
# D1.3 Ethical and Legal Analysis Report

| | |
|---|---|
| **Lead Beneficiary** | KUL |
| **Dissemination Level** | PUBLIC |
| **Date** | 29/02/2024 |
| **Grant Agreement Number** | 101121152 |

Funded by
the European Union

# Project Information

| | |
|---|---|
| **Grant Agreement Number** | 101121152 |
| **Acronym** | ENACT |
| **Name** | European Network Against Crime and Terrorism |
| **Call Topic** | HORIZON-CL3-2022-SSRI-01-02 Knowledge Networks for Security Research & Innovation |
| **Action Type** | Coordination and Support Action |
| **Start Date** | 01/09/2023 |
| **Duration** | 36 Months |
| **Coordinator** | PJ |

# Document Information

| | |
|---|---|
| **Work Package** | WP1: Coordination and management 1 |
| **Deliverable** | D1.3: Ethical and legal analysis report |
| **Date** | 29/02/2024 |
| **Type** | [REPORT][ETHICS] |
| **Dissemination Level** | [PUBLIC] |
| **Lead Beneficiary** | KUL |
| **Main Author(s)** | Isabela Maria Rosal (KUL) |
| **Contributors** | Irmak Erdogan Peter (KUL) |
| **Document Reviewers** | Andre Alegria (PJ); Theoni Spathi (CERTH) |
| **Security Reviewer** | Rocío Carbayo Martín (ESMIR) |
| **Ethics Reviewer** | Triantafyllos Kouloufakos (KUL) |

# Revision History

| Version | Date | Author | Comments |
|---|---|---|---|
| 0.1 | 16/01/2024 | Isabela Maria Rosal (KUL) | ToC |
| 0.2 | 23/02/2024 | Isabela Maria Rosal (KUL) | 50% of the Deliverable Content |
| 0.3 | 14/02/2024 | Isabela Maria Rosal (KUL)<br>Irmak Erdogan Peter (KUL) | 80% of the Deliverable Content |
| 0.4 | 19/02/2024 | Isabela Maria Rosal (KUL) | First Draft |
| 0.5 | 20/02/2024 | Andre Alegria (PJ) | 1st Review |
| 0.6 | 26/02/2024 | Theoni Spathi (CERTH) | 2nd Review |
| 0.7 | 27/02/2024 | Isabela Maria Rosal (KUL) | Final Draft |
| 0.8 | 28/02/2024 | Rocío Carbayo Martín (ESMIR) | Security Review: verify that no security-sensitive information is included in the document, ensure appropriate classification of the deliverable, and confirm that no security-relevant issues are present |
| 0.9 | 29/02/2024 | Triantafyllos Kouloufakos (KUL) | Ethics Check: peer review of content; evaluation of accessibility, transparency and non-discriminatory language aspects. |
| 1.0 | 29/02/2024 | Isabela Maria Rosal (KUL) | Final |
| 2.0 | 14/08/2025 | Isabela Maria Rosal (KUL) | Updated in line with feedback from EAB and REA expert review. |

# Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

# Copyright

# Abbreviations

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **the Charter** | Charter of Fundamental Rights of the European Union |
| **CJEU** | Court of Justice of the European Union |
| **CoE** | Council of Europe |
| **D** | Deliverable |
| **DEDA** | Data Ethics Decision Aid |
| **DMP** | Data Management Plan |
| **EAB** | Ethics Advisory Board |
| **ECHR** | European Convention on Human Rights |
| **ECtHR** | European Court on Human Rights |
| **ELS** | Ethical, Legal and Societal |
| **ELSO** | Ethical, Legal and Societal Observatory |
| **ENISA** | European Union Agency for Cybersecurity |
| **EU** | European Union |
| **FCT** | Fight against Crime and Terrorism |
| **FRIA** | Fundamental Rights Impact Assessment |
| **GDPR** | General Data Protection Regulation |
| **LEA** | Law Enforcement Authority |
| **LED** | Law Enforcement Directive |
| **M** | Month |
| **OECD** | Organisation for Economic Co-operation and Development |
| **R&I** | Research and Innovation |
| **RRI** | Responsible Research and Innovation |
| **TFEU** | Treaty on the Functioning of the European Union |
| **UDHR** | Universal Declaration of Human Rights |
| **UN** | United Nations |
| **WP** | Work Package |

