifies as an 'extraction' under Article 7(2) of the Database Directive. Evaluating whether a part is indeed substantial can be performed quantitatively (in relation to the total size of the database) and/or qualitatively (i.e., by measuring the scale of the human, technical or financial investment). Hence, even when only a small part of the entire database is extracted, this may represent a qualitatively substantial part, e.g., when the affected part constitutes the core part of the database or the part containing the most useful information.

[50] It must be highlighted that the sui generis database right protects only databases whose makers or rightsholders are nationals of an EU Member States or have their habitual residence in an EU Member State. This excludes the databases (e.g., websites) owned by companies based in the US, which can obviously still be protected by copyright.

[51] 'Reutilization' or 'reuse' is understood as making the contents of the database available to the public by any means.

As indicated by Szwed (2021), a balance is sought between database rights and free access to information and the development of innovative products. For that reason, there is no reproduction of a substantial part of a database if scraping is technically limited to the required extent within the framework of the research objective. Assuming that scraping is limited to posts relevant to individual topics, such as posts including certain hashtags from the numerous written contributions available on a social media platform, the courts usually consider that there is no reproduction of substantial parts of a database (Golla and Müller, 2020). Moreover, it must always be examined whether there is any damage on the part of the database holder. Database holders will therefore have to prove their damage.

The CJEU ruled on **Judgment of the Court (Fifth Chamber) of 3 June 2021, SIA 'CV-Online Latvia' v SIA 'Melons', Case C-762/19**, that a balance must be sought between database rights and free access to information and the development of innovative products and that for that reason it must always be examined whether there is any damage on the part of the database holder. Database holders will therefore have to prove their damage.

The proof of inflicted damage is likely to be very difficult in many cases. After all, aggregator websites very often refer exactly to the source website where they have copied data. In many cases the question will be whether more visitors (and therefore potential customers) are or are not led to the source website in this way. In the first case, there can hardly be any damage.

To make a local copy and then analyse that local copy systematically, though, does not avoid risks.

Online company Melons did not scrape websites in real time. It periodically made a local copy and then analysed that local copy systematically. CV Online, a Latvian online job database whose vacancies database was used by Melons via a search request from users on the Melons website, protested. Melons made a copy of (meta) data from the CV Online site and searched that local copy every time a search was made by users on its website. The CJEU ruled on **Judgment of the Court (Fifth Chamber) of 3 June 2021, SIA 'CV-Online Latvia' v SIA 'Melons', Case C-762/19**, that even if a search engine does not search other websites in real time but makes a local copy to search them, it still (potentially) violates database law, if there are investments that ensure a protected database. The court confirms that the terms 'reclaim' and 'reuse' from the Database Directive must be interpreted in the broadest sense and that the aim of the Directive is to prevent someone else taking the income on the back of those who made the investment to establish the database. The court also says that a balance must be sought between database rights and free access to information and the development of innovative products and that for that reason it must always be examined whether there is any damage on the part of the database holder. Database holders will therefore have to prove their damage.

If all conditions are met, the sui generis database right protects the content of a database. Protection is granted automatically for 15 years starting either from the creation date or from when the database was first made publicly available. Such data can be scraped (and, therefore, copied and contents of the protected database collected - which falls under the definition of 'extraction' under the analysed Directive) as long as there is no scraping of a 'substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database' and no reuse of it (meaning basically selling or publishing it); or the appropriate licence has been received; or

scraping falls under the Text and Data Mining ('TDM') exception described below.

Even if databases are copyrighted, it is allowed to copy databases (and use them for one's own purposes, not republishing or selling), if one's actions fall under the TDM exception. Article 4 of the Database Directive provides an exception from the rights of the database owner mentioned above in case of 'reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining', unless 'the use of works and other subject matter referred to in that paragraph has not been expressly reserved by their rightsholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online.' Generally, then, the DSM Directive allows for scraping (reproduction and extraction) of data from the databases for the purpose of text and data mining even if they are granted copyright or sui generis protection (Szwed, 2021). However, the TDM exception is limited. On the one hand, neither qualitatively nor quantitatively substantial parts of a database can be extracted or re-utilized without the permission from the holder of the sui generis database right. Repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the owner of the database are expressly prohibited (Article 7(5) of the Database Directive). Therefore, a crawling operation in which the crawler repeatedly and systematically visits a website only to copy a non-substantial part of its contents (e.g., 3%) at each visit is unlawful when this activity can be considered as a mean to circumvent the obligation to obtain the rightsholder's authorisation (Kamocki et al., 2018). On the other hand, database owners are granted the possibility to restrict the reproduction and extraction of the databases and their content. That restriction must be made in a manner that will allow bots, crawlers, etc., to see it. Therefore, on a website there should be some means of communicating scraping bots that scraping is prohibited, such as RFC 9309 'Robots.txt files'. Any such restriction should, in any case, be respected. Whenever a scraping company uses a proxy service for some data sources, the company must take into account that the proxy service may not be respecting such restrictions. Moreover, utilizing these proxy services is related with the use of Residential IPs and IP rotation, which avoids blocking upon the website detects the scraping activity.

The **Spanish Supreme Court, First Civil Chamber**, in **Judgment of 9 October 2012, rec. 536/2010**, in the case **Ryanair v Atrápalo**, decided that the website of an airline company is not a database protected by copyright. In the lawsuit concerning copyright infringement committed by a travel agency (Atrápalo, defendant) by accessing the website of an airline company (Ryanair, plaintiff) and, by means of a computer programme (screen scraping), extracting the information requested by its clients, projecting the result on the agency's own website, the action was dismissed. The court did not find infringement of the sui generis right of database manufacturers linked to a quantitative or qualitative investment for the collection, verification or presentation of their content. The expenditure and investment in the creation or production of the data cannot be compared with the expenditure and investment necessary for the collection, verification or presentation of the data. The investment made by the applicant concerned the creation of software that allows the generation of the information based on certain parameters, i.e., the investment concerns the generation of the information, but not its collection and presentation. Regarding the possibility of unfair competition, the court did not find free riding on the efforts of others. The decision of the question was based on the fact that there is no database

but a computer programme that makes it possible to obtain the information requested, by generating it on the basis of the parameters previously entered. Consequently, there is no 'extraction' of data from it, and, in any event, it is the travel agency's client, and not the travel agency, who contracts and incorporates the data generated by the applicant into other media.

In Italy there was also a case over a dispute about the practice of screen scraping (**decision of June 4, 2013, of the Court of Milan, in the Viaggiare S.r.l. vs Ryanair Ltd case**), representing the first time that an Italian court addressed the issue of the lawfulness of screen scraping practices (we follow here Barbieri and Belleza, 2014). According to the court, there was no infringement by Viaggiare of Ryanair's trademark rights - by showing Ryanair's logo via its website without Ryanair's consent since, according to the Court, such use falls within the 'descriptive use' exception set out by Section 21 of the Italian IP Code (Legislative Decree 30/2005), thus it is lawful even without Ryanair's authorisation. In this respect the Court says that Viaggiare "uses the defendant's logos, as well as those of other air carriers, only to inform prospective clients about the real identity of the relevant air carrier [...] database rights - by 'screen scraping' Ryanair's website to provide consumers with relevant information on flights (e.g., place of departure and arrival, time, date, price, etc.), since Ryanair's database cannot be deemed 'creative', thus it is not eligible for database copyright protection under the Italian Copyright Law (Law 633/1941)". Moreover, the court gives relevance to the fact that the screen scraping carried out by Viaggiare did not trigger the reproduction of the Ryanair's website but only the reproduction of pieces of information contained on the website. The court notes that Ryanair has in principle sui generis database rights on the relevant database (which contains information on flights), having provided evidence of significant investments made to collect and present the relevant contents of said database. However, in the specific case, the court states that Ryanair did not suffer an undue prejudice to its investments because of the screen scraping activity, being this demonstrated by the circumstance that Ryanair does not prevent to extract and reuse data on flights included in its database to protect its investments.

2.3.2.3 Screen and cached copies and the Article 5(1) of the Copyright Directive exception

Browsing the internet without the copyright owner's permission does not infringe copyright. The ordinary use of internet involves the creation of temporary copies at several stages. Copies are created during transmission in internet routers and proxy servers. Where a webpage is viewed by an end user on his or her computer, without being downloaded, the technical processes involved require temporary copies to be made on screen and in the internet cache on the hard disk. Screen or cached copies only refer to temporal storage of data for its processing. Therefore, it is not considered data storage, but data processing. The screen copy is self-evidently an essential part of the technology involved, without which the webpage cannot be viewed by the user. It remains on screen until the user moves away from the webpage. The function of the internet cache is more complex. It is a universal feature of current internet browsing technology: it is a folder full of web pages in the user's computer that is maintained by the web browser for a period. If the local, cached page has not been updated on the web, it is retrieved immediately by the browser, saving download time. In none of these cases (screen copy and cached copy) does the end user set out to make a copy of the webpage unless he or she chooses to download it or print it. The case law of the CJEU holds that the creation of the screen and cached copies does not conflict with a normal exploitation of the works.

The Public Relations Consultants Association ('PRCA') is an association of public relations professionals, who use the media monitoring service offered by the Meltwater group of companies ('Meltwater'), which makes available to them, online, monitoring reports on press articles published on the internet, those reports being compiled on the basis of key words provided by the customers. The Newspaper Licensing Agency ('NLA') is a body set up by the publishers of newspapers in the United Kingdom for the purpose of providing collective licensing of newspaper content. The NLA took the view that Meltwater and its customers were required to obtain authorisation from the copyright holders for, respectively, providing and receiving the media monitoring service. Meltwater agreed to enter a web database licence. The PRCA, however, maintained that the online receipt of the monitoring reports by Meltwater's customers do not require a licence. In **Judgment of the Court (Fourth Chamber), 5 June 2014, Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and Others, Case C-360/13**, the CJEU ruled that Article 5 of the Copyright Directive must be interpreted as meaning that the copies on the user's computer screen and the copies in the internet 'cache' of that computer's hard disk, made by an end-user in the course of viewing a website, satisfy the conditions that those copies must be temporary, that they must be transient or incidental in nature and that they must constitute an integral and essential part of a technological process, as well as the conditions laid down in Article 5(5) of that directive, and that they may therefore be made without the authorisation of the copyright holders. Concretely, first, since the on-screen copies and the cached copies are created only for the purpose of viewing websites, they constitute, on that basis, a special case. Next, although the copies make it possible, in principle, for internet users to access works displayed on websites without the authorisation of the copyright holders, the copies do not unreasonably prejudice the legitimate interests of those rightsholders. In this connection, it is pointed out that the works are made available to internet users by the publishers of the websites, those publishers being required, under Article 3(1) of the Copyright Directive, to obtain authorisation from the copyright holders concerned, since that making available constitutes a communication to the public within the meaning of that article. The legitimate interests of the copyright holders concerned are thus properly safeguarded. In those circumstances, there is no justification for requiring internet users to obtain another authorisation allowing them to avail themselves of the same communication as that already authorised by the copyright holder in question. Lastly, it must be held that the creation of the on-screen copies and the cached copies does not conflict with a normal exploitation of the works.

The CJEU did not address whether the copying exemption under Article 5(1) applies where internet users download, print, or store the material being browsed. The conditions that a reproduction be temporary and transient or incidental, however, suggest that it does not.

3 In research and development. National legal frameworks

3.1 Introduction

Member States' legal framework governing issues relevant to this report, such as data protection, accessibility, or dual-export regulation, is essentially a transposition of the EU law. This means that the general principles that rule these legal areas are set up in EU regulations and directives. Insofar as they assign rights and obligations to certain social groups or institutions and almost all required

regulatory decisions, regulations are often complete regulatory actions. However, in some circumstances, they permit the maintenance or introduction of national laws to more precisely define how their rules must be applied. For instance, the GDPR seeks to ensure a consistent and high level of protection of natural persons about the processing of personal data, but it also provides a margin of manoeuvre for Member States to specify its rules, including, e.g., determining more precisely the conditions under which the processing of personal data is lawful. Directives, unlike regulations, are not meant to be complete normative acts. They are binding as to the result to be achieved, upon each Member State to which they are addressed, but they also leave to national authorities the choice of form and methods. Thus, directives impose on national legislators the regulatory result which they must achieve but leave them the choice how to achieve such result. This implies that they provide domestic politics room to choose extra policies in a particular policy area. Therefore, even if these directives bind the States in terms of the regulatory outcome to be attained, how this outcome will be obtained in various States may vary. In practice, directives vary from those which do leave to national legislator wide space for making additional policy choices to those which are very detailed and leave no real, substantive choice. Therefore, a correct analysis of the European and national legal frameworks must bear in mind such legal instruments and the differences among them. Concerning data protection, one of the positive consequences of this interplay is that Member State law on these areas is mostly very similar to that in other EU countries, i.e., the different European domestic laws on data protection are harmonised. Careful attention, though, merit some national particularities that are relevant for this report. They can be found in some EU Member States, but not in others, or not to the same extent. In the following country-case studies, attention will be focused on these particularities, but only if they have any relevance for the industry partner's activity on behalf of the RITHMS Consortium. Therefore, this report does not offer a complete explanation of all aspects related to data protection. It only addresses those that are relevant for RITHMS.

3.2 Belgium[52]

3.2.1 Relevant texts

The main legal instrument implementing the GDPR in Belgium is the **Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data** ('the Act'). The Act incorporates elements of the GDPR. It also transposes the LED, establishing the Police Information Supervisory Body. Moreover, the Act specifically addresses the processing of personal data by other authorities such as intelligence and security services and the armed forces, processing in the context of classification, and security clearances, security certificates, and security advice, processing by the coordination body for threat analysis and the processing of passenger data. Several laws have also been adapted to align them with the GDPR (e.g., the Video Surveillance Act).

In addition, the Belgian DPA, established by the Act of 3 December 2017 establishing the Data Protection Authority (the 'DPA law'), publishes guidance for professionals and citizens, including guidelines that address frequently asked questions on specific themes, formal advice, recommendations, and decisions of its Litigation

[52] In this section we follow the very complete reports of Stassen and Van Remoortel (2022), D'hulst, Van Bael and Bellis (2022) and DLA Piper Data Protection Laws of the World – Belgium, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=BE&c2=

Chamber. There are legislative proposals for a reform of Belgian data protection law (i.e., both the Data Protection Act and the DPA law). The exact timing of adoption of these proposals is currently unclear.

3.2.2 Legal bases

In general, the Belgian Act does not differ much from the GDPR. It lists specific processing operations that are considered to be for reasons of substantial public interest, in accordance with Article 9(2)(g) of the GDPR, but they are not relevant for RITHMS. Moreover, regarding scientific or historical research purposes, Article 186 of the Act establishes that controllers who intend to rely on the exceptions foreseen by Article 89(2) and (3) of the GDPR must comply with the provisions of Title 4 of the Act. It requires data controllers to include, among other things, following information in their record of processing:

- a justification for the non-use of pseudonymised data;
- the reasons why the exercise of data subject rights is likely to seriously impair or render impossible the pursued purposes; and
- the DPIA.

In addition to what is required under Article 13 of the GDPR, data controllers must also inform the data subject as to whether the personal data are anonymised or not, and the reasons why the exercise of the data subject rights is likely to seriously impair or render impossible the achieved purposes. Regarding further processing, a data controller that processes personal data for scientific or historical research purposes not directly obtained from the data subjects must enter into an agreement with the original controller, unless an exception applies. This agreement must contain the details of both controllers and the reasons why the exercise of the data subject rights is likely to seriously impair or render impossible the pursued purposes. The agreement must be added to the record of processing. Furthermore, scientific or historical research must be performed based on anonymised data. If it is not possible to achieve the research purpose with anonymised data, then the controller must use pseudonymised data. If it is not possible to achieve the research purpose with pseudonymised data, then the controller may use non-pseudonymised data. Personal data obtained directly from the data subject must be pseudonymised or anonymised after collection. In case of further processing for scientific or historical research purposes, the personal data must be pseudonymised or anonymised before initiating further processing or before disclosure to another controller for further processing. Pseudonymised data may only be de-pseudonymised if necessary for the research and after advice from the DPO. In case of further processing by another controller, the other controller may not have access to the pseudonymisation keys.

3.2.3 Principles

All principles of Article 5 of the GDPR are applied as such in Belgium.

3.2.4 Controller and processor obligations

Most provisions regarding controller and processor's obligations foreseen in the GDPR apply in Belgium without variations.

Data processing notification

The registration of processing activities through a notification has been abolished. However, in the public sector, the Act obliges the controller of processing activities in the context of police services to publish a protocol detailing the transfer to a public authority or private body based on public interest and compliance with legal obligations (Article 20).

DPIA

Regarding DPIAs, the Belgian DPA has adopted following guidelines:

- Guidelines on DPIAs.[53]
- Prior consultation form for DPIAs.[54]
- DPIA Guide.[55]

In application of Article 35(4) of the GDPR, the Belgian DPA has issued a draft list of the types of processing operations for which a DPIA shall be required, but there is no final list available yet. The Draft List provides that the following types of processing operations require a DPIA:[56]

- biometric data, when collected for the purpose of uniquely identifying data subjects who are in a public space or a private publicly accessible area;
- data collected from third parties which are subsequently taken into account in the context of a decision to refuse or terminate a service contract;
- health data, when collected by automated means with the aid of an active implantable medical device;
- data collected on a large scale from third parties in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons;
- special categories of data, when systematically exchanged between several controllers;
- large-scale processing of data, when generated by Internet of Things devices which serves to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons;

[53] Available in French at: https://www.autoriteprotectiondonnees.be/comment-savoir-si-un-traitement-de-donnees-doit-faire-lobjet-dune-aipd.

[54] Available in Dutch at: https://www.gegevensbeschermingsautoriteit.be/publications/formulier-voor-voorafgaande-raadpleging-over-een-verwerking-met-hoog-restrisico.docx. Also available in French at: https://www.autoriteprotectiondonnees.be/publications/formulaire-pour-une-consultation-prealable-sur-projet-de-traitement-a-haut-risque-residuel.docx.

[55] Available in Dutch at: https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-gegevensbeschermingseffectbeoordeling.pdf. Also available in French at: https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf.

[56] Available in English at:

- large-scale and/or systematic processing of telephony or communication data, metadata or location data which allows to trace natural persons when the processing is not strictly necessary for a service requested by the data subject; and
- large-scale processing of data whereby the behaviour of natural persons is systematically observed, collected, established or influenced by automated processing, including for advertising purposes.

The Belgian DPA has not issued a list with activities for which no DPIA is required. If the risk can be adequately reduced by appropriate technical and organisational measures, no prior consultation with the DPA is necessary.

Special categories of data

The Act requires that the controller, when processing genetic data, biometric data and data concerning health, lists the categories of persons having access to those personal data (Article 9).

The Act also specifies a limitative list of cases where the processing of data relating to criminal convictions and offences is authorised (Article 10).

3.2.5 Data subject rights

In general, data subjects' rights in Belgium do not offer significant variations from what is guaranteed in the GDPR. The Act provides for some limitations to these rights, e.g., in the context of processing of personal data by state intelligence services (Articles 11-17).

3.3 Croatia[57]

3.3.1 Relevant texts

The main legal instrument implementing the GDPR in the Republic of Croatia is the **Act on the Implementation of the General Data Protection Regulation** ('the Data Protection Act'), enacted on 27 April 2018, which entered into force on 25 May 2018.

This Act covers the same scope as the GDPR. It establishes additional rules on the processing of personal data in the following cases: children's consent in relation to information society services; processing of genetic and biometric data, processing of personal data in connection with video surveillance; and processing of personal data for statistical purposes.

Beyond this text, there are other national statutes that foresee specific rules for data processing and use, such as: the Bylaw on the Content and Manner of Keeping Records on Employees, the Labour Law, the Act on Anti-Money Laundering and Terrorism Financing, or the Act on Legal Consequences of a Conviction, Criminal Records, and Rehabilitation. The Electronic Communications Act and the Electronic Commerce Act are also relevant regarding confidentiality of electronic communications, and transmission, caching and hosting of data in the communication network when providing information society services.

[57] In this section we follow Manuilenko and Novoselic (2023) and DLA Piper Data Protection Laws of the World – Croatia, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=HR.

In addition, the Personal Data Protection Agency, which is the Croatian DPA ('AZOP') has published guidance and recommendations on specific data processing issues.

3.3.2 Legal bases

The Croatian Data Protection Act does not contain any specifications to the definitions contained in the GDPR. It is important to highlight that once data has been acquired, the data controller cannot modify the legal basis for data processing. For instance, if there were issues with the legality of the consent, it would not be permitted to later invoke the legitimate interest legal basis for processing. The controller must select the legal basis it will use prior to the acquisition of personal data due to the requirement that the legal basis be identified by the controller at the time of the collection of personal data.

According to the AZOP, determining whether a legitimate interest exists necessitates careful consideration of various factors, including whether the data subject might reasonably expect processing for the relevant purpose at the time and within the circumstances of the collection of personal data. If personal data is processed in a situation where data subjects do not reasonably expect further processing, their interests and basic rights may prevail over the controller's interests.

3.3.3 Principles

All principles of Article 5 of the GDPR are applied as such in Croatia.

3.3.4 Controller and processor obligations

Most provisions regarding controller and processor's obligations foreseen in the GDPR apply in Croatia without variations.

DPIA

Regarding **DPIAs**, the AZOP adopted the Decision on Determining and Publicising a List of the Kind of Processing Operations that are Subject to the Requirement for a Data Protection Impact Assessment ('the Croatian Blacklist').[58] This list contains the following cases:

1) processing personal data for systematic and extensive profiling or automated decision-making to bring conclusions that are of significant influence or may affect an individual and/or several persons, or that help deciding about someone's access to a service or convenience (e.g. such as personal data processing related to economic or financial status, health, personal preferences, interests, reliability, behaviour, location data, etc.);
2) processing of special categories of personal data for profiling or automated decision-making;
3) processing of personal data of children for profiling or automated decision-making, for marketing purposes, or for direct offering of services intended for them;

[58] Available in English at: https://edpb.europa.eu/sites/default/files/decisions/list_of_the_types_of_processing_for_dpia_croatia_35_4.pdf.

4) processing of personal data collected from third parties that are considered for making decisions regarding the conclusion, termination, rejection, or extension of service contracts with natural persons;
5) processing of special categories of personal data or personal data on criminal or misdemeanour liability on a large scale;
6) processing of personal data by using systematic monitoring of publicly available places on a large scale;
7) use of new technologies or technological solutions for personal data processing or with an option of personal data processing (e.g. the application of Internet of Things such as smart TVs, smart home appliances, smart toys, smart cities, smart energy meters, etc.) that serve to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movement of natural persons;
8) processing of biometric data in combination with any of the other criteria set out in the WP29 DPIA Guidelines used to evaluate whether certain processing operations are likely to cause a high risk to the rights and freedoms of the data subjects;
9) processing of genetic data in combination with any of the other criteria set out in the WP29 DPIA Guidelines used to evaluate whether certain processing operations are likely to cause a high risk to the rights and freedoms of the data subjects;
10) processing of personal data by linking, comparing, or verifying their matching by using multiple sources;
11) processing of personal data in a manner that involves monitoring of the location or behaviour of an individual in case of systematic processing of communication data (metadata) generated by the use of a telephone, the internet, or other communication channels such as GSM, GPS, Wi-Fi, monitoring or processing of location data;
12) processing of personal data by means of devices and technologies where an incident may put at risk the health of an individual or more persons; and
13) processing of employee personal information by means of applications or monitoring systems (e.g. processing of personal data for monitoring of work, movement, communication, etc.).

This list is not exhaustive and could be changed if new processing dangers are discovered or experienced. No prior consultation with the AZOP is required if the risk can be adequately addressed by appropriate technical and organizational measures.

Special categories of data

Regarding the processing of genetic and biometric personal data in the public sector, public authorities may process biometric data if such processing is defined by law and is necessary for the protection of persons, assets, classified information or professional secrets, provided that the interests of data subjects that contravene such processing do not prevail. Processing of biometric data necessary for fulfilment of international treaties related to identification of data subjects during crossing of state borders is considered as lawful. In the private sector, biometric data can only be processed if it is prescribed by statutory law and necessary for the protection of persons, property, classified data, business secrets, or for individual and safe identification of

service users, if the purposes for processing biometric data do not prevail over the interests of data subjects. Private entities may process biometric data for the purposes of safe identification of users of services, but only based on explicit consent given by the users in accordance with the provisions of the GDPR.

When it comes to criminal conviction data, the national Act on Legal Consequences of a Conviction, Criminal Records, and Rehabilitation, adopted in 2012, has not been amended since the GDPR entered into force. Therefore, its provisions are not aligned with the GDPR. Among other aspects, this Act establishes that criminal records are maintained by the Ministry of Justice and Administration (except for juvenile convicts, which are maintained by the Ministry of Demography, Family, Youth and Social Policy). According to this Act, direct access to criminal records is provided to courts and the State Attorney's Office, as well as to the police for the prevention, detection and prosecution of criminal offences.

3.3.5 Data subject rights

In general, no substantial variations from the GDPR are provided by the Croatian data protection law. There is only one exception regarding the processing of personal data for the purpose of producing official statistic, which is not relevant for RITHMS.

3.4 Finland[59]

3.4.1 Relevant texts

In Finland the GDPR has been implemented by the **Data Protection Act (1050/2018)** ('Data Protection Act'), which entered into force on 1 January 2019 and repealed the old Personal Data Act (523/1999). According to Article 3 of the Data Protection Act, if the controller is based in Finland, then Finnish law regulates the processing of personal data when it involves establishments of controllers or processors operating on EU territory.

In addition to general data protection legislation, Finland has other specific laws on the processing of personal data. Most of such laws deal with the processing of personal data by the authorities. Specific enactments either impose more precise provisions on the processing of personal data in a certain field or specify how the personal data may be processed by derogation from the general legislation. Some examples are the Act on the Protection of Privacy in Working Life (759/2004, amended in 2019);[60] the Act on the Secondary Use of Health and Social Data (552/2019);[61] the Public Administration Information Management Act (906/2019),[62] which defines the entire lifecycle of information in public administration; and the Act on the Processing of Personal Data in Criminal

[59] In this section, we follow Nevalainen, Vaaraniemi and Hård af Segerstad (2023) and DLA Piper Data Protection Laws of the World – Finland, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=FI&c2=.
[60] Available in English (non-binding unofficial translation) at: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf.
[61] Available in English (non-binding unofficial translation) at: https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf.
[62] Available in English (non-binding unofficial translation) at: https://www.finlex.fi/en/laki/kaannokset/2019/en20190906.pdf.

Matters and in Connection with Maintaining National Security (1054/2018),[63] which implements the LED (Directive (EU) 2016/680), providing detailed rules for processing information on criminal offences by authorities. It is also important the Act on Electronic Communications Services (previously called the Information Society Code) (917/2014),[64] which includes provisions on confidentiality of electronic communications. This Act sets out obligations for the processing of communications data, data retention, and electronic direct marketing.

The Finnish Data Protection Authority is the Data Protection Ombudsman.

3.4.2 Legal bases

In Finland, all definitions laid down by Article 4 of GDPR are applied as such.

Finish Data Protection legislation includes all legal grounds foreseen in Article 6 of the GDPR. The Data Protection Act contains certain specifications on the application of some of these legal bases. For instance, the applicable age of consent in relation to information society services offered directly to a child is 13 years. Moreover, there are specific rules regarding the processing of personal data for the performance of tasks carried out in the public interest. Article 4 of the Data Protection Act permits controllers to process personal data under Article 6(1)(e) of the GDPR if:

- the data describe the position of a person, his or her duties or the performance of these duties in a public sector entity, business and industry, activities of civil society organisations, or other corresponding activities, in so far as the objective of the processing is of public interest and the processing is proportionate to the legitimate aim pursued;
- the processing is proportionate and necessary for the performance of a task carried out in the public interest by an authority;
- the processing is necessary for scientific or historical research purposes or statistical purposes and it is proportionate to the aim of public interest pursued; or
- the processing of research material and cultural heritage material containing personal data and the processing of personal data included in their metadata for archiving purposes is necessary and proportionate to the aim of public interest pursued and to the rights of the data subject.

The Data Protection Act states that processing of personal data done only for academic, artistic, or literary expression is not covered by the legal justifications outlined in Article 6 of the GDPR. Data protection in scientific research merits much attention by the Finnish Data Protection Act.[65] It is indicated that 'in certain situations, the processing of personal data for the purposes of scientific and historical research can be considered compatible with the original purpose if the appropriate technical and organisational safeguards are implemented in the processing. The controller's processing of personal data for compatible purposes can be based on the same processing basis as the original processing, in which case a new basis is not required. The processing must also

[63] Available in English (non-binding unofficial translation) at: https://www.finlex.fi/fi/laki/kaannokset/2018/en20181054.pdf.
[64] Avaiable in English (non-binding unofficial translation) at: https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf.
[65] Office of the Data Protection Ombudsman. Scientific research and data protection. [Online]. Available at: https://tietosuoja.fi/en/scientific-research-and-data-protection.

be lawful from the perspective of other data protection regulations; a compatible purpose does not justify non-compliance with other data protection regulations. When a controller intends to process personal data for purposes other than the original purpose of processing, it must notify the data subjects of this before starting processing.'

Additionally, the Data Protection Act contains special provisions regarding the processing of personal identity codes. These codes may only be processed in situations where it is important to identify a person, and in those situations, only with that person's consent or if the processing is required by law. Personal identity codes may also be handled in a few additional circumstances that are listed in the Data Protection Act. A personal identity code may not, unless essential, be included in printed documents or documents created using data from a file system, according to the Data Protection Act.

3.4.3 Principles

Finland legislation has implemented all principles contained in Article 5 of the GDPR.

The Data Protection Ombudsman has stated that the accountability principle entails the obligation to document the measures taken to fulfil accountability requirements, such as internal and external guidelines for exercising the data subjects' rights.

On the other hand, according to the principle of openness of government activities, the documents of the public authorities shall be public, unless otherwise provided by law (Article 28 of the Data Protection Act).

3.4.4 Controller and processor obligations

Data processing notification

According to Finish legislation, it is not obligatory to notify regulators of any processing under the GDPR, with the exception of the requirement to notify the details of a DPO to the Office of the Data Protection Ombudsman.

The Act on Electronic Communications Services 917/2014 provides that legal persons who are involved in the provision of communication services or an added value service for a purpose other than telecommunications operations (corporate subscribers) must inform the Office of the Data Protection Ombudsman in advance of processing data traffic for certain purposes.

DPIA

The Office of the Data Protection Ombudsman has issued a List of Processing Operations which require at (Finnish Blacklist), in line with Article 35(4) of the GDPR and the EDPB's Guidelines on Data Protection Impact Assessment and determining whether processing is 'likely to result in a high risk' for the purposes of the GDPR. The Finnish Blacklist complements and further specifies these guidelines. It is of non-exhaustive nature. Thus, a DPIA must be conducted:

1. When biometric data is processed for the purpose of uniquely identifying a natural person, if at least one of the following circumstances are present:

- the processing of biometric data is used in systematic monitoring of data subjects;
- biometric data is processed for evaluation or scoring of the data subject;

- processing of biometric data is aimed at automated decision making with legal or similar significant effect;
- biometric data is processed on a large scale;
- processing of biometric data includes matching or combining datasets;
- processed biometric data is concerning vulnerable data subjects;
- biometric data is processed in innovative use or applying new technological or organisational solutions;
- processing of biometric data prevents data subjects from exercising a right or using a service or a contract.