# Table of Contents

## Contents

# List of Tables

# Executive Summary

This Deliverable, D1.3 “Ethical and Legal Analysis Report”, is the result of the work already developed within T1.4 “Ethical Management & Legal Analysis”. The tasks goals are twofold. First, the task will identify the relevant legal and ethical frameworks to be considered in the project’s activities and duration, with focus on human rights, data protection, cybersecurity and data management. Mapping the relevant framework is essential to establish good practices and to identify attention points for all the partners of the projects. Second, the results of this analysis will allow the identification of the effects, negative and positive, of the project into society. Reflecting upon possible risks, it will be possible to create and test mitigation measures to guarantee that ENACT’s results are compliant by-design and by-default.

D1.3 will present the methodology adopted in the assessment of legal and ethical requirements. ENACT, then, will follow the Responsible Research and Innovation (RRI) approach[1], which will allow a continuous and effective implementation of mitigation measures in parallel with a comprehensive analysis of the risks of the project, via engagement with different stakeholders. Following, the Deliverable will present an initial assessment of which human rights might be interfered by the project activities. As a knowledge hub, ENACT will handle different datasets. Thus, this report also presents the initial analysis of the relevant framework for data management to be considered by ENACT partners, evaluating the differences between personal and non-personal data. Finally, the report also will establish an introduction to cybersecurity aspects that shall be applied and considered in the design of ENACT’s products.

As the evaluation of risks and benefits of a product is a continuous activity, this Deliverable should be understood as the inaugural assessment of the relevant ethical and legal frameworks. The results here presented will be updated in the following cycles of the project.

[1] Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D., (2013). A framework for responsible innovation. **Responsible innovation: managing the responsible emergence of science and innovation in society,** 31, 27-50.

# 1 Introduction

## 1.1 ENACT Concept and Approach

Knowledge is one of the most strategic assets available to the European Union. The ability to anticipate threats, adapt to emerging challenges, and ensure evidence-based policymaking depends not only on technological capabilities or operational readiness, but also on the existence of robust, structured, and accessible knowledge ecosystems. Recognising this, the European Commission, through DG HOME, launched a dedicated effort to establish Knowledge Networks in key security domains, including the fight against crime and terrorism, border management, disaster resilience, among others.

The creation of these networks responds to a fundamental challenge: while Europe has invested heavily in security research and operational innovation, the results of these efforts are often fragmented, difficult to access, or disconnected from the needs of practitioners. Valuable knowledge produced in EU-funded projects, national initiatives, or institutional bodies frequently remains isolated within specific communities, limiting its practical impact and slowing the uptake of innovation.

Knowledge Networks are intended to address this structural gap. By promoting cooperation, knowledge sharing, and strategic alignment among researchers, practitioners, policymakers, and industry, these initiatives seek to create long-term, service-oriented platforms that consolidate existing expertise and make it actionable. More than just repositories or research summaries, these networks are designed to foster dialogue, support policy development, and contribute to the long term resilience and effectiveness of the security of the European Union.

Through these efforts, DG HOME aims to ensure that the wealth of knowledge already produced, and still to come, can be better organised, better used, and ultimately better connected to the priorities of the Union and its citizens.

ENACT – European Network Against Crime and Terrorism – is one of the thematic Knowledge Networks aiming to strengthen Europe's capacity to fight crime and terrorism through structured knowledge, strategic collaboration, and innovation uptake. As a network, ENACT brings together law enforcement agencies, researchers, policymakers, and industry to collect, organise, and make sense of the vast and fragmented body of knowledge generated across the FCT landscape. It provides a platform for sharing insights, identifying gaps, validating solutions, and aligning research and innovation with real operational needs, serving as both a knowledge hub and a bridge between research and practice.

## 1.2 Purpose of the deliverable and links to other deliverables

ENACT aims to contribute and facilitate the Research and Innovation (R&I) ecosystem in the Fight against Crime and Terrorism (FCT) by presenting a knowledge hub with structured and accessible information regarding the expertise already produced in the field. Even though the goals of the project are legitimate and contribute to different stakeholders, ethical and legal risks may arise. Understanding said possible negative effects is relevant to guarantee that ENACT results, including its Knowledge Hub, are compliant-by-design, meaning that the

relevant legal and ethical framework is considered and effectively applied since the design phase of the project.