2. When genetic data is processed, if at least one of the following circumstances apply:

- genetic data is processed on a large scale;
- genetic data is processed to evaluate or score a person;
- genetic data is processed in automated decision making which has legal or similar significant effects on the data subject;
- genetic data is processed in the context of systematic monitoring of data subjects;
- genetic data includes matching or combining datasets;
- processing the genetic data of vulnerable data subjects;
- in connection with the innovative use or application of new technical and organisational solutions;
- processing of genetic data to prevent data subjects from using a service or contract.

3. When location data is processed, if at least one any of the following circumstances apply:

- when location data processed reveals sensitive data or data of a highly personal nature;
- location data is processed for evaluation or scoring;
- location data is processed for automated decision making with legal or similar significant implications;
- location data is processed in the context of systematic monitoring;
- location data is processed on a large scale;
- location data includes matching or combining datasets;
- location data of vulnerable data subjects;
- location data is processed in innovative use or applying new technological or organisational solutions;
- processing of location data prevents data subjects from exercising a right or using a service or contract.

4. When personal data is collected from a source other than the individual without providing them with a privacy notice, if at least one of the following circumstances apply:

- when personal data concerns vulnerable data subjects;
- personal data is processed for evaluation or scoring a person;
- personal data is processed for automated decision making with legal or similar significant effects;
- personal data is processed in the context of systematic monitoring;
- personal data is processed on a large scale;
- processing personal data includes matching or combining datasets ;
- personal data of vulnerable data subjects:
- personal data is processed for an innovative use or applying new technological or organisational solutions;
- personal data prevents data subjects from exercising a right or using a service or contract.

5. When personal data is processed in whistle-blowers systems.

No exceptions for the requirement for a DPIA have been specified.

Data breach notification

The general breach notification procedure follows the rules set by GDPR. However, certain special national legislation does include additional requirements on breach notifications. This is the case of the Act on Electronic Communications Services 917/2014.[66]

According to Article 27 of the Data Protection Act, when processing is performed for purposes of personal data solely for journalistic purposes or academic, artistic, and literary expression purposes, notification of a personal data breach to the data subject is not mandatory unless required by the supervisory authority.

Data retention

The Data Protection Act does not specify any precise storage time for personal data. However, national legislation contains various statutory data retention obligations.

Special categories of personal data

Article 6 of the Data Protection Act allows, among other cases, the processing of special categories of personal data for scientific or historical research purposes or for statistical purposes; the processing of research and cultural heritage materials for archiving purposes in the public interest, with the exception of genetic data; and the processing of data that is provided by law or that derives directly from a statutory duty set out for the controller by law. In these cases, the controller and the processor shall take suitable and specific measures to safeguard the rights of the data subject (specified in Article 6(2)).

According to Article 7 of the Data Protection Act, processing of personal data relating to criminal convictions and offenses is allowed if:

[66] Available in English (non-binding official translation) at: https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf.

- necessary to investigate, establish, exercise, defend, or resolve legal claims;
- an insurance institution processes data on an insured person's or claimant's health, illness, or disability during insurance activities;
- the processing is legally required or derives directly from a controller's statutory duty.
- for scientific or historical research or statistical purposes.

3.4.5 Data subject rights

The Data Protection Act foresees that the data subject's right to receive information on the processing and the right to access may be restricted, if the information could cause harm to national safety or defence, public order and safety, or preventing or solving crimes, among other cases.

Article 31 of the Finnish Data Protection Act permits controllers to restrict certain data subject's rights when processing for scientific or historical research or statistical purposes, including access (Article 15 GDPR), rectification (Article 16 GDPR), processing restriction (Article 18 GDPR) and objection (Article 21 GDPR), if:

- the processing is based on an appropriate research plan;
- an assigned person or group is responsible for the research;
- the controller only uses and discloses the personal data for scientific or historical research or another compatible purpose; and
- the controller does not disclose personal data related to a specific individual to third parties.

Controllers processing special categories of personal data or criminal conviction and offense data that restrict data subject rights for scientific or historical research or statistical purposes must either carry out a written DPIA and submit it to the Data Protection Ombudsman before starting the processing or comply with applicable Article 40 of the GDPR (Article 31 Finnish DPA). Data subjects shall be informed of the reasons for the restrictions unless this endangers the purpose of the restriction. If the restriction covers only a part of the data relating to the data subject, they still have a right to access the remaining information concerning them. If the data subject does not have the right to access their personal data, such information shall be provided to the Ombudsman on the data subject's request.

Moreover, Articles 33 and 34 of the Data Protection Act allow restrictions concerning the controller's obligation to provide information to data subjects and the data subject's right of access if this is necessary for national security, defence or public order and security, for preventing or investigating offences, or for a supervisory task relating to taxation or public finances. The controller shall take appropriate measures to protect the data subject's rights. If only a part of the data concerning the data subject is such that it falls within the restriction on the right of access provided above, the data subject will have the right of access to the remainder of the data provided that:

- the data subject must be informed of the reasons for restricting the access, unless it would compromise the purpose of the restriction; and

- if the data subject is not provided with access to information that has been collected from them, information in accordance with Article 15(1) of the GDPR must be provided to the relevant DPA upon the data subject's request.

3.5 Germany[67]

3.5.1 Relevant texts

The main legal instrument implementing the GDPR in Germany is the **Federal Data Protection Act of 30 June 2017** ('the Act'), which entered into force on 25 May 2018.[68] Since Germany is a federal state, there are also regional laws in the 16 Länder.

The Federal Commissioner for Data Protection and Freedom of Information ('BfDI') is the supervisory authority on issues relating to processing at a federal level. The BfDI is the data protection supervisory authority for all public bodies of the federal government, as well as certain social security institutions. It also enforces data protection with regards to all telecommunications and postal service providers. Moreover, there are also regional regulators in each of the Länder. The 16 regional DPAs enforce data protection laws in the public and private sectors of their respective states.

3.5.2 Legal bases

There are no substantial variations from the GDPR.

Section 22 of the Act permits the processing of special categories of personal data by private and public bodies in specific cases. Specific security measures to be taken in these cases are also specified in the section 22 of the Act.

Section 24 of the Act stipulates that private bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected if:

- processing is necessary to prevent threats to state or public security or to prosecute criminal offences; or
- processing is necessary for the establishment, exercise, or defence of civil claims;
- unless the data subject has an overriding interest in not having the data processed.

Section 27 of the Act foresees the regulation of the data processing for purposes of scientific or historical research and for statistical purposes, specifying in which cases it is allowed and with which preventive measures.

Finally, section 28 assesses the data processing for archiving purposes in the public interest.

[67] In this section, we follow Nebel (2023) and DLA Piper Data Protection Laws of the World - Germany, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=DE&c2=.

[68] Available in English at: http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf.

3.5.3 Controller and processor obligations

Chapter 3 of the Law provides for general obligations for controllers and processors, such as the obligation to have a data protection officer and to obtain the corresponding accreditation.

Regarding the processing of special categories of personal data, Section 48 of the Act indicates in which cases it is allowed and which specific safeguards should be provided by the controller:

(1) The processing of special categories of personal data shall be allowed only where strictly necessary for the performance of the controller's tasks.

(2) If special categories of personal data are processed, appropriate safeguards for the legally protected interests of the data subject shall be implemented. Appropriate safeguards may be in particular

1. specific requirements for data security or data protection monitoring;

2. special time limits within which data must be reviewed for relevance and erasure;

3. measures to increase awareness of staff involved in processing operations;

4. restrictions on access to personal data within the controller;

5. separate processing of such data;

6. the pseudonymization of personal data;

7. the encryption of personal data; or

8. specific codes of conduct to ensure lawful processing in case of transfer or processing for other purposes.

Likewise, as far as the processing for archiving, scientific and statistical purposes specific obligations, section 50 of the Act states that "Personal data may be processed in the context of purposes listed in Section 45 in archival, scientific or statistical form if doing so is in the public interest and appropriate safeguards for the legally protected interests of data subjects are implemented. Such safeguards may consist of rendering the personal data anonymous as quickly as possible, taking measures to prevent unauthorized disclosure to third parties, or in processing them organizationally and spatially separate from other tasks".

3.5.4 Data subject rights

The **right to be informed** is primarily governed by Sections 32 and 33 of the Act. A distinction is made as to whether the information was obtained directly from the data subject or indirectly.

The **right of access** is primarily governed by Section 34 of the Act. There are no variations from the provisions of the GDRP, except the following exceptions or grounds for refusing a request:

- Processing for purposes of scientific or historical research and for statistical purposes. The rights of data subjects provided in Article 15 of the GDPR shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes. Further, the right of

access according to Article 15 of the GDPR shall not apply if the data is necessary for purposes of scientific research, and the provision of information would involve disproportionate effort (Section 27(2) of the Act).

- Processing for archiving purposes in the public interest. The right of access according to Article 15 of the GDPR shall not apply if the archival material is not identified with the person's name or no information is given which would enable the archival material to be found with reasonable administrative effort (Section 28(2) of the Act).
- Secrecy obligations. The right of access according to Article 15 of the GDPR shall not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party (Section 29(1) of the Act).
- Other general exceptions. In addition to the exceptions in Sections 27(2), 28(2), and 29(1) of the Act, the data subject's right of access according to Article 15 of the GDPR shall not apply if providing information would require a disproportionate effort, and appropriate technical and organisational measures make processing for other purposes impossible, and if (Section 34 of the Act):
  - the data subject shall not be informed pursuant to the exception grounds under Sections 33(1)(1), 33(1)(2)(b), or 33(3) of the Act, which relate to public bodies;
  - the data was recorded only because it may not be erased due to legal or statutory provisions on retention; or
  - the data only serve the purposes of monitoring data protection or safeguarding data.

Regarding the **right to rectification**, sections 27 and 28 of the Act establish restrictions (see section on grounds for refusing a rectification): Regarding processing for purposes of scientific or historical research and for statistical purposes, the rights of data subjects provided in Article 16 of the GDPR shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes (section 27(2) of the Act); regarding processing for archiving purposes in the public interest, the right of the data subject to rectification according to Article 16 of the GDPR shall not apply if personal data is processed for archiving purposes in the public interest. If the data subject disputes the accuracy of the personal data, they shall have the opportunity to present their version, and the responsible archive shall be obligated to add this version to the files (section 28(3) of the Act).

The **right to erasure** is primarily governed by Section 35 of the Act. There are no national variations, except for the following grounds for refusing a request:

- Non-automated processing, If in the case of non-automated data processing, erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage, and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure, and the controller shall not be obligated to erase personal data. In this case, restriction of processing in accordance with Article 18 of the GDPR shall apply in place of erasure. However, these exceptions shall not apply if the personal data was processed unlawfully (Section 35(1) of the Act).

- Legitimate interests of the data subject. As long and as far as the controller has reason to believe that erasure would adversely affect the legitimate interests of the data subject, the controller shall not be obligated to erase personal data if (Section 35(2) of the Act):
  - the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - the personal data has been unlawfully processed;
  - the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; and
  - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims.

  In this case, restriction of processing in accordance with Article 18 of the GDPR shall apply in place of erasure. The controller shall inform the data subject of the restriction of processing if doing so is not impossible or would not involve a disproportionate effort (Section 35(2) of the Act).

- Statutory or contractual retention requirements. Section 35(1) of the Act shall also apply in case of Article 17(1)(a) of the GDPR (i.e., where the personal data is no longer necessary in relation to the purposes for which it was collected) if erasure would conflict with retention periods set by statute or contract (Section 35(3) of the Act).

There are no national variations regarding the **right to restriction of processing**. However, Sections 27 and 28 of the Act establish restrictions to the right to restrict processing: Regarding processing for purposes of scientific or historical research and for statistical purposes, the rights of data subjects provided in Article 18 of the GDPR shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes (Section 27(2) of the Act); regarding processing for archiving purposes in the public interest, the rights provided in Articles 18(1)(a), 18(b), and 18(d) of the GDPR shall not apply as far as these rights are likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and the exceptions are necessary to fulfil those purposes (Section 28(4) of the Act).

The **right to object** is primarily governed by Section 36 of the Act. There are not national variations, except for the grounds for refusing a request:

- Processing for purposes of scientific or historical research and for statistical purposes. The right to object shall be limited to the extent that it is likely to render impossible or seriously impair the achievement of research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes (Section 27(2) of the Act).
- Processing for archiving purposes in the public interest. The right to object to data processing shall not apply as far as it renders impossible or seriously impairs the achievement of the archiving purposes in the public interest, and the exception is necessary to fulfil those purposes (Section 28(4) of the Act).

There are no national variations with regards to the **right to data portability**. However, there are some grounds for refusing a request in case of processing for archiving purposes in the public interest, since the right to data portability shall not apply as far as these rights are likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and the exception is necessary to fulfil those purposes (Section 28(4) of the Act).

The right not to be subject to automated decision-making is primarily governed by Section 37 of the Act. There are some exceptions to its application for decisions made in the context of providing services pursuant to an insurance contract.

3.5.5 Specific reference to Baden-Württemberg texts, organisms, and relevant information

Germany is composed of 16 Länder that have complementary competences in the privacy sector. Regarding data protection legislation, in addition to the Act, every Land has adopted its own regional data protection law implementing the GDPR, which applies to the public sector and has priority over the Act. Furthermore, each Land has its own regulatory body. Therefore, it is necessary to analyze the legislation and institutions of the Land in which the Consortium partner is located, Baden-Württemberg.

The main legal instrument in Baden-Württemberg is the **State Data Protection Act [of the Land Baden Württemberg] 2018** ('LDSG').[69]

Regarding the regulator, Baden-Württemberg has its own organism, the Baden-Württemberg data protection authority ('**LfDI Baden-Württemberg**') (website accesible here: https://www.baden-wuerttemberg.datenschutz.de/).

The LfDI Baden-Württemberg announced, on 18 November 2022, its approval of the national code of conduct, titled 'Requirements for processors under Article 28 of the GDPR - Trusted Data Processor.' The code of conduct covers requirements, among other things, on:

- contracting sub-processors;
- data subject rights;
- the reporting of data breaches; and
- confidentiality obligations.

Companies can voluntarily commit to the code of conduct under the supervision of a monitoring body, which oversees their compliance with the code of conduct and serves as the point of contact for complaints. The Accreditation Society Data Protection ('DSZ') is the new monitoring body for processing applications to become Trusted Data Processors and monitor complaints.

[69] Available in German at: https://www.landesrecht-bw.de/jportal/portal/t/9j7/page/bsbawueprod.psml/action/portlets.jw.MainAction?p1=0&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-DSGBW2018rahmen&doc.part=R&toc.poskey=#focuspoint.

In the event of data breach, the owner or authorized representative of a data processing facility must report it to the Baden-Württemberg authorities at the following link: https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/

3.6 Italy[70]

3.6.1 Relevant texts

Italy has implemented the GDPR by amending the Italian **Personal Data Protection Code** (Legislative Decree no. 196/2003, setting out the Italian Data Protection Code) through Legislative Decree no. 101 of 10 August 2018 (Decree 101), that entered into force on 19 September 2018.

The Italian DPA is the 'Garante', which, among other things, manages data subjects' complaints, provides specific data protection measures for data controllers and processors, and adopts guidelines to assist organisations' compliance with personal data protection laws. Moreover, the Garante has the power to adopt general authorizations (see below) and ethical rules and approve codes of conduct, which set forth further specifications on conditions of lawfulness on certain processing activities, such as the processing for statistical and scientific research purposes.[71]

3.6.2 Legal bases

In general, no variations from the GDPR are provided by Italian data protection laws, except with regard to legal obligations and public interest.