Deliverable 1.3 “Ethical and Legal Analysis Report” is part of T1.4 “Ethical Management & Legal Analysis”. This Task aims to develop a proactive approach in identifying and mitigating relevant ethical and legal risks, especially those related to human rights, data protection, cybersecurity, and data management. The Report presents the initial effort of mapping and understanding the relevant ethical and legal framework while underlining the connection of said norms and principles to the project activity. For this goal, the purposes and foreseen uses of ENACT’s products were understood via an ongoing engagement with partners, an essential activity for a complete and useful assessment.

This Deliverable will be updated in the next cycles of the project. Each cycle will be implemented in each of the years of the project, meaning that currently the activities are under the first cycle (M1-M12), and the next cycles will be equivalent to the next years of the project (cycle 2 from M13 to M24, and cycle 3 from M25 to M36). New developments will be presented in new documents to guarantee that the compliance-by-design of the project results continue up to date and in accordance with new discoveries. For this, the ethical partner (KUL) will continue to follow-up on the new additions on the ENACT final products (e.g., technological changes, increased databases).

The report intends to present an initial evaluation of the applicable legal and ethical frameworks related to the ENACT project as a result of the work already developed in Task T1.4. This initial assessment allows a summarization of points of attention for all the partners of the project, also highlighting which legal and ethical principles should be the main guidelines of the research developed in ENACT. However, the report does not exist in isolation. It connects to different activities developed in the project.

As an ongoing part of the coordination and management of the project, the legal and ethical analysis will continue in the next years of the project, especially in T2.4 (Ethical Management & Legal Analysis) and T3.4 (Ethical Management & Legal Analysis). In each of these tasks, a new version of the report will be presented as part of D2.1 and D3.1, accordingly. Updating the legal and ethical analysis is important for guaranteeing that new developments of the framework and of the project are considered, which will allow the project to have relevance and an optimal timing for the results to serve R&I and FCT community.

Additionally, considering that this report presents aspects that must be considered by the whole project, the present Deliverable also support the needed knowledge for the development of T5.1, T6.1 and T7.1 (Deliver knowledge on capability needs and gaps, technology R&I, market, funding and standardisation opportunities and socio-technical dimensions). Since the legal and ethical partners (especially KUL and VICOM) will also be part of these tasks, it is expected that the topics brought in this deliverable are embedded in the data collection and analysis of the project, adopting the most adequate and less risky methods for the goals of the project.

Also, since this report focus on the risks, and legal and ethical frameworks related to the results of the research project, it does not further details the internal data management of personal data handled by partners inside and in the context of the project. So, it is relevant to notice

that the conclusions produced in this report are complemented by the Data Management Plan (DMP), already submitted (M03) in D1.2. The DMP will also be updated in the next deliverables WP2 and WP3, namely D2.1 and D3.1, adding to the methodology also adopted in this report of having a continuous approach of risks evaluation of the project activities.

Additionally, considering that ethical aspects will also be assessed in this report, the findings of the research will have a close connection to WP9, the additional ethics WP. The activities developed in this WP will result in ethical reports drafted by specialists composing the external Ethics Advisory Board (EAB). This group will provide further guidance on ethical aspects that should be considered in the project via the reports, and also meetings, emails or other forms of communication.

Finally, it is crucial to notice that these connections illustrate a part of the horizontal approach for legal and ethical topics in ENACT but does not exhaust it. In other words, beyond the connections here presented, the ethical and legal analysis and assessment rely on engagement with all the partners involved in the project and, to a certain extent, external stakeholders (see section 2.1.). Throughout biweekly general meetings, extraordinary, dedicated meetings, review of all deliverables and other forms of communication (e.g., e-mail exchange), the ethical and legal partners will be kept informed about any changes in the project's approach and design. Via these, it will be possible to also ensure that the defined best practices for legal and ethical considerations are well discussed and incorporated in everyday activities within the project, allowing for any specific doubt or ambiguity to also be further considered and addressed.

## 1.3 Structure of this Deliverable

As an initial assessment report, this Deliverable presents key elements of the relevant mapped legal framework that directly affect the goals and results of the ENACT project, by following this structure:

- Section 2, Legal and Ethical Analysis, presents the rationale behind having a legal and ethical analysis and presents the methodology to be followed by ENACT for this analysis, the Responsible Research and Innovation (RRI) approach, which will allow a better understanding of societal needs and guarantee the engagement with different stakeholders to implement effective and useful measures in the project;
- Section 3, Human rights, offers an initial evaluation of relevant legal instruments in the field of human rights and presents a preliminary discussion and evaluation of possible effects to fundamental rights in ENACT;
- Section 4, Data Protection Framework, develops an overview of the EU Data Protection Framework, considering regulations on personal and non-personal data, and Artificial Intelligence, highlighting obligations and principles to be observed in ENACT, since the non-compliance with these rules may lead to risks in the project;
- Section 5, Cybersecurity, goes about the cybersecurity legal rules, risks, obligations and principles that should be considered by the project, which will lead to a future further assessment of cybersecurity risks.

## 1.4 Intended Audience

This Deliverable is direct to the full public, especially for highlighting considerations around the re-use of ENACT's outputs and limitations to incompatible re-use. D1.3 is relevant, in particular, to all ENACT partners, establishing minimal requirements for the work to be developed in the project. This report is also intended to reach other research projects, aiming to serve as reference for certain practices and to also receive feedback from all the content here presented. Finally, the present analysis is also a relevant document for the members of the project Ethics Advisory Board (EAB). Considering this broad intended audience, this report is public and open to access via the project's website and research repositories, such as the KUL library.

# 2 Legal and Ethical Analysis

ENACT aims to establish a knowledge hub for providing resourceful information for actors of the FCT R&I system. A knowledge hub can be understood as an institution or network "dedicated to capture, share and exchange development experiences with national and international partners, in order to accelerate development"[2]. So, a knowledge hub can be defined as a tool or space for sharing information and resources about a certain domain to interested stakeholders[3]. In ENACT, this means moderating and aggregating information to provide inputs for various actors about the domain of FCT.

As a knowledge hub, ENACT will be part of a data ecosystem, where different parties take part on data sharing [4]. This scenario requires the observation, consideration and implementation of different legal and ethical principles, norms and instruments since data sharing occupies such a relevant place in today's society. Since it is a research project, ENACT will also consider the best practices for research activities, evaluating and implementing crucial principles and complying with rules of access and dissemination. Finally, as a project involved in the FCT topic, ENACT will also consider specific guidelines and norms for knowledge handling in this domain, ensuring that relevant information is available for various actors.

## 2.1 Methodology

For achieving results that are ethical and legally compliant, ENACT will establish methods for adopting ethics-by-design, active and effective considering and implementing legal requirements. While it is essential to bear in mind that ENACT will not develop any technologies or tools, the project understands the importance of considering ethical aspects in all outputs developed. ENACT is not working with 'big data', as only a limited and controlled amount of information is used for the project's goals and deliverables. Nevertheless, understanding the importance of data for public governance, including in the field of FCT, to allow data-driven policy decisions, the project will apply the Data Ethics Decision Aid (DEDA) framework to the extent applicable to ENACT. The DEDA framework is accepted and applied by different entities, especially public ones, what is valuable for ENACT's involvement in the FCT domain. This methodology proceduralises considerations about AI use, data sources, anonymisation, access, responsibility, transparency, and privacy; topics that are also essential for ENACT.[5] An initial exploration and analysis of these themes is already presented in this Deliverable. However, evaluation on these topics and other points connected to DEDA will continue throughout the project and will be presented in future deliverables due in the end of each cycle of the project under WP2 and WP3.

Since the proposal stage, ENACT has been taking into consideration the relevant legal framework that applies to the project, the research best practices, and ethics guidelines and

---

[2] The Bali High-Level Meeting on Knowledge Hubs. (2012). **Bali Communiqué 2012**.
[3] European Commission Pact for Skills Knowledge Hub, available at: https://pact-for-skills.ec.europa.eu/community-resources/knowledge-hub_en
[4] Data Spaces Support Centre. (2023). DSSC Glossary – Version 1.0. Online Report. March 2023.
[5] FRANZKE, A. S.; MUIS, I.; SCHÄFER, M. T. (2021) 'Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands.' **Ethics and Information Technology,** 23:551-567.
DEDA, **Poster**, retrieved from: https://deda.dataschool.nl/en/poster/.
DEDA, **Handbook**, retrieved from: https://deda.dataschool.nl/en/handbook/

good practices. A continuous monitoring of these aspects is foreseen in the project, being this Deliverable the first version of the analysis, that will count with updated versions in the end of each cycle of the project (version 2, part of D2.1, due on M12; version 3, part of D3.1, due on M36). Continuous observation and implementation of ethical and legal aspects is central for a broad acceptance and usefulness of the products developed in ENACT.