- Legal obligation. Section 2(b)(1) of the Code provides that processing based on 'legal obligations' pursuant to Article 6(3)(b) of the GDPR shall only be permitted when required either by a law or a regulation or an administrative instrument of a general nature.
- Public interest. Section 2(b)(3) of the Code provides that personal data may be disseminated or communicated between controllers for the performance of a task carried out in the public interest or in the exercise of official authority only if either the dissemination or communication is provided by a law or a regulation or an administrative instrument of a general nature or the communication is necessary to carry out tasks in the public interest or to fulfil institutional duties and the Garante has been informed at least ten days prior to commencement of the said communication or dissemination. Furthermore, according to Section 2(b)(1)(a) of the Code, public administrations, independent authorities, as well as state-owned companies or companies managing public services owned by local authorities, are always allowed to process personal data if necessary for the performance of a task carried out in the public interest or for the exercise of official authority conferred to the same. Where the purpose of the processing is provided neither by a law nor a regulation or an administrative instrument of a general

[70] In this section we follow Olivi (2023) and and DLA Piper Data Protection Laws of the World - Italy, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=IT&c2=.

[71] Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101, 19 dicembre 2018, available only in Italian at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637.

nature, the purpose of the processing is indicated by the same entity in line with the task performed or the authority exercised.

- General authorisations issued by the Garante, which set forth the conditions for certain processing activities by indicating the permitted purposes and modalities of the processing. The general authorisations currently effective are those regarding, among others, the processing of judicial data by individuals, economic entities, and public bodies (former general authorisation no. 7/2016); the processing of genetic data (former general authorisation no. 8/2016); and the processing of personal data for scientific research purposes (former general authorisation no. 9/2016).[72]

3.6.3 Principles

All principles of Article 5 of the GDPR are applied as such in Italy.

3.6.4 Controller and processor obligations

Data processing notification

According to Section 110(a) of the Code, the Garante may authorise processing of personal data (including sensitive personal data) by third parties for scientific research or statistical purposes, when informing the data subjects may prove impossible, require disproportionate efforts, or endanger the research purposes, subject to appropriate safeguards (e.g., minimization and anonymization).

Furthermore, data controllers are required to notify the Garante before the commencement of the processing based on a legitimate interest and involving the use of new technologies or automated tools, where processing personal data which is functional to authorising a change of name or surname of minors (Article 22(5) of Decree 101). With reference to such processing, the Garante may, within the limits and in the manner set forth in Article 36 of the GDPR, adopt general measures pursuant to Article 2(quinquiesdecies) of Decree 101, concerning processing activities that present high risks for the performance of a task of public interest. Following such notification, the Garante will assess the processing and, should it establish that there is a risk to the rights and freedoms of the data subjects, it may request further information and integrations, and where it deems that the processing would have a negative impact, it may forbid the same (Article 1(1023) of the Budget Law).

DPIA

Pursuant to Article 35 of the GDPR, the Garante issued Resolution no. 467 on 11 October 2018 providing for a non-exhaustive list of processing operations subject to a DPIA.[73] It is the same list contained in the Guidelines on DPIA (wp248rev.01).

Data breach notification

[72] They are indexed only in Italian here: https://www.garanteprivacy.it/home/provvedimenti-normativa/provvedimenti/autorizzazioni.

[73] 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 Code does not set out additional rules on data breach notifications. Data breaches that require notification should be notified to the Garante by completing a form available at the Garante website. The notification form, once completed with the required information, must be sent via certified e-mail to the Garante and must be signed digitally (with qualified electronic signature/digital signature) or with handwritten signature.

Data retention

Section 99 of the Code provides that processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be carried out also for longer than is necessary for achieving the purposes for which the data had been previously collected or processed.

Special categories of data

Criminal data may only be processed (Article 2(octies) of the Code):

- under the control of a public authority; or
- where authorised by a specific legal provision, providing appropriate security measures. No such provision has yet been adopted in Italy.

3.6.5 Data subject rights

Some substantial variations from the GDPR are provided by Italian data protection laws with regard to data subjects' rights. Pursuant to Article 2(undecies) of the Code, data subjects' rights may be exercised within the limits established in the law and regulations on the proceeding and procedures before the courts. The exercise of such rights may be delayed, limited or excluded for as long as and to the extent that it is a necessary and proportionate measure, having regard to the fundamental rights and legitimate interests of the data subject. Finally, the Code sets out data protection rights of deceased persons. Indeed, the rights provided for in Articles 15 through 22 of the GDPR referring to personal data concerning deceased persons may be exercised by those having an interest of their own, or act to protect the data subject, as her/his delegate, or for family reasons worthy of protection. The exercise of such rights is not permitted when provided for by the law or when, specifically limited to the offer of information society services, the data subject expressly prohibited it in writing by way of a declaration sent to the data controller. The data subject may withdraw or modify such declaration at any time.

3.7 Romania[74]

3.7.1 Relevant texts

Legal rules regarding data protection in Romania are mainly set in **Law No. 190/2018 Implementing the General Data Protection Regulation (Regulation (EU) 2016/679)** ('Law 190/2018'), which in principle reiterates the GDPR rules. In 2019, the Law was subject to a 'corrigendum'. Specifically, processing for statistical purposes was included amongst the cases benefiting of the exemption regulated by Article 89(2) of the GDPR. The processing

[74] We follow here Cretu and Timofte (2022), Lazar and Costescu (2018) and DLA Piper Data Protection Laws of the World - Romania, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=RO&c2=.

of traffic data, location data and the implementation of cookies is regulated under Law no. 506/2004, on the processing of personal data and the protection of privacy in the electronic communications sector.

Specific decisions issued by the National Supervisory Authority for Personal Data Processing ('ANSPDCP') regulate main areas of the GDPR such as when a DPIA will be mandatory, the accreditation of certification bodies, the conduct of investigations and management of complaints, and the notification security breaches. In general, these guidelines are quite generic, most of them only reiterating the main GDPR principles and standards. They are only available in Romanian:

- Decision No. 20/2021 on the approval of the additional requirements for the accreditation of certification bodies pursuant to Article 43 of the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Regulation (EU) 2016/679);
- Decision No. 238/2019 on the amendment of Annex no. 2 to the procedure for conducting investigations, approved by the Decision of the President of the National Authority for the Supervision of Personal Data Processing No. 161/2018;
- Decision No. 174/2018 on the list of kinds of processing operations which are subject to the requirement for a DPIA;
- Decision No. 161/2018 on the approval of the procedure for conducting investigations;
- Decision no. 133/2018 on the approval of the procedure for receiving and resolving complaints;
- Decision No. 128/2018 on the approval of the standard form for the notification of personal data breach in accordance with GDPR;
- Decision No. 99/2018 regarding the cessation of the applicability of some normative acts with administrative character issued in the application of Law No. 677/2001 for the protection of individuals with regard to the processing of personal data and the free movement of such data; and
- Decision No. 184/2014 on the approval of the standard form of notification of personal data breach for providers of public network services or electronic communications services, in accordance with the European Commission Regulation on measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on confidentiality and electronic communications (Regulation (EU) No. 611/2013).

3.7.2 Legal bases

Regarding legal bases of data processing, Law 190/2018 provides for express consent as legal basis for processing of biometric data and health data. Consent is also provided as a valid legal basis for processing national identification numbers. There are no national variations regarding contracts. The GDPR definition applies. The GDPR definition also applies to interests of the data subject, with no national variations.

Law 190/2018 provides for the possibility to process special categories of data in the context of performance of a task carried out in the public interest. Such processing requires special guarantees: the implementation of technical and organisational measures to ensure the integrity and confidentiality of data in line with Article 5 of the GDPR, the appointment of a DPO, and the implementation of retention periods according to the nature of

the data and the purpose of processing (Article 6 of Law 190/2018). There are no national variations regarding legitimate interests of the data controller. The GDPR definition applies.

The processing of the national identification number for the purposes of the legitimate interests pursued by the controller or by a third party can only be carried out if the controller has implemented the following safeguards (Article 4 of Law 190/2018):

- the implementation of appropriate technical and organisational measures to respect the principle of data minimisation, as well as to ensure the security and confidentiality of personal data processing in accordance with Article 32 of the GDPR;
- the designation of a DPO;
- the setting of retention periods in accordance with the nature of the data and the purpose of the processing, as well as specific terms for data erasure or revision for deletion; and
- the regular training of the personnel with duties related to the processing of such personal data by both the controller and processor.

The processing of traffic data and location data is regulated under Law no. 506/2004, on the processing of personal data and the protection of privacy in the electronic communications sector. Traffic data relating to subscribers and users processed and stored by the provider of a public electronic communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, but no later than three years from the date of such a communication. However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value-added services, solely throughout the marketing period and provided that data subjects have previously consented to the processing of traffic data. Data subjects may withdraw such consent at any time. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data, and the duration of processing, prior to obtaining their consent. The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is permitted solely for a period of three years following the due date of the respective payment obligation. The provider of publicly available electronic communication services must inform data subjects in respect of the processed categories of traffic data and the duration of processing. The processing of traffic data for the establishment of contractual obligations of the communication services subscribers, with payment in advance, is permitted solely for a period of three years following the date of the communication. The processing of traffic data as mentioned above may be done only by persons acting under the authority of providers of public electronic communications networks or of publicly available electronic communications services for: Management of billing and traffic; dealing with enquiries of data subjects; prevention of fraud, or the provision of communication services or value-added services, and it is permitted only if it is necessary to fulfil such purpose.

The processing of location data, other than traffic data is permitted when:

- Data is rendered anonymous;
- Data subjects have explicitly and consented prior to such processing for the duration necessary for the performance of value-added services, or

- The purpose of the value-added service is the unidirectional and nondifferentiated transmission of information towards users.

The provider of publicly available electronic communications services must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value-added service. Users or subscribers shall be given the possibility to withdraw their consent at any time. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the provider of publicly available electronic communications services must grant users the possibility, using a simple and free of charge means, of withdrawing consent or of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3.7.3 Principles

Law 190/2018 provides for derogations from the principles entailed in the GDPR. Hence, according to Article 7 of Law 190/2018, in order to ensure the freedom of expression and the right for information, processing of data may be carried out for journalistic purposes or for the purpose of academic, artistic, or literary expression, being exempted from data privacy principles, if such data:

- have been manifestly made public by the data subject;
- are closely linked to the data subject's status as a public person; or
- are closely linked to the public nature of the facts the data subject is part of.

As per Article 8(1) of Law 190/2018, the processing of personal data for scientific or historical research purposes may be carried out without the observance of the provisions of Articles 15, 16, 18, and 21 of the GDPR, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific goals, and the respective derogations are necessary for the achievement of these purposes.

According to Article 8(2) of Law 190/2018, the processing of personal data for archiving purposes in the public interest may be carried out without the observance of the provisions of Articles 15, 16, 18, 19, 20, and 21 of the GDPR, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the achievement of these purposes. In any case, these specific derogations stemming from Article 8 of Law 190/2018 are subject to the conditions and safeguards referred to in Article 89(1) of the GDPR.

Furthermore, where the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes serves at the same time another purpose, the exemptions shall apply only to processing for the purposes referred to in Article 8(1) and (2) of Law 190/2018.

3.7.4 Controller and processor obligations

The main obligations and processing requirements are aligned with the GDPR.

DPIA

Pursuant to Decision No. 174/2018 ('the Blacklist'), the ANSPDCP established that the following activities shall result in a high risk to the rights and freedoms of natural persons and, therefore, for them a DPIA is required:

- processing of personal data carried out for a systematic and extensive evaluation of personal aspects relating to natural persons, that is based on automated processing, including profiling, and based on which decisions that produce legal effects concerning the natural person or, similarly, significantly affect the natural person, are taken;
- processing on a large scale of personal data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, as well as biometric data for the purpose of uniquely identifying a natural person, data concerning health, or a natural person's sex life or sexual orientation, and personal data relating to criminal convictions as well as offences;
- processing carried out for systematic monitoring of a publicly accessible area on a large scale, such as video surveillance in shopping centres, stadiums, markets, parks, and other similar spaces;
- processing on a large scale of personal data pertaining to vulnerable natural persons, especially to minors or employees, via means of automated monitoring and/or systematic recording of their behaviour, including carrying out activities involving commercials, marketing, and advertising;
- processing on a large scale of personal data by use of innovative, or by the implementation of, new technology, particularly when such activities limit the ability of data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;
- processing on a large scale of personal data generated by devices with sensors which send data over the internet or by other means (Internet of Things ('IoT') applications such as Smart TVs, connected vehicles, smart meters, smart toys, smart cities, or other similar applications); and
- processing on a large scale and/or systematic processing of traffic data and/or geolocation data of the data subjects (such as Wi-Fi monitoring, geolocating passengers in public transportation, or other similar cases) when the processing is not necessary for the performance of the services requested by the data subject.

In addition, the Blacklist provides that a DPIA is not mandatory where the processing pursuant to Article 6(1)(c) and (e) of the GDPR has a legal basis in Union law or in the law of the Member State and DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis.

Special categories of data

Law 190/2018 provides additional requirements in respect of: electronic monitoring of employees in the workplace; processing for legitimate interest of the newly defined concept 'national identification number' (e.g., personal code number, ID series and number, passport number etc.); and processing of genetic data, biometric data, data concerning health for automated decision-making and profiling.

3.7.5 Data subject rights

No variations from the GDPR are provided by Romanian data protection laws.

3.8 Switzerland[75]

Since it is not an EU member state, the case of Switzerland requires a deeper explanation. Swiss data protection laws are not based on the GDPR and differ from it in numerous ways. However, Switzerland places a high priority on compliance with the GDPR for a variety of reasons, which explains recent law modifications in this sense.

3.8.1 Relevant texts

The right to privacy in personal or family life and at one person's home is protected by Article 13 of the Federal Constitution of the Swiss Confederation ('SFC' or 'the Swiss Constitution'). Article 28 of the Swiss Civil Code and the Federal Act of 19 June 1992 on Data Protection ('FADP') materialise this fundamental right to privacy at the statutory level. The revised FADP will enter into force on September 1, 2023. It applies the standards of the Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ('Convention 108+').[76] Moreover, the Revised FDAP adapts the Swiss regulation to the requirements of the GDPR, in order to maintain the EC's adequacy finding,[77] and with the LED, as Switzerland must implement it, in accordance with the Schengen Association Agreement with the EU.[78] Finally, Ordinance of 14 June 1993 to the Federal Act on Data Protection ('FODP') provides more specific provisions on some aspects of the FADP.

Other specific criteria for data processing are set out in the sectoral regulations on data privacy and security, contained in legislation governing corporations and organizations in various fields (such as the health, pharmaceutical, energy, telecommunications and financial sectors). The requirements of the FADP are often replaced by sector-specific provisions.

Each of the 26 cantons have enacted their own data protection laws, regulating the processing of personal data by public authorities both at cantonal and communal level.

Among the main soft-law (non-binding) guidelines published by the Federal Data Protection and Information Commissioner ('FDPIC', the Swiss DPA) we can highlight the following:

- Guidelines on data subjects' rights in relation to the processing of personal data;

[75] This section is based on Steiner (2022), Staiger (2018) and DLA Piper Data Protection Laws of the World – Switzerland, available at: https://www.dlapiperdataprotection.com/index.html?t=law&c=CH&c2=.

[76] Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[77] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C (2000) 2304) (Text with EEA relevance), OJ L 215, 25.8.2000, p. 1–3. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518.

[78] Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application, and development of the Schengen acquis - Final Act - Joint Declarations - Declarations - Agreement in the form of an exchange of letters, OJ L 53, 27.2.2008, p. 52–79. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22008A0227%2803%29.

- Guidelines on the processing of personal data in the private sector;[79]
- Guidelines for technical and organizational security measures;[80]
- Guidelines on international data transfers;
- Guidelines to determining whether direct or indirect data transfers to third countries are permissible (Art. 6 para. 2 letter a FADP).[81]

3.8.2 Legal bases

In contrast to the GDPR's requirement of 'lawfulness of processing', the FADP permits the processing of personal data by companies, organizations, and individuals. A legal ground is required for the processing carried out by public authorities, but the FADP allows private controllers to legitimately process personal data without a legal justification. Thus, legal grounds, or more properly 'justifications,' are important when they serve as an explanation for a violation of a person's right to privacy, without which it would be unlawful. In accordance with Article 30.2 of the revised FADP, this concept will remain unchanged.

A general requirement of consent for the processing of personal data does not exist. Both the FADP and the Revised FADP simply set the requirements for a valid consent that must be met if a controller needs to justify the processing and seeks consent as a basis for the processing instead of other bases, such as the performance of a contract or legitimate interests. Only informed and freely given consent is valid. Consent must be expressly given with a clear affirmative action to justify the disclosure of sensitive personal data or so-called 'personality profiles' of the controller to third parties (other controllers, not processors) or if it is intended to justify an infringement of personality rights (e.g., processing for other purposes or for longer than necessary) in relation to sensitive personal data. According to Article 6(6) of the Revised FADP, if a data controller needs to justify processing and intends to use consent to do so, it will be valid if it is informed, freely given and specific to one or more processing activities. However, according to Article 6(7) of the Revised FADP, consent must be requested explicitly when a controller needs to defend processing of sensitive personal data or high-risk profiling. In this sense, there is not a specific procedure or requirements to obtain the 'high-risk profiling', defined as profiling that poses a high risk to the privacy of individuals by combining data that enable an assessment of critical components of a natural person's personality.

According to Articles 13(1) of the FADP and 31(1) of the Revised FADP, the controller's interests may justify the processing if they override the data subject's right to privacy. In this sense, an interest that may take precedence

[79] Only available in German, French and Italian (official versions). See Guida per il trattamento di dati personali nel settore privato, August 2009 at: https://www.edoeb.admin.ch/edoeb/it/home/documentazione/basi-legali/guide/trattamento-di-dati-personali-nel-settore-privato.html.

[80] See A Guide for technical and organizational measures, August 2015, available in English (official version) at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/dokumentation/guides/technical-and-organizational-measures.html.

[81] See Guide for checking the admissibility of data transfers with reference to foreign countries (Art. 6 para. 2 letter a FADP), June 2021, available in English (official version) at: https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html.

over a data subject's privacy interests is one that is necessary for the conclusion or fulfilment of a contract with the data subject (Articles 13(2)(a) of the FADP and 31(2)(a) of the Revised FADP). Another justification for processing may be the need for the controller to fulfil its legal obligations (Articles 13(1) of the FADP and 31(1) of the Revised FADP). Only legal obligations under Swiss law are considered.

According to Articles 13(1) of the FADP and 31(1) of the Revised FADP, the data subject's interests may be considered 'private interests' and thus allow for the justification of a violation of personality rights that would otherwise be illegal. However, processing that is necessary for the data subject is less likely to qualify as an initial violation of their privacy rights.

Overriding public interests may justify an otherwise unlawful personality rights infringement, particularly if invoked by public authorities (Articles 13(1) of the FADP and 31(1) of the Revised FADP). However, Swiss courts are unwilling to accept the public interest as a ground for justification.

According to Articles 13(1) of the FADP and 31(1) of the Revised FADP, the controller's "private interests"—which may need to be justified—are those that override the data subject's privacy interests. The following are just a few examples of the data controller's legitimate interests, which are detailed in Articles 13(2) of the FADP and 31(2) of the Revised FADP, respectively:

- processing with the objective of conclude or perform a contract with the data subject;
- processing with the aim of competing economically with another organisation, on the condition on not sharing the personal data with third parties (in this context, intragroup transfers are not considered transfers to third parties); and
- processing to verify the creditworthiness of a data subject (with restrictions).

3.8.3 Principles

The following processing principles are key principles and responsibilities of controllers under the FADP:

- Lawfulness: Controllers (businesses or organizations) are only permitted to process personal data that has been legally obtained. Contrary to the 'lawfulness of processing' principle that grounds the GDPR, corporations, organizations and natural persons are allowed po process personal data under the FADP. Legal justification for processing is only necessary for public authorities.
- Fairness (good faith): Controllers are only permitted to carry out processing in ways that data subjects may reasonably anticipate. Fairness also dictates that processing be carried out in accordance with privacy notices.
- Transparency: Controllers must agree with data subjects on all information necessary to ensure transparent data processing, ensuring that interested parties can exercise their rights in under the FADP. The types of information that controllers must convey with data subjects will be more specifically outlined in the Revised FADP. Controllers will have to inform data subjects at least about: the identity and contact information of the controller; the contact information of the DPO (if applicable); the contact information of the Swiss representative (if applicable); the purposes of the processing; the recipients or its categories (if applicable); the concerned categories of

personal data, if it is not obtained directly from the data subject; and, whenever the controller plans to send personal data to a recipient outside of Switzerland, the controller must specify the recipients' countries, the safeguards (such as Standard Contractual Clauses, or "SCCs"), or derogations that will be used, and (if applicable) whether automated individual decision-making will be used.

- Purpose limitation: Data processing by controllers may only be carried out for the specified purposes that have been notified to or are known to the data subjects. The processing may only be carried out in a way that is compatible with those purposes. Specificity is required when describing the processing's purposes. Controllers should also ensure that the further processing of personal data received from other controllers complies with the purposes identified and communicated to the data subjects when collected.
- Proportionality: The processing of personal data must be proportionate—that is, it must be limited to what is needed to achieve the stated purposes, considering the type of personal data involved, as well as the extent and length of the processing.
- Two important aspects of the proportionality principle are the data minimization and storage limitation. This means that controllers must only collect and process the minimum amount of personal data necessary to achieve the purposes, and they must delete personal data when it is no longer necessary for those purposes.
- Accuracy: Controllers should ensure that the process is made only with accurate and up to date personal data. They should take all reasonable measures to delete or rectify inaccurate or incomplete data, taking into account the purposes of the processing.
- Data security: It is the responsibility of controllers and (under the Revised FADP) processors to provide an acceptable level of data security. They must take sufficient technical and organizational security measures to safeguard the accuracy, privacy, and accessibility of personal data. Controllers and processors are required to take into consideration the purpose, nature, and extent of the data processing, the evaluation of any potential dangers to data subjects, and the most recent security technologies when determining the acceptable level of security.

If the processing of personal data by companies and organizations complies with the requirements described above, the processing shall be considered lawful if the data subject has not expressly objected to the processing. Personality rights of the affected data subject are violated when these processing principles are infringed, such as when processing is carried out in violation of the data subject's objection or when it is made for longer than is necessary to achieve the specified purposes. Likewise, it is considered a violation of personality rights to disclosure of sensitive personal information or (under the current FADP only) personality profiles to other parties without a legitimate justification. Unless the controller can prove that the relevant data processing is justified by overriding private or public interests, or by the necessity of its compliance with legal duties set forth by Swiss law, breaches of personality rights are regarded unlawful.

3.8.4 Controller and processor obligations

Data processing notification

There is no need to register or notify the FDPIC to process personal data in Switzerland or to carry out data processing operations with implications in Switzerland. However, according to the present FADP, organizations or corporations who regularly process sensitive personal data, personality profiles, or regularly disclose personal data to third parties are required to register their data files with the FDPIC. According to Article 3(1) of the Ordinance, before being used operationally, data files must be registered with the FDPIC. According to Article 3(2) of the Ordinance, controllers are required to regularly update the data listed in the registration of the data files.

Article 11(a)(5) of the FADP states that, in cases of processing of personal data by private persons, the controller is not obliged to declare its files if:

- the data are processed to comply with a legal obligation;
- the Federal Council has exempted the processing from the obligation to register because it does not prejudice the rights of the data subjects;
- the data controller uses the data only for publication in the edited section of a periodically published medium and does not transmit any data to third parties without informing the data subjects;
- the data is processed by journalists using the data file as a personal job aid;
- the data controller appointed a DPO who externally verifies that internal procedures are following data protection laws and keeps a record of the data files; or
- the data controller has acquired a data protection the quality mark under a certification procedure foreseen in article 11 of the FADP and has notified the result of the evaluation to the FDPIC.

Pursuant to Article 4 of the Ordinance, the data controller is exempt from the obligation to register its files with the FDPIC if:

- the information files are from suppliers or clients, provided that no sensitive personal information or personality profiles are present;
- The data files include information that is only utilized for general, non-person-specific reasons, particularly in research, planning, and statistics;
- the data is retained only for historical or scientific purposes, and the files are archived data files;
- the data files only include information that has been made publicly available or that the data subjects themselves have made broadly accessible without specifically forbidding their processing;
- the data serve only to meet the requirements of maintenance of a register of automated processing of sensitive personal data or profiling (article 10 of the Ordinance);
- the data files are accounting records; or
- the files are secondary data files for the data controller's personnel management, as long as they do not contain sensitive personal data or personality profiles.

Under the Revised FADP, there is no requirement to register data files.

Data transfers

Under the current FADP, the FDPIC presents a list of states with an appropriate level of data security, under the standards of FDPIC. According to the Revised FADP, the Federal Council will decide if a jurisdiction offers an acceptable level of protection. The Federal Council will follow the European Commission's example and deem appropriate those jurisdictions regarding which the EC has issued an adequacy determination.

Transferring personal data to nations lacking an adequate degree of protection needs necessary safeguards or derogations for particular circumstances. In accordance with the Revised FADP, appropriate safeguards include SCCs that are issued, approved, or recognized by the FDPIC, Binding Corporate Rules (or "BCRs") that have been approved by the FDPIC or a competent data protection supervisory authority in a state that offers an adequate level of protection, or (upon prior notification to the FDPIC) contractual provisions incorporated into a controller-to-processor data processing agreement. The new SCC issued by the European Commission in June 2021 has been recognized by the FDPIC as a valid safeguard for transfers from Switzerland to nations lacking a sufficient level of protection, given that the parties augment the SCC with an annex that incorporates protections particular to Swiss law.

In addition, FDPIC expects a Transfer Impact Assessment ('TIA') to be conducted in relation to the use of SCC. Additionally, the Revised FADP stipulates exceptions for data transfers in certain circumstances, such as when the transfer is directly connected to the signing or carrying out of a contract between the controller and the data subject.

The aforementioned data transfer standards are also applicable in outsourcing situations, such as when a controller in Switzerland hires a processor in another country or a processor in Switzerland hires a sub-processor in a different country. A data processing agreement is also required to regulate relationships between controllers and processors as well as between processors and sub-processors.

Data processing records

Controllers (and processors) will be obliged by the Revised FADP to keep records of processing activity. Exemptions apply to low-risk processing of personal data carried out by companies with less than 250 workers. The specifics of this and other exemptions that might be applicable are outlined in the revised FODP.

DPIA

Controllers will be required to conduct DPIAs for planned high-risk processing of personal data under the Revised FADP. The nature, scope, conditions, or aims of the processing, as well as the employment of new technologies, could all contribute to the elevated risk. Under the Revised FADP, a DPIA will be necessary, particularly in cases of extensive processing of sensitive personal data or extensive systematic monitoring of publicly accessible locations. Prior to the adoption of profiling, a privacy risk assessment and, maybe, a DPIA will be necessary.

According to the Revised FADP's Article 22(3), the DPIA must include a description of the intended processing, an evaluation of the risks to data subjects' identities or fundamental rights, as well as the steps intended to safeguard those rights.

As regards exemptions, the revised FADP provides for an exemption for controllers who carry out a processing activity in accordance with a legal obligation under Article 22(4). Furthermore, an exemption is also provided for controllers who use a system, product or service certified in accordance with Article 13 of the revised FADP, or if it complies with a code of conduct within the meaning of Article 11 of the revised FADP.

In accordance with the article 23 of the Revised FADP, a controller is required to contact the FDPIC when the DPIA reveals that the processing poses a significant danger to the data subject's personality rights or fundamental rights, despite the measures foreseen by the data controller. However, article 23(4) of the Revised FADP foresees an exception to this obligation of consultation when the controller has consulted its designated data protection advisor.

Appointment of a DPO

Companies and organizations participating in the FADP or the Revised FADP are not required to appoint a DPO. Nevertheless, the Revised FADP encourages the appointment of a DPO or "data protection advisor." Voluntary appointment of a DPO is strongly recommended, as complying with documentation and reporting obligations and responding to data subject requests under the revised PADE requires companies to establish, in practice, an internal data protection function.

Representative

Private controllers (businesses or organizations) not located in Switzerland are required by the Revised FADP to designate a representative in Switzerland in some cases. If they often process personal data in a high-risk, large-scale manner in connection with the provision of products or services in Switzerland, or in conjunction with the observation of persons' behaviour in Switzerland, they will be forced to comply.

Data breach notification

Although notification is the best practice, the current FADP does not specify any obligations for data breach notification. However, under the Revised FADP, controllers will be required to notify the FDPIC of personal data breaches that pose a significant danger to data subjects. There is no specified time limit for the notification. The FDPIC must be notified by controllers as soon as possible, without unnecessary delay. The type of personal data breach, its effects, and the steps taken or planned to remediate the breach and reduce risks for data subjects must all be covered in the notification.

Additionally, the revised FADP contains a formal requirement to notify the data subject when doing so is necessary to protect the data subject's interests or when the FDPIC requests it.

Data retention

Once controllers no longer require personal data for the specified purposes, or in order to pursue legitimate interests (like the enforcement of legal claims or archival purposes), or to meet legal requirements (like record-keeping requirements), controllers must delete or sufficiently de-identify (i.e., render anonymous) personal data.

Special categories of personal data

Special categories of personal data, also known as "sensitive data," may only be disclosed with justification, such as the subject's consent, the controller's overriding interests, or the need to comply with legal obligations. It is not acceptable to disclose sensitive personal data when you hire processors to carry out certain processing tasks.

Additionally, there are stricter requirements for data security and transparency in relation to the processing of special categories of personal data, and a DPIA will probably be necessary if this is the case with the proposed processing activity.

Controller and processor contracts

The relationship between the controller and the processor must be governed by a contract (or by law). The controller must guarantee that the processor can adequately secure the data and that the processor only carries out processing operations that the controller would likewise be permitted to carry out. Additionally, the Revised FADP stipulates that a processor may only employ a sub-processor with the controller's prior approval. For the purposes of the Revised FADP, the criterion outlined in Article 28(3) of the GDPR will often be adequate. Therefore, parties should make it clear that for the purposes of the data processing agreement, Switzerland is a member of the EEA.

Controllers will remain primarily responsible for compliance with the revised FADP. However, in contrast to the current FADP, the revised FADP will also outline legal requirements that directly apply to processors, such as obligations regarding data security, limitations on using sub-processors, and the need to keep a record of processing activities.

Under the FADP and the Revised FADP, the disclosure of personal data by controllers to processors (or rather, entrusting processors with the controller's data processing activities) is "privileged" in that it does not qualify as a disclosure to third parties in the sense of Articles 12(2)(c) FADP and 30(2)(c) Revised FADP. They don't need to be justified as a result.

3.8.5 Data subject rights

The FADP requires that the collection and the processing purposes must be clear to the data subject. In consequence, data subjects have a right to be informed about the collection of their personal data and the reasons for processing it (Articles 4(2) and (4) of the FADP) if it is not obvious because of the circumstances. This transparency principle is derived under the Revised FADP from the "fairness" principle stated in Article 6(2) of the Revised FADP. Privacy notices then become required. However, in some cases, the controller will also be required to actively notify data subjects about the collection and processing of personal information that may appear clear to them and would not call for active information under the current FADP. A list of essential details that controllers must provide to data subjects at the time of the collecting of personal data is found in Article 19 of the updated FADP. Articles 10(3)(d) (obligation to publish the DPO's contact information), 14(3) (obligation to publish the Swiss representative's contact information), and 21(1) (obligation to inform about automated individual decision-making) of the Revised FADP contain additional obligations to actively inform data subjects.

Data subjects have the right to access their own personal information that is being processed under Article 8 of the FADP, including the right to obtain a copy of the personal data being processed. Data subjects have the option to request information about the sources of the personal data, the objectives of processing, the

categories of personal data being processed, and the categories of recipients of the personal data when making an access request.