Understanding the need to guarantee a good level of acceptance by society, while also promoting a useful and effective instrument, ENACT will follow the Responsible Research and Innovation (RRI) approach. This process considers the societal needs and the public interest in the development of scientific and innovative solutions[6], developing results that are socially and ethically acceptable, while producing a positive impact in society and relevant stakeholders. While RRI in practice can have many different applications[7], it is possible to observe four common characteristics in RRI approaches[8]:

1. **Engagement** (or inclusiveness, involvement of society)
2. **Anticipate** (assessing at an early stage in the research and innovation lifecycle the benefits and risks)
3. **Reflect** (reflecting on values and beliefs during the research and innovation lifecycle)
4. **Act/Response** (the capacity to respond to changes and amend routines, structures and systems to accommodate novel insights)

This interactive process requires a multidisciplinary involvement of various societal stakeholders throughout the whole research development[9]. In ENACT, the engagement will be established by different forms (e.g., interviews, participation in events, engagement with external specialists), to guarantee that the research partners can have a good understanding of the possible needs of society, considering different social groups. Even though ENACT will not produce a new technology *per se*, it is a goal of the project to guarantee that the knowledge hub platform creates positive effects to society, considering regulations, risks, ethics and responsibility.

To guarantee expert feedback on ethical matters, ENACT counts with a dedicated Ethics Advisory Board (EAB). Composed by three independent specialists, this body provides comments and suggestions to project's activities that may have societal impacts. In the first phase of the project, all deliverables were presented to the body to ensure that they would

---

[6] UK Research and Innovation. (2023). **Framework for Responsible Research and Information**. Available online at: https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/framework-for-responsible-innovation/#:~:text=Responsible%20research%20and%20innovation%20is,undertaken%20in%20the%20public%20interest.

[7] Sutcliffe, H. (2011). A report on responsible research and innovation. **MATTER and the European Commission;**Rip, A. (2014). The past and future of RRI. **Life Sciences, Society and Policy 10**(1), 17;
Taebi, B., Correlje, A., Cuppen, E., Dignum, M., & Pesch, U. (2014). Responsible innovation as an endorsement of public values: The need for interdisciplinary research**. Journal of Responsible Innovation**, 1(1), 118-124.

[8] Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D., (2013). A framework for responsible innovation. **Responsible innovation: managing the responsible emergence of science and innovation in society,** 31, 27-50.
DARLENE. (2022). D7.4: Legal and ethical assessment – 1st version.

[9] Von Schomberg, R. (2013). A vision of responsible research and innovation. In R. Owen, J.R. Bessant and M. Heintz (Eds.), **Responsible innovation: Managing the responsible emergence of science and innovation in society** , pp.51–74.

have a complete overview of the project's activities, including the functioning of the Observatories and the development process of reports. From this engagement, the Deliverables already developed were revisited and updated to guarantee more clarity on certain aspects, such as the handling of personal information and what the security and the ethics reviews entail.

Beyond that, via the different dissemination activities, including the project's annual event, the consortium intends to incorporate the feedback received from different stakeholders engaging with the project's outputs. Stakeholders involved in these activities include law enforcement offices, policy makers, public servants, academics and, to a certain degree, technology developers. Ongoing engagement with these actors will also be made possible via the communication channels developed by ENACT, including the possibility of requesting specific outputs.Anticipation in ENACT will be closely linked to the legal and ethical analysis reports and the DMP, which will be presented in different stages of the project. The reports and Deliverables will be used as channels to showcase the result of analysis of possible risks related to ENACT's activities. For the anticipation stage, published guidelines, best practices, media publications and research results will be considered to evaluate the chances of any risk developing by the project's activities. For this, ongoing exchange with other partners involved in the project is necessary. The bi-weekly general assemblies will be the main channel for this communication, while extraordinary meetings or e-mails will also be used to discuss potential risks that may arise from the project. By discussing updated and changes on methodology and approaches, the anticipation of risks will be kept up-to-date and documented yearly in Deliverables.

The engagement stage will also be essential to think before any materialisation of potential risks. An example of anticipation is the analysis of possible misuse of ENACT's outputs (see section 3.5). The effort of the present Deliverable thoroughly illustrates the need to anticipate possible negative effects in an early stage of the research project. Findings of the initial assessment will be further detailed and complemented in future versions of the report. Nonetheless, it is via the early analysis of possible risks, limitations and obligations that it will be possible to achieve results that are compliant-by-design.

For this, it will be crucial to define points of attention and priorities to be considered by partners in the project via a group reflection on ethical and legal values. Additionally, existing guidelines and research serve as an initial point for critically reflect on the best use and application of knowledge, by ethical and open access considerations, but also by understanding limitations of handling data for FCT purposes. Contemplate the apparent duality between open data and research, and FCT and public interest/security may contribute to the complex policy framework on the topics.

With the close interaction between partners, it will be possible to guarantee that action will be taken whenever good practices or mitigation measures should be in place to guarantee the best use of the research results. Having an ongoing assessment of risks and effects is also crucial to guarantee that the proposed solutions are tested in an environment where they can be reconsidered and updated, which will be applied in ENACT. In other words, a proposed mitigation measure should also be evaluated once it is put into force. In case it presents new risks or effects not yet foreseen, it can be modified to better address the purposes of the project.

Reflectiveness will be essential for aligning the project with the pillars and values directing ENACT. After the engagement with society, users, innovators, and other members of the FCT Community, it will be possible to elaborate and understand how to best apply their considerations. This moment will allow for the response and actions emerging from this interactive cycle to be suitable for the project's goals. ENACT must continue to consider that the project's outputs are aimed at different actors members of the FCT R&I community, including LEAs, policy-makers, members of the academic sector, among others.

To exemplify the value of the RRI approach for ENACT, even though the project is not developing a technology tool, a mapped aspect can be mentioned. ENACT's observatories intend to serve as initiatives for knowledge gathering, classification and dissemination, allowing for the use of this existent information for the development of more research and useful outputs. However, the work developed in the observatories is sometimes mistaken by the project's internal management. So, for instance, the Ethical, Legal and Societal Observatory (ELSO) does not develop any specific assessment of the project's activity or of any specific innovation solution. Nevertheless, the Observatory is the means for the insertion of ELS considerations on ENACT's products such as Flash or Advanced Reports. From the observations added to this repository, is possible to draw certain trends in ELS matters in the FCT R&I community. On the other hand, the project's partners involved in the ethical, legal and societal assessment activities evaluate the project's activities in itself, not the content of the observations part of the ELSO. This report is an example of the internal ethical and legal management. From this understanding, ENACT's outputs will work on highlighting such difference, ensuring that each output serves for its purpose.

# 3 Human rights

Assessing the possible effects of a project in human rights is a particularly important step in the development of an ethical research project. Human rights set limitations (negative obligations) and (positive) obligations to different actors, including public bodies and States. Negative obligations can be understood as a duty not to act (e.g., a State should not interfere in someone's privacy unless the surveillance measure is proportional and there is a legal provision for it), while positive obligations are required actions[10] (e.g., a State should establish mechanisms to guarantee the existence of redress mechanisms for individuals to complain in cases where they find there was an unfair interference to their fundamental rights). These obligations do illustrate shared values between nations, establishing ethical rules of behaviour, setting obligations and limits to the action of societal stakeholders (public or private). This system derives from the fact that these rights are protected and guaranteed to all human beings, regardless of their characteristics[11], making it mandatory for all society to protect and observe them[12].

Playing an essential role in national and international law, several legal instruments structure the ideas behind fundamental rights. For this assessment, three main instruments will be considered. The first is the Universal Declaration of Human Rights (UDHR), a non-binding norm adopted in 1948 as a result of the United Nations actions[13]. Second, the European Convention on Human Rights (ECHR), adopted in 1950 by the Council of Europe (CoE) and binding to its members[14]. Last, a more recent instrument, the European Union Charter of Fundamental Rights (the Charter), a binding instrument adopted in 2002 by the EU[15].