A written statement from the controller is required, together with a copy of the personal data, such as a printout or an excerpt from the pertinent data base. There is a 30-day limit, but controllers can also let the data subject know that acquiring the necessary information and data would take longer, or they can deliver the information and data gradually. According to Article 9 of the FADP, controllers can refuse, limit, or postpone the provision of information and data if doing so is necessary to uphold a legal obligation established by Swiss law, to safeguard the overriding interests of third parties, or (so long as the controller does not disclose the personal data to third-party recipients). This provision results in a relatively weak protection of the controller's business secrets. The Revised FADP (Articles 25–27) mostly preserves this idea, with the exception that it will include a list of the minimal pieces of information that a controller must supply in response to access requests (Article 25(2) of the Revised FADP), namely:

- the controller's identity and contact information;
- the personal data undergoing processing, including a right to receive a copy of the personal data;
- the processing's purposes;
- the length of storage or, if not possible, the factors considered in determining this duration;
- the information available on the source of the personal data (where the controller did not get the data directly from the subject);
- the existence of individual automated decision-making, when applicable; and
- the recipients or categories of recipients of the personal data, when applicable.

The grounds for refusal, restricting, or delaying the information and data essentially remain the same. Professional secrecy responsibilities are defined as a legal obligation that may support a denial, restriction, or deferral in Article 26(1)(a) of the Revised FADP. Furthermore, the Revised FADP's underlines that a controller has the right to deny information and access to personal data if the request is clearly frivolous, not based on legitimate grounds, or both, in Article 26(1)(c).

It is the right of data subjects to request that inaccurate information that a controller may have about them be rectified. On the grounds of statutory requirements or predominating private or public interests, the controller may reject the correction. The Revised FADP will still include the right to rectification, but it will restrict the grounds for rejecting it. According to Article 32(1) of the Revised FADP, controllers may only refuse to correct inaccurate personal data if a legal need forbids the correction or if the processing of the personal data is being done for purposes in the public interest.

The right to object to the processing of one's personal data is granted to data subjects under articles 12(2)(b) of the FADP and 31(2)(b) of the Revised FADP, essentially configured as an opt-out right. However, the right to protest or opt out is not absolute, since controller may refuse to restrict processing of personal data or refuse to delete personal data if and to the extent that it is required for the controller to comply with legal obligations, perform a contract, or further legitimate public or public interests.

A right to data portability is not currently included in the FADP. However, courts have ruled that having a copy of the personal data being processed falls under the scope of the right to access. A right to data portability is introduced in Article 28 of the Revised FADP, which stipulates a right to request a transfer of personal data to another controller or a copy of the data subject's personal information in a frequently used format under the following conditions:

- The controller performs automatic data processing; and
- The processing of the data is done with the consent of the data subject or directly related to the signing or carrying out of a contract with the subject.

The limitations to the right to access also apply, as stated in Article 29 of the updated FADP in connection with Articles 26(1) and (2), as exceptions to the right to data portability. If doing so would require a disproportionate effort, a controller may also decline to grant the right to transfer personal data to another controller.

Currently, there is no entitlement to be exempt from automated decision-making in the FADP. In accordance with Article 21 of the Revised FADP, data controllers must notify data subjects if they employ automated individual decision-making. Additionally, it stipulates that in the event of automated individual decision-making, data subjects have the right to be heard. If the decision is made in connection with the signing or carrying out of a contract with the data subject, and the controller accedes to the request made by the data subject, or if the data subject has given their agreement to the automated individual decision-making, then these rights do not apply.

The Revised FADP recognizes data subjects all the rights provided under GDPR and more, as it also provides remedies for personality rights violations under the Civil Code (see Article 32(2) of the Revised FADP).

According to Swiss courts, the right to object under Article 12(2)(b) of the FADP also includes the right to restrict processing and the right to have personal data deleted. These rights are also included in the Revised FADP's Article 31(2)(b). The erasure or destruction of personal data and the prohibition of processing are now specifically mentioned in the Revised FADP as legal remedies that data subjects may pursue in court.

4 RITHMS platform for Law Enforcement. European legal framework applicable to validation and future deployment in operational scenarios

4.1 Introduction

This section will present the European legal framework on the use of RITHMS tools by LEAs, both in the testing and validation phase of the project (WP5) and in future operational deployments beyond the project's duration. Before the discussions on the appropriate limitations and safeguards are summarised, however, it should be noted that the debates at international and EU fora do not question the general necessity and proportionality of law enforcement use of practices such as data scraping or hacking to overcome the reported challenges faced by LEAs in the fight against crime (see Gutheil et al., 2017: 24). In fact, most discussions presume such necessity

and proportionality, focusing on how national-level legislation should govern such activities and the restrictions they place on privacy.

At the international level, in November 2016, the UN General Assembly adopted its third resolution on the right to privacy in the digital age.[82] Reaffirming the 2013[83] and 2014[84] resolutions on the same topic, the General Assembly expressed its concern regarding the threats posed to human rights by State-driven surveillance, interception of digital communications and data collection capabilities. Specifically, this concern relates to the 'interlinked and mutually dependent' rights to privacy and freedom of opinion and expression, as enshrined internationally in Articles 12 and 19 of the Universal Declaration of Human Rights (UDHR) and Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR). Both documents stipulate that 'everyone has the right to the protection of the law against such interference or attacks.' In addition to highlighting the UN's concerns, these resolutions offer a range of recommendations for UN States to consider.

Key recommendations of the third UN General Assembly resolution on the right to privacy in the digital age (2016)

- Review 'procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data';
- Establish and maintain existing oversight mechanisms capable of ensuring transparency and accountability – these should be 'independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic' mechanisms (point 5(d)); and
- Provide an effective remedy for the subjects of unlawful or arbitrary surveillance (point 5(e)).

Furthermore, the third resolution recognises the need to further discuss and analyse the promotion and protection of the right to privacy in the digital age, covering 'procedural safeguards, effective domestic oversight and remedies… as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments.' Thus, the resolution also commits to the continued consideration of the issue.

Beyond these General Assembly resolutions, the international-level debates have primarily evolved through the work of the Human Rights Council,[85] the Special Rapporteur on the right to privacy[86] and the Special Rapporteur on the right to freedom of opinion and expression.[87] By contrast, international justice sector bodies – e.g., the UN Office on Drugs and Crime (UNODC), the International Criminal Police Organisation (Interpol) and the Commission for Crime Prevention and Criminal Justice (CCPCJ) – have published very little on the topic. Primarily, the documentation published by these entities echoes, while adding depth and detail to, the third UN

[82] UN General Assembly. 2016. The right to privacy in the digital age. A/C.3/71/L.39/Rev.1.

[83] UN General Assembly resolution 68/167 of 18 December 2013 on the right to privacy in the digital age.

[84] UN General Assembly resolution 69/166 of 18 December 2014 on the right to privacy in the digital age.

[85] Human Rights Council resolutions 28/16 of 26 March 2015; 32/13 of 1 July 2016; and 47/23 of 13 July 2021 (A/HRC/RES/47/23).

[86] Through reports on the right to privacy in the digital age, such as the ones of 30 June 2014 (A/HRC/27/37), of 30 August 2016 (A/71/368), of 24 November 2016 (A/HRC/31/64), of 6 September 2017 (A/HRC/34/60), of 25 January 2021 (A/HRC/46/37)…

[87] A/71/373, A/HRC/23/40 and A/HRC/29/32.

General Assembly resolution. A 2014 report by the UN High Commissioner for Human Rights[88] notes that many UN contributors consider surveillance, interception, and the collection of personal data to be necessary and effective law enforcement practices, when used in compliance with an appropriate legislative framework. In a 2019 resolution,[89] the UN Human Rights Council expresses concern about 'the unlawful or arbitrary collection of personal data' as a highly intrusive act that violates or abuses the right to privacy, can interfere with other human rights and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale. These statements were preceded by the 2013 Report of the Special Rapporteur on the right to freedom of opinion and expression, which provides the following legislative recommendations that are applicable[90] use of the RITHMS Platform by LEAs:

- Complete transparency in the use and scope of surveillance techniques and powers;
- Independent supervision and oversight mechanisms capable of ensuring transparency and accountability;
- Safeguards relating to the nature, scope, and duration of possible measures, as well as the grounds for ordering them and the remedy provided by national law; and
- Notification of individuals that have been subjected to communications surveillance.

This report also reiterates the need for clarity and precision in the legal framework and the importance of the principles of necessity and proportionality. Furthermore, the UN High Commissioner's report states that many UN States currently have "[in]adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight," (para. 47), factors which contribute to an overall lack of accountability for interference in the right to privacy. This position is further supported by the 2016 Report of the Special Rapporteur on the right to freedom of opinion and expression,[91] which states that relevant legislation in this field is often too broad and does not sufficiently engage the public.

Interestingly, while earlier resolutions focused on the negative effects of mass surveillance and the responsibility of states to constrain the powers of intelligence authorities, more recent resolutions reflect a key development in the debate on privacy in the UN. The need to limit the powers of intelligence agencies was the main point of interest in 2016 and 2017.[92] However, these documents also explicitly state that 'the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age.' Thus, in addition to the responsibility of public authorities, the

[88] UN High Commissioner for Human Rights. 2014. The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/27/37.

[89] UN Human Rights Council. 2019. The right to privacy in the digital age: Resolution adopted on 26 September 2019. A/HRC/RES/42/15.

[90] UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

[91] UN General Assembly. 2016. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/71/373.

[92] See UN, General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/ Rev.1, New York, 16 November 2016; UN, Human Rights Council, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 March 2017.

resolutions point to the private sector's responsibility to respect human rights, and call for companies to inform users about the collection, use, sharing and retention of personal data and to establish transparent processing policies.

The Council of Europe has been also very active regarding the protection of fundamental rights and digital technologies, from the Declaration of the committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies),[93] to the Committee of Ministers Recommendation Rec/CM(2020)1 on the human rights impacts of algorithmic systems,[94] along with its accompanying guidelines, or to the recommendation of the Council of Europe Commissioner for Human Rights entitled 'Unboxing Artificial Intelligence: 10 steps to protect Human Rights'.[95] Regarding in particular the use of AI for law enforcement, the Council of Europe's Parliamentary Assembly Resolution 2342 (2020), 'Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems'[96] concludes that the use of AI in policing and criminal justice systems may have significant benefits, but only if properly regulated, since it risks having a particularly serious impact on human rights if it is not.

Key recommendations of the Parliamentary Assembly Resolution 2342 (2020)

1 adopt a national legal framework to regulate the use of AI, based on the core ethical principles mentioned above;

2 maintain a register of all AI applications in use in the public sector and refer to this when considering new applications, so as to identify and evaluate possible cumulative impacts;

3 ensure that AI serves overall policy goals, and that policy goals are not limited to areas where AI can be applied;

4 ensure that there is a sufficient legal basis for every AI application and for the processing of the relevant data;

5 ensure that all public bodies implementing AI applications have internal expertise able to evaluate and advise on the introduction, operation and impact of such systems;

6 meaningfully consult the public, including civil society organisations and community representatives, before introducing AI applications;

7 ensure that every new application of AI is justified, its purpose specified and its effectiveness confirmed before being brought into operation, taking into account the particular operational context;

8 conduct initial and periodic, transparent human rights impact assessments of AI applications, to assess, amongst other things, privacy and data protection issues, risks of bias/ discrimination and the consequences

[93] Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c8011.
[94] Available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.
[95] Available at: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights.
[96] Available at: https://pace.coe.int/en/files/28805/html.

for individuals of decisions based on the AI's operation, with particular attention to the situation of minorities and vulnerable and disadvantaged groups;

9 ensure that the essential decision-making processes of AI applications are explicable to their users and those affected by their operation;

10 only implement AI applications that can be scrutinised and tested from within the place of operation;

11 carefully consider the possible consequences of adding AI-based elements to existing technologies;

12 establish effective, independent ethical oversight mechanisms for the introduction and operation of AI systems;

13 ensure that the introduction, operation and use of AI applications can be subject to effective judicial review.

At the EU level, when focusing on personal data processing for law enforcement and criminal justice taking as a starting point the general standards of the GDPR is unsuited, for two reasons:

- first, the GDPR might in many relevant cases not apply, as other instruments will be applicable;
- second, even when the GDPR does apply, restrictions grounded on the fact that the processing relates to law enforcement and criminal justice might apply, de facto modulating the general safeguards it foresees.

It is thus crucial to appropriately situate discussions on data protection regulation in this field by grounding them on a refined understanding of applicable rules. Many relevant provisions of the GDPR and the LED in relation to data processing are not fully coincidental, and some provisions of the LED are specific to the law enforcement context and have no equivalent in the GDPR, e.g., the distinction between categories of data subjects and between classes of personal data and verification of its quality, and specific logging requirements. Moreover, as explained by the EDPS, data processing activities used are often opaque to individuals, which makes it difficult for them to know who is processing their data and for what purposes, although 'the impact of data processing activities on their rights and freedoms is significant' (EDPS, 2019, 38). An additional challenge from a data subject's perspective is the fact that to some data processing activities might apply intricate combinations of different provisions, which often results in a problematic lack of clarity (FGB, 2019: 4).

4.2 Law enforcement and data protection

4.2.1 Relevant texts

The most relevant text in the context of law enforcement and data protection is the 'Law Enforcement Directive' (LED), Directive 1016/680. The LED entered into force on 6 May 2016. Pursuant to its Article 63(1), Member States had until 6 May 2018 to transpose it in their national laws. The LED repealed and replaced the Council Framework Decision 2008/977/JHA.[97] Prior to the Council Framework Decision 2008/977/JHA, the most important instrument of data protection in the field of criminal justice was the Council of Europe's Recommendation R(87)15 regulating

[97] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60-71.

the use of personal data in the police sector,[98] which complemented Convention 108 for the protection of individuals with regard to automatic processing of personal data.[99] These two instruments of the Council of Europe did not produce a significant convergence of national laws regarding data protection in the context of law enforcement.

The LED aims at producing such convergence. It applies to both domestic and cross-border processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (hereinafter referred to as 'law enforcement') (Article 1(1) LED). In the EU, it is the first instrument that takes a comprehensive approach in the field of law enforcement, as opposed to the previous ad hoc approaches whereby each law enforcement instrument was governed by its own data protection rules. It is also the act through which the EU gives effect to the fundamental right to protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights, in the context of processing of personal data by law enforcement authorities. As Vogiatzoglou et al. (2022: 14) put it, 'The LED seeks to... 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.' Now then, the sensitivity of the area of police and judicial cooperation in criminal matters, together with the complexity of the national legal frameworks that regulate criminal law enforcement, led to a directive being considered the best instrument for achieving a high level of data protection in this field. A directive leaves Member States the necessary flexibility when implementing the principles, rules, and exemptions at national level.[100] As we will see, Member States have made use of this flexibility to adapt the LED to their own police culture.

The LED required the amendment of at least two relevant EU acts (and implementing national rules) to ensure a consistent approach to the protection of personal data within its scope:

- Council Framework Decision 2002/465/JHA on joint investigation teams[101] now specifies that the personal data obtained under Council Framework Decision 2002/465/JHA may be processed for purposes other than those for which these data were collected to the extent laid down in national law and agreed between the Member States setting up the team, in line with the conditions of Articles 4(2) and 9(1) of the LED.

[98] Council of Europe, Committee of Ministers, Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector, 17 September 1987 ('Recommendation R(87) 15').

[99] Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.01.1981 ('Convention 108').

[100] According to the Explanatory memorandum to the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012.

[101] Council Framework Decision of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002, p. 1–3.

- Directive 2014/41/EU regarding the European Investigation Order in criminal matters[102] now clarifies that any processing of personal data obtained under this Directive for purposes other than those for which these data are collected is permitted only under conditions provided for under Article 4 or 9(1) of the LED or Article 6 of the GDPR.

Most acts, though, should still be aligned. It is the case of:

- Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences.[103]
- Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities.[104]
- Council Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States.[105]
- Council Decisions on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decisions).[106]
- Council Decision 2009/917/JHA on the use of information technology for customs purposes.[107]
- Directive (EU) 2015/413 on exchange of information on road safety-related traffic offences.[108]
- Directive (EU) 2016/681 on the use of passenger name record (PNR) data.[109]

[102] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

[103] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253, 29.9.2005, p. 22–24.

[104] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

[105] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332, 18.12.2007, p. 103–105.

[106] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11, and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 12–72.

[107] Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ L 323, 10.12.2009, p. 20–30.

[108] Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences (Text with EEA relevance), OJ L 68, 13.3.2015, p. 9–25.

[109] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

4.2.2 Key notions

The scope of the LED is defined by two key elements (Article 2(1) and Recitals 2-14 LED): the notion of competent authority (personal scope) and the notion of criminal offence (material scope). As regards the personal scope, data processing falls under the LED when, firstly, it is undertaken by a competent authority and, secondly, when the personal data is processed for LED purposes (according to Article 1 LED, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security). 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 have been proved challenging in the implementation of the LED.

'Competent authorities', as defined by Article 3(7) of the LED, may be any public authority competent for 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. A competent authority may be any other body or entity entrusted by Member State law to exercise public authority and public powers for the same law enforcement purposes, even if only sporadically or in isolated cases.

Recital 12 specifies that law enforcement purposes under Article 1 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". Anyway, different understandings of 'criminal offence' at national level led to different types of national authorities falling within the scope of the LED. Certainly, as established in Recital 13, a criminal offence 'should be an autonomous concept of Union law' as interpreted by the CJEU,[110] but, as a matter of fact, Member States have different definitions. The concept of 'public security', on the other hand, risks to expand the LED scope beyond purely criminal justice matters (Vogiatzoglou et al. 2022: 22). Moreover, the LED applies to processing activities in pursuit of public security, but not in pursuit of national security, while there are different understandings of national and public security on a national, European, and international level.

4.2.3 Principles

The LED and the GDPR are based on similar principles, with the aim to produce a consistent interpretation and application of EU data protection rules. The main principles include: lawfulness and fairness (Article 4(1)(a)), purpose specification and limitation (Article 4(1)(b)), data minimization (Article 4(1)(c)), accuracy (Article 4(1)(d)), storage limitation (Article 4(1)(e)), appropriate security (Article 4(1)(f)), and accountability (Article 4(4) of the LED).

[110] See the criteria in Judgment of 22 June 2021, B v Latvijas Republikas Saeima, C-439/19, para. 87.

4.2.4 Data subject rights

The LED ensures the protection of the fundamental rights and freedoms of individuals, and in particular, the right to data protection. It provides a comprehensive framework for the rights of the data subject and how these rights can be exercised, including their right to information, to access, rectify or erase their personal data as well as providing for the restriction of processing.

Due to the specificity of the scope of the LED, some rights included in the GDPR are not found in the LED (e.g., the right to portability) or are more limited that under the GDPR. The LED allows limits to be placed on certain rights (the right of access, Article 15 LED, and the right to rectification or erasure, Article 16 LED) and on the information a data controller must provide to the data subject in relation to personal data that has been processed (Article 13 LED). Data subjects can request DPAs to review a competent authority's restriction of the right in question or ask them to verify whether the restriction was carried out in accordance with the LED (indirect exercise of the right, Article 17 LED).

The LED provides for a not-for-profit body, organisation, or association to lodge a complaint on behalf of a data subject.

4.2.5 Controller and processor obligations

The LED and the GDPR contain similar obligations for data controllers and processors.[111]

Obligations	GDPR	LED
Data protection by design	Article 25	Article 20
Data protection by default	Article 25	Article 20
Record	Article 30	Article 24
Logging	N/A	Article 25

[111] Such as: implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive (Article 19); implement data protection by design and by default (Article 20); use processors that provide sufficient guarantees and act only on instructions from the controller (Article 22); maintain a record of processing activities (Article 24); implement logging measures (Article 25); cooperate with the supervisory authority in the performance of its tasks on request (Article 26); carry out a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 27); consult the supervisory authority in advance in the cases listed in Article 28 of the LED; implement appropriate measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10 (Article 29); notify the supervisory authority of a personal data breach without undue delay, and, where feasible, not later than 72 hours after having become aware of it, when the breach is likely to result in a risk to the rights and freedoms of natural persons (Article 30); communicate the personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to his/her rights and freedoms (Article 31); designate a data protection officer under the conditions set out in Article 32 of the LED; respect the conditions defined for the transfer of personal data to third countries or to international organizations (Article 35 and following).

Cooperation with DPAs	Article 31	Article 26
DPIAs	Article 35	Article 27
Prior consultation with DPIAs	Article 36	Article 28
Security of processing	Article 32	Article 29
Data breach notification	Articles 33 and 34	Articles 30 and 31
DPOs	Articles 37 and 39	Articles 32 and 34

Table 1: Overview of data controller and processor obligations in the GDPR and the LED

The LED also specifically addresses risks linked to the processing of personal data in the criminal law enforcement context. The corresponding provisions include obligations to set time limits for the maximum storage period, distinguish between different categories of data subjects, distinguish between personal data based on facts and data based on a personal assessment, keep a log about the use of personal data, and comply with specific security requirements (Articles 5, 6, 7, 25 and 29 LED, respectively).

4.2.5.1 Storage limitation

Using principles of necessity and proportionality as justification, the LED requires each Member State to provide for appropriate time limits for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures must ensure that those time limits are observed.

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. If 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.

4.2.5.2 Categorisation of data subjects

Unlike the GDPR, the LED explicitly distinguishes different categories of data subjects. 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 (e.g., a person for whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, a 'suspect') (Article 6). 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 requirements such as: lawfulness of the processing, purpose limitation, data minimization, data accuracy and updating, and maximum storage period or information to data subject in LEAs investigation activities.

4.2.5.3 Distinction between classes of personal data and verification of its quality

Another difference between the GDPR and the LED is that the latter requires competent authorities to register facts and opinions separately. Pursuant to Article 7 of the LED, Member States must provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments. They also have to take measures to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. Where incorrect data has been transmitted, recipients should be notified without delay and in such cases the personal data is to be rectified, erased or its processing restricted.

4.2.5.4 Record and logging of processing activities

Article 24 LED 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.

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.

4.2.5.5 Security of processing

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. Article 29 LED imposes on Member States the obligation to provide that 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, 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, and, in particular, 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').

4.2.6 Cross-border data transfers

In an interconnected world, crime (and heritage crime in particular) is increasingly of a cross-border nature. Even when investigating domestic cases, competent authorities increasingly find themselves in cross-border situations because information is stored electronically in a third country. This increases the need for international cooperation in criminal investigations, both on the part of the Member States' authorities and on the part of EU bodies such as Europol and Eurojust. Such cooperation, and in particular the collection and exchange of electronic evidence,[112] often involves the transfer of personal data. Strong data-protection safeguards are essential. Such safeguards also help to build confidence between law enforcement authorities, ensuring faster and more effective information exchange and strengthening legal certainty when information is then used in criminal proceedings. In this respect, the LED provides different tools for facilitating such transfers of personal data from the EU to a third country or an international organisation (for instance, Interpol), while simultaneously ensuring that the personal data continues to benefit from a high level of protection.

[112] Electronic information and evidence are needed in about 85% of investigations into serious crimes, and 65% of the total number of requests are made to providers based in another jurisdiction. See the Commission Staff Working Document, 'Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings', SWD (2018) 118 final.

5 National legal frameworks applicable to RITHMS' use by LEAs

5.1 Introduction

This section presents the study findings on the status of the national legal frameworks for using the RITHMS platform by LEAs, as well as the context in which these frameworks were developed, across the four Member States and two non-EU Member States covered by this study. It explores the presence (or not) of specific legal frameworks that govern the use of tools such as the RITHMS Platform by law enforcement, highlighting examples from national level.

An important starting point are the national provisions transposing the LED. When transposing the LED, Member States either amended their previous legislation on data protection or repealed and replaced it with a new horizontal data protection act. In many instances, the national laws transpose the LED by referring to the same or equivalent provision of the GDPR (e.g., as regards definitions, notifications of data breaches, the appointment of the data protection officer and provisions on the organisation, status, competences, tasks, and powers of the national data protection supervisory authorities). A number of the LED's provisions were also transposed through new provisions in, for instance, general administrative law, administrative procedural law or criminal procedure. Some Member States also transposed several LED's provisions in sectoral legislation regulating the operation and powers of specific competent authorities. As we will see, overall, the national laws largely reflect the LED's principles and core provisions.[113]

But this is not all. The use of AI-based tools by law enforcement, as discussed throughout this study, is a relatively new phenomenon. It is therefore not surprising, considering the notion of 'law lag', that not all Member States examined have specific legislative provisions. Furthermore, those that do have specific legislative provisions have, for the most part, enacted them recently. More specifically, one of the four Member States examined (The Netherlands) has passed specific legal provisions related to the use of AI-based techniques by law enforcement. As illustrated below, they passed these legislative changes only after 2016. Anyway, the absence of specific legislative provisions does not necessarily prohibit or prevent the use of AI-based tools by LEAs. In fact, it is widely acknowledged that LEAs in Italy and Spain (i.e., the two Member States examined that do not currently have specific legal provisions) use such tools and techniques. The use of these so-called 'grey area' legal provisions is not considered sufficient by the UN, which calls instead for legislative clarity and precision.[114] In countries such as Italy and Spain, the existing legal bases for the use of AI-based tools by law enforcement are tied to more traditional investigative tools that are considered similar.

[113] As indicated in the Communication from the Commission to the European Parliament and the Council, 'First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')', 25 July 2022. Available at:

[114] UN Human Rights Council. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40.

5.2 Bosnia and Herzegovina

5.2.1 Relevant texts

In Bosnia and Herzegovina there is not a specific legal instrument directly implementing the LED Directive, as this country is not an EU member. General rules on data protection can be found on the Law on the Protection of Personal Data No. 49/06, amended in 2011, as well as in several Regulations.[115]

5.2.2 Data subject rights

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.

5.2.3 Controller and processor obligations

DPIA

There is no obligation to conduct a DPIA.

Storage limitation

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.

Categories of data subjects

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.

[115] Regulation on procedure upon complaint by the data subject issued to the agency for personal data protection ("Official Gazette of Bosnia and Herzegovina" 51/09); Regulation on supervision inspection regarding protection of personal data („Official Gazette of Bosnia and Herzegovina" 51/09); Regulation on the manner of keeping and special measures of technical protection of personal data ('Official Gazette of Bosnia and Herzegovina' 67/09); Regulation on the manner of keeping the records of personal data filing systems and the pertinent records form ('Official Gazette of Bosnia and Herzegovina' 52/09). Available here: http://www.azlp.ba/propisi/Default.aspx?id=5&langTag=en-US&template_id=149&pageIndex=1

Processing of special categories of data

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.

Record and logging

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.

Data breach notification

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.

5.3 Bulgaria

5.3.1 Relevant texts

The Personal Data Protection Act of the Republic of Bulgaria (PDPA) was amended in 2019 in order to implement Directive (EU)2016/680. In particular, Chapter 8 was created to rule the protection of natural persons with regard to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including safeguarding against and prevention of threats to public order and security.

It is also important to consider the Ministry of the Interior Act No. 53, of 27 June 2014 (known as ZMVR), which empowers the Ministry of Interior to process personal data to carry out operational research, surveillance and investigative activities relating to offences, as well as intelligence activity (art. 6). The Ministry of the Interior Act also regulates the creation of police records as a form of processing of personal data (Art. 68).

Other important legal texts regarding the implementation of Directive (EU)2016/680 in Bulgaria are the Regulation laying down detailed rules for the implementation of police records (DV No. 90 of 31 October 2014), the Criminal Procedure Code and the Special Intelligence Assets Act.

The Commission for Personal Data Protection ('CPDP') is the national DPA of the Republic of Bulgaria responsible for the protection of personal data both in the public and private sectors.

5.3.2 Data subject rights

Bulgaria has made use of the possibility given by Article 15(1) of the LED to restrict data subjects' right of access to their personal data. 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 (Art. 37a of the Bulgarian Personal Data Protection Act). The terms and conditions for application of this provision should be further regulated by a specific law.

5.3.3 Controller and processor obligations

DPIA

The CPDP adopted a List of processing operations requiring data protection impact assessment pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679[116] 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;
- 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;

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

- 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.

Storage limitation

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.

Categories of data subjects

Article 47 of the Bulgarian PDPA simply reproduces Article 6 LED.

Processing of special categories of data

Article 51 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 (Art. 51(2) PDPA).

Judgment of the CJEU (Fifth Chamber) of 26 January 2023, in Case C-205/21 regarding Bulgarian legislation on the recording of biometric and genetic data by the police,[117] concludes that 'Article 10 of Directive 2016/680... must be interpreted as precluding national legislation which provides for the systematic collection of biometric and genetic data of any person accused of an intentional offence subject to public prosecution in order for them to be entered in a record, without laying down an obligation on the competent authority to verify whether and demonstrate that, first, their collection is strictly necessary for achieving the specific objectives pursued and, second, those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned.'

117 Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=269704&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1

Record and logging

Articles 62 and 63 of the Bulgarian PDPA simply reproduce Articles 24 and 25 LED

Data breach notification

The Bulgarian Act contains exemptions to the obligation of communication of a personal data breach to the data subject 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.

5.4 Italy

5.4.1 Relevant texts

In Italy the LED has been implemented by 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 offence.

5.4.2 Data subject rights

Italy has made use of the possibility given by Article 15(1) of the LED to restrict data subjects' right of access to their personal data. 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.

5.4.3 Controller and processor obligations

DPIA

Article 23 of Decree 51 simply reproduces Article 27 of the LED. The Garante adopted the same list contained in the EDPB's Guidelines on DPIA.[118]

Storage limitation

Decree 51 does not include any provision regarding storage limitation.

Categories of data subjects

[118] 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.

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.

Processing of special categories of data

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.

Record and logging

Articles 20 and 21 of Decree 51 simply reproduce Articles 24 and 25 LED.

Data breach notification

Article 27 of Decree 51 does not introduce substantive changes in this obligation.

5.5 Moldova

5.5.1 Relevant texts

Moldova is not an EU Member State and European provisions on personal data protection are not directly applicable in Moldova. However, many provision of the GDPR and the LED have been implemented in the Law on Personal Data Protection (No. 133 of 8 July 2011), amended by Law No. 175 of 11 November 2021). The processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences in Moldova is also ruled by the Instructions on the Processing of Personal Data in the Police Sector (Order of May 2013). Article 16(1) of the Law No. 320 of 27 December 2013, on police activities and the status of police officers,[119] 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, in accordance with the provisions of the legislation regarding the protection of personal data.

5.5.2 Data subject rights

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.

[119] Available in English (automatic translation) at: https://cis-legislation.com/document.fwx?rgn=58035.

5.5.3 Controller and processor obligations

DPIA

In Moldova, controllers have the obligation to perform a DPIA, considering the nature, scope, context, and purposes of the processing using new technologies, whenever it 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.

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:

- 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.
- 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.
- The processing of personal data with the aim of systematic monitoring, on a large scale, of an area accessible to the public.

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

Storage limitation

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.'

Article 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 pursued purpose.

Categories of data subjects

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.

Processing of special categories of data

Article 6 of the PDPA 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 PDPA 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.

Record and logging

Article 4(1)(e) of the LPDP 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.

Data breach notification

In Moldova, data controllers shall submit to the National Centre for Personal Data Protection an annual report on any security incidents involving information systems during that year.

5.6 The Netherlands

5.6.1 Relevant texts

The Dutch DPA has issued guidelines on the processing of personal data by the police, in the judicial system, and during private investigations.

5.6.2 Data subject rights

The Netherlands has made use of the possibility given by Article 15(1) of the LED to restrict data subjects' right of access to their personal data. Articles 24(b) and 27 of the Dutch Police Data Act reproduce Article 13 LED. Article 24(b) does not refer 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.