Although these instruments do not represent the whole system of protection to human rights, they foreshow the essence of the core fundamental rights to be considered by ENACT. Nonetheless, whenever necessary and relevant, other instruments will also be considered

[10] UNODC. Positive and negative obligations of the State. Available at: https://www.unodc.org/e4j/zh/tip-and-som/module-2/key-issues/positive-and-negative-obligations-of-the-state.html#:~:text=Negative%20obligations%20refers%20to%20a,by%20the%20corresponding%20negative%20obligation.

[11] See Article 2 of the Universal Declaration of Human Rights.

[12] Article 1 of the European Convention on Human Rights establishes that "the Hight Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention".

[13] United Nations. (1948). **Universal Declaration of Human Rights**. 10 December 1948. Online version available at: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

[14] Council of Europe. (1950). **European Convention on Human Rights.** 4 November 1950. Online version available at: https://www.echr.coe.int/documents/d/echr/convention_eng

[15] European Union. (2012). **Charter of Fundamental Rights of the European Union**. 26 October 2012. Publication online available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT

(e.g., Convention 108 by the CoE[16], International Covenant on Economic Social and Cultural Rights[17], International Covenant on Civil and Political Rights[18]).

Important to highlight that fundamental rights will be used as a synonym to human rights. Even though fundamental rights are usually applied in a specific EU context, being found in constitutional discussions, while human rights are mainly applied in the international context, both expressions illustrate the essence of the rights being discussed and evaluated in this Deliverable[19].

Cooperation between public bodies is a crucial step in the fight against crime and terrorism in Europe. ENACT aims to contribute to this goal by conjugating several sources of information that then can be used by different actors for several purposes, but, mainly, the FCT R&I community. Nonetheless these purposes are aligned with the public interests of the Member States, ENACT and any other activity within the EU must respect and observe the human rights.

In spite of their central role in the judicial system, fundamental rights are not absolute. By adopting proportionate means, for legitimate aims, with legal certainty, and following specific case-by-case requirements, an interference to a fundamental right may be legal. This follows a case-by-case approach, which may elucidate apparent conflicts of rights and is the basis for several judicial decisions by courts evaluating the protection of human rights (e.g., ECtHR). From the already established case-law is possible to delimit legitimate reasons that justify certain level of interference to fundamental rights.

The Fight against Crime and Terrorism (FCT) is one of EU's top priorities, serving for a public interest of national and public security[20]. Since 2015 attacks, it became clearer that a joint international approach is needed for combating terrorism and serious crimes[21], requiring

---

[16] Council of Europe. (1981). **Convention 108**. Convention for the Protection on Individuals with regard to Automatic Processing of Personal Data. Online publication available at: https://rm.coe.int/1680078b37

[17] United Nations. (1976). **International Covenant on Economic Social and Cultural Rights**. Online publication available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

[18] United Nations. (1966). **International Covenant on Civil and Political Rights.** Online publication available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[19] European Union Agency for Fundamental Rights. **What are fundamental rights?** Publication online available at: https://fra.europa.eu/en/content/what-are-fundamental-rights#:~:text='Fundamental%20rights'%20expresses%20the%20concept,is%20used%20in%20international%20law.

[20] European Council. (2023). **The EU's response to terrorism**. Available online at: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/.
European Council. (2024). **The EU's fight against organised crime**. Available online at: https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/#:~:text=The%20EU%20is%20taking%20action,on%20asset%20recovery%20and%20confiscation.
European Parliament Multimedia Centre. (2015). **Europol: fighting crime and terrorism in Europe**. Available online at: https://multimedia.europarl.europa.eu/en/video/europol-fighting-crime-and-terrorism-in-europe_N005-151130-001

[21] European Council. **Statement by the members of the European Council.** Informal meeting of the Heads of State or Government. Brussels, 12 February 2015. Available at:

effective and timely data and knowledge sharing. It is clearly understood that the fight against crime and terrorism is a legitimate aim which might justify a proportionate interference in someone's fundamental rights. Since an antiterrorist operation presents different stages (surveillance phase, arrest, and punitive phase), various rights may be affected during one operation or one policy[22]. It is also relevant to underline that each of these stages pose different levels of intervention to rights. Thus, the means used in different stages must justify the severity of inference accordingly to ensure that said interventions are proportional.