5.6.3 Controller and processor obligations

DPIA

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 DPA has published an overview of types of processing activities that require a DPIA.[120] 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.

Storage limitation

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).

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

Categories of data subjects

Article 6(b) of the Dutch Police Data Act simply reproduces Article 6 LED.

Record and logging

Articles 31(d) and 32(a) of the Dutch Police Data Act simply reproduce Articles 24 and 25 LED.

Data breach notification

Article 33(a)(5)-(7) of the Dutch Police Data Act simply reproduces Article 31 LED, not including, though, Article 31(4) LED.

5.7 Spain

5.7.1 Relevant texts

In Spain, the LED has been implemented by 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.

5.7.2 Data subject rights

Spain has made use of the possibility given by Article 15(1) of the LED to restrict data subjects' right of access to their personal data. Article 24 of Organic Law 7/2021 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.

5.7.3 Controller and processor obligations

DPIA

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')[121] or do not require ('Whitelist')[122] 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 of the GDPR; the use of data on a large scale; the

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

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

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.

Storage limitation

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.

Categories of data subjects

Article 9 of Organic Law 7/2021 simply reproduces Article 6 LED.

Processing of special categories of data

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.

Record and logging

Articles 32 and 33 of Organic Law 7/2021 simply reproduce Articles 24 and 25 LED.

Data breach notification

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[123] that when data subject notification may compromise the outcome of an ongoing investigation, the controller may delay notification under the AEPD's supervision.

[123] AEPD, Guía para la notificación de brechas de datos personales. Available at:

6 Conclusion

Even though actual end-users have a responsibility of their own for legal compliance, not all responsibility for a proper functioning and use of the RITHMS Platform can be ascribed to the end-users. In practice, some responsibility for a proper functioning of the RITHMS Platform also lies with the developers of the Platform. It is interesting to note, though, that the legal analysis taught that more restrictions seem to apply to the researchers within the RITHMS project, than is the case with the actual end-users. Actual end-use might have a huge impact on society, which will be explored in -D7.3 Report on RITHMS social benefits and risks (UDC, R, PU, M12). However, foreseen end-users quite often can call upon special authorities and competencies in the field of law enforcement, which, in contrast, do not exist for the private parties developing and testing the RITHMS Platform.

List of laws

1.1 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.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 152, 3.6.2022, p. 1–44.

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 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.06.2001, p. 0010-0019.

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), OJ L 111, 5.5.2009, p. 16–22.

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) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance), OJ L 130, 17.5.2019, p. 92–125.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, p. 56–83.

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.

Resolutions

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

1.2 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.

Council of Europe's Convention for the protection of individuals with regard to the processing of personal data ('Convention 108 +').

Council of Europe Committee on Artificial Intelligence's 'Zero Draft' of the Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law ('the Framework AI Convention').

1.3 National regulations

Belgium

Act on the protection of natural persons with regard to the processing of personal data,[124] available in English (unofficial translation) at: https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf.

Act of 3 December 2017 establishing the Data Protection Authority (as amended), available in Dutch at: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018052501&table_name=wet.

[124] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Bosnia and Herzegovina[125]

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,[126] 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,[127] available in Bulgarian at: https://lex.bg/bg/laws/ldoc/2134163459.

Ministry of the Interior Act.[128]

Croatia

Act on the Implementation of the General Data Protection Regulation, available in English at: https://azop.hr/national-legislation/.

Finland

Data Protection Act (1050/2018), available in English (non-binding translation) at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

[125] 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.

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

[127] ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА.

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

Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018), available in English at: https://www.finlex.fi/en/laki/kaannokset/2018/en20181054.pdf

Germany

Federal Data Protection Act of 30 June 2017, available in English (official translation) at: http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf.

Italy

Legislative Decree No. 196/2003, setting out the 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,[129] available in English at https://www.garanteprivacy.it/documents/10160/0/PERSONAL+DATA+PROTECTION+CODE.pdf/96672778-1138-7333-03b3-c72cbe5a2021?version=1.0.

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,[130] available in Italian at https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/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,[131] available in Italian at https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2021-11-29&atto.codiceRedazionale=21G00195&elenco30giorni=false.

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,[132] available In Italian at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

[129] 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.

[130] 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.

[131] 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.

[132] 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

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),[133] 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,[134] available in Italian at: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.

Moldova[135]

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.

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.

Instructions on the Processing of Personal Data in the Police Sector (Order of May 2013),[136] only available in Romanian at: http://datepersonale.md/wp-content/uploads/2020/01/instructiune-20130712.pdf.

Law No. 320 of 27 December 2013 on police activities and the status of police officers, available in English (automatic translation) at: https://www.legis.md/cautare/getResults?doc_id=120699&lang=ru.

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.

---

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).

[133] 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.

[134] 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.

[135] 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.

[136] Instrucţiunilor privind preluerarea datelor cu caracter personal în sectorul poliţienesc.

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,[137] 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 prosecution of criminal offences or the execution of criminal penalties,[138] 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),[139] available in Dutch at: https://zoek.officielebekendmakingen.nl/stcrt-2022-15876.html.

Code of Criminal Procedure (henceforth DCCP),[140] which incorporates the Special Powers of Investigation Act,[141] and the Computer Crime Act III 2018.[142]

Romania

Law No. 190/2018 (Data Protection Law),[143] available in English at: https://www.dataprotection.ro/servlet/ViewDocument?id=1685.

[137] 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).

[138] 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

[139] 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.

[140] Wetboek van Strafvordering.

[141] Wet Bijzondere Opsporingsbevoegdheden.

[142] Wet Computercriminaliteit III.

[143] Law no. 190/2018 on implementing measures 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 (General Data Protection Regulation).

Law No. 506/2004, on the processing of personal data and the protection of privacy in the electronic communications sector, available in English at: https://www.dataprotection.ro/servlet/ViewDocument?id=173.

Spain

Spanish Data Protection Law,[144] 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,[145] 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,[146] 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),[147] available in English (official version, not updated) at: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.

Switzerland

Federal Act of 19 June 1992 on Data Protection, available in English (official non-binding translation) at: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en. In force until September 1, 2023.

Revised Federal Act of 25 September 2020 on Data Protection, available in German, French and Italian (official translations) at: https://www.fedlex.admin.ch/eli/oc/2022/491/de. Not yet in force.

Ordinance of 14 June 1993 to the Federal Act on Data Probation, available in English (official non-binding translation) at: https://www.fedlex.admin.ch/eli/cc/1993/1962_1962_1962/en. In force until September 1, 2023.

Revised Ordinance of 31 August 2022 to the Federal Act on Data Probation, available in German, French and Italian (official translations) at: https://www.fedlex.admin.ch/eli/oc/2022/568/de. Not yet in force.

Agreement between the European Union and the Swiss Confederation on security procedures for the exchange of classified information, signed on 28 April 2008, as attached to the Council Decision 2008/568/PESC of 24 June 2005, as well as its implementing arrangements, available in English (official version) at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22008A0710(01).

[144] 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).

[145] 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.

[146] 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.

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

References

[1] AlgorithmWatch, Automating Society. Taking Stock of Automated Decision Making in the EU. Report, January 2019. Available at: https://algorithmwatch.org/en/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf.

[2] C. Altobelli, N. Forgó, E. Johnson, A. Napieralski, "To Scrape or Not to Scrape? The Lawfulness of Social Media Crawling under the GDPR." In Deep Driving into Data Protection - 1979-2019 Celebrating 40 Years of Privacy and Data Protection at the CRIDS, Larcier, 2020.

[3] D. Ang, "The web scraper's world of copyright exceptions and contractual overrides," Singapore Law Review, vol. 13, 2021, pp. 1-16.

[4] I. Ballon, "Data Scraping, Database Protection and the Use of Bots and Artificial Intelligence to Gather Content and Information." In E-Commerce & Internet Law: Treatise with Forms. Volume 1, 2nd ed. Thomson Reuters, 2020.

[5] A. Barbieri, M. Bellezza, "Linking, Searching, Scraping: What's Going On In Europe And Italy," 4 April 2014. [Online] Available at: https://www.mondaq.com/italy/copyright/301346/linking-searching-scraping-what39s-going-on-in-europe-and-italy.

[6] V. Barrera, A. Malm, D. Décary-Hétu, R. Munksgaard, "Size and scope of the tobacco trade on the darkweb," Global Crime, vol. 20, no. 1, 2019, pp. 26-44.

[7] R. Belfiore, "The Protection of Personal Data Processed within the Framework of Police and Judicial Cooperation in Criminal Matters." In Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings. Springer, Berlin-Heidelberg, 2013, pp. 355-370.

[8] M. Bellezza, "CJEU ruling in Svensson case: Free linking in a free web?," 4 March 2014. Available at: https://www.dirittocomparati.it/cjeu-ruling-in-svensson-case-free-linking-in-a-free-web/.

[9] F. Campbell, "Data scraping - what are the privacy implications?" Privacy and Data Protection, vol. 20, no. 1, 2019, pp. 3-6.

[10] S. Cretu, C. Timofte, Romania - Data Protection Overview. [Online] August 2022. Available at: https://www.dataguidance.com/notes/romania-data-protection-overview.

[11] D. Décary-Hétu, B. Dupont, F. Fortin, "Policing the Hackers by Hacking Them: Studying Online Deviants in IRC Chat Rooms," in Networks and Network Analysis for Defence and Security. Cham: Springer, 2014, pp. 63-82.

[12] T. D'hulst, Van Bael, Bellis, Data Protection in Belgium: Overview. Practical Law Data Privacy & Security [Online] January 2022. Available at: https://uk.practicallaw.thomsonreuters.com/2-502-2977?transitionType=Default&contextData=(sc.Default)&firstPage=true.

[13] E.S. Dove, J. Chen, "What does it mean for a data subject to make their personal data 'manifestly public'? An analysis of GDPR Article 9(2)(e)," International Data Privacy Law, Vol. 11, No. 2, 2021, pp. 107-124.

[14] L. Edwards, L. Urquhart, "Privacy in public spaces: what expectations of privacy do we have in social media intelligence?" International Journal of Law and Information Technology, vol. 24, 2016, pp. 279-310.

[15] R. Frank, A. Mikhaylov, "Beyond the 'Silk Road': Assessing Illicit Drug Marketplaces on the Public Web," in Open-source intelligence and cybercrime. Springer, 2020.

[16] S. Golla, D. Müller, "Web Scraping Social Media: Pitfalls of Copyright and Data Protection Law," 15 April 2020. [Online] Available at: https://blog.prif.org/2020/04/15/web-scraping-social-media-pitfalls-of-copyright-and-data-protection-law/.

[17] G. González Fuster, Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights. Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, July 2020. [Online] Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf.

[18] M. Gutheil, Q. Liger, A. Heetman, J. Eager, M. Crawford, et al., "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices," Study for the LIBE Committee, 2017. [Online] Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

[19] T. J., Holt, A. M. Bossler, Cybercrime in progress: Theory and prevention of technology-enabled offenses. London: Routledge, 2015.

[20] C. Jasserand, "Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?", Computer Law & Security Review, vol. 34, no. 1, 2018, pp. 154–165.

[21] P. Kamocki et al., ELRC Report on legal issues in web crawling. Report, 22 March 2018 [Online]. Available at: http://www.elra.info/media/filer_public/2021/02/12/elrc-legal-analysis-webcrawling_report-v11.pdf.

[22] V. Krotov, L. Johnson, "Legality and Ethics of Web Scraping," Communications of the Association for Information Systems, 2020. Available at: https://www.researchgate.net/publication/324907302_Legality_and_Ethics_of_Web_Scraping.

[23] H. L. Larsen, J. M. Blanco, R. Pastor Pastor, R. R. Yager (eds), Using open data to detect organized crime threats. Cham: Springer, 2017.

[24] E. Lazar, D. N. Costescu, "Data Protection Regulations: Overview of the Romanian Legislation and Deficiencies," in Data Protection in the Internet. Cham: Springer, 2018, pp. 285-308.

[25] M. Leistner, L. Antoine, "IPR and the use of open data and data sharing initiatives by public and private actors," Study requested by the JURI committee, May 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf.

[26] A. Luscombe, K. Walby, "Theorizing freedom of information: the live archive, obfuscation, and actor-network theory," Government Information Quarterly, vol. 34, no. 3, 2017, pp. 379–387.

[27] O. Manuilenko, S. Novoselic, Croatia – Data Protection Overview. [Online] March 2023. Available at: https://www.dataguidance.com/notes/croatia-data-protection-overview.

[28] T. Margoni, M. Kretschmer, "A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology," GRUR International, Journal of European and International IP Law, vol. 71, no. 8, 2022, 685-701.

[29] T. Marquenie, "Legal and Ethical Challenges in Algorithmic Policing and Law Enforcement AI," in Technology and Society: The Evolution of the Legal Landscape, Gompel & Svacina, 2020.

[30] N. Marres, E. Weltevrede, "Scraping the social? Issues in live social research," Journal of Cultural Economy, vol. 6, no. 3, 2013, pp. 313–335.

[31] R. McAlister, "Webscraping as an Investigation Tool to Identify Potential Human Trafficking Operations in Romania", WebSci '15: Proceedings of the ACM Web Science Conference, no. 47, June 2015, 1–2, https://doi.org/10.1145/2786451.2786510

[32] M. Nebel, Germany - Data Protection Overview. [Online] April 2023. Available at: https://www.dataguidance.com/notes/germany-data-protection-overview.

[33] J. Nevalainen, L. Vaaraniemi, A. Hård af Segerstad, Finland - Data Protection Overview. [Online] March 2023. Available at: https://www.dataguidance.com/notes/finland-data-protection-overview.

[34] G. Olivi, Italy – Data Protection Overview. [Online] February 2023. Available at: https://www.dataguidance.com/notes/italy-data-protection-overview.

[35] S. O'Reilly, "Nominative fair use and Internet aggregators: Copyright and trademark challenges posed by bots, web crawlers and screen-scraping technologies," Loyola Consumer Law Review, vol. 19, no. 3, 2007, pp. 273-288.

[36] M. Peguera, "Hyperlinking Under the Lens of the Revamped Right of Communication to the Public", Computer Law & Security Review, vol. 34, issue 5, 2018, pp. 1099-1118.

[37] L. W. Perry, B. McInnis, C. C. Price, S. Smith, J. S. Hollywood, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations." Report, Rand Corporation, 2013.

[38] K. Soska, N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem." In Proceedings of the 24th USENIX Security Symposium. Washington, DC, 2015, pp. 33-48.

[39] D. N. Staiger, "Swiss Data Protection Law", in Data Protection in the Internet. Cham: Springer, 2018, pp. 397-408.

[40] M. Stassen, F. van Remoortel, Belgium – Data Protection Overview. [Online] November 2022. Available at: https://www.dataguidance.com/notes/belgium-data-protection-overview.

[41] T. Steiner, Switzerland – Data Protection Overview. [Online] August 2022. Available at: https://www.dataguidance.com/notes/switzerland-data-protection-overview.

[42] P. Szwed, Is web scraping legal? A short guide on scraping under EU law. [Online] May 22, 2021. Available at: https://discoverdigitallaw.com/is-web-scraping-legal-short-guide-on-scraping-under-the-eu-jurisdiction/.

[43] M. Truyens, P. van Eecke, "Legal Aspects of Text Mining," Computer Law & Security Review, vol. 30, 2014, pp. 153-170.

[44] P. Vogiatzoglou, T. Marquenie, Assessment of the implementation of the Law Enforcement Directive. Study requested by the LIBE Committee, December 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf.

[45] G. Xiao, "Bad Bots: Regulating the Scraping of Public Personal Information," Harvard Journal of Law & Technology, vol. 34, no. 2, 2021, pp. 701-732.

[46] A. Zamora, "Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online," The Journal of Business, Entrepreneurship & the Law, vol. 12, no. 1, 2019, pp. 203-227.

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