ENACT aims at developing a tool useful for the establishment of tendencies and insights in the FCT domain, but with a main focus on the research before any of the stages of an antiterrorist operation. However, this does not mean that human rights are not affected by ENACT actions and results. Considering the close relationship with the FCT stakeholders, the project must consider possible effects to fundamental rights in the implementation and use of the knowledge hub. On this note, it must be noted that ENACT's main purposes are not directly linked to antiterrorist operations, but more to an initial phase in the FCT, beyond other uses of the knowledge structured by the project (e.g., development of the EU market, creation of policies). Thus, the aims related to the project are legitimate, from the FCT to the research or to the economic development within the domain of FCT. Nonetheless, it is part of the legal and ethical analysis of the project to considerate mitigation measures and to evaluate if the risks and effects are proportionate to the goals pursued in the project.

Even though all fundamental rights are going to be considered throughout the lifetime of ENACT, this first analysis will focus on the ones that have a direct connection to the activities of the project, namely: (a) non-discrimination; (b) access to information; (c) privacy; (d) data protection; and (e) risks of misuse. The following analysis presented in the next annual Deliverables under the subsequent WPs will further address foreseeable impacts and mitigation measures of the project in fundamental and human rights. A full Fundamental Rights Impact Assessment (FRIA) will not be performed, since ENACT will not develop any technology *per* se. Nevertheless, considerations on the protection and promotion of rights still remain of utmost importance for the project. From this, considerations on possible impacts and negative effects from the project will guide the work done by the consortium, especially the legal and ethical partners. Lesson from already developed methodologies of FRIA, such as the ALIGNER project[23] and the Netherlands government[24], will be applied to the extent relevant to the project. Evaluation of potential effects of fundamental rights will focus on possible consequences connected to the outputs produced by ENACT, namely the Flash and Analytical Reports, Stakeholders Map, and Structured Knowledge Repository, with special attention to possible misuse.

---

https://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/

[22] Council of Europe. (2022). **Guide to the case-law of the European Court of Human Rights - Terrorism**. Published online at: https://www.echr.coe.int/documents/d/echr/Guide_Terrorism_ENG

[23] ALIGNER. 'Fundamental Rights Impact Assessment – FRIA', retrieved from: https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

[24] Netherlands. 'Impact assessment fundamental rights and algorithms', retreived from: https://www.government.nl/binaries/government/documenten/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms/fundamental-rights-and-algorithms-impact-assessment-fraia.pdf

## 3.1 Non-discrimination

As already mentioned, fundamental rights apply to everyone, regardless of any specific characteristic. So, non-discrimination of persons is intrinsically embedded by human rights. Specifying the right to non-discrimination, the Article 7 of the UDHR establishes that “all are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination”.

In the ECHR, non-discrimination is repelled by Article 14 – Prohibition of discrimination, which sets that “[t]he enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground (…)”. During the first five decades of the Convention, this Article was considered unclear, with a limited scope, which lead to a lack of application of said provision by the EctHR. For this reason, Protocol 12 was established, making it clear that the list of bases for discrimination is non-exhaustive and will rely on Court understandings for establishing if an action is discriminatory or not[25].

While in a European level, the right to non-discrimination is established by Article 21 of the Charter as the following:

> 1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited;
>
> 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

Activities foreseen by ENACT may leave room for discriminatory actions, especially the ones part of the Networking Pillar of ENACT, which will count with open calls for validation and advanced research. Since there will be a dispute between external stakeholders for fulfilling a spot, it is crucial that objective requirements and criteria are established beforehand without benefiting or harming any specific group or person. This type of action cannot be considered as a breach of the right to non-discrimination because the criteria are well justified and are set for real and legitimate reasons (e.g., need for specialists, budget limitation). Underlying this risk since the beginning of the project is crucial to guarantee that this will be considered in the development of ethical criteria and procedures for this action. Thus, ENACT will adopt reasonable and pertinent requirements for said open calls. Also, additional inputs from the EAB may be requested for the creation of these actions in the most adequate manner.

It is important to notice that Article 14 of the ECHR “complements the other substantive provisions of the Convention and the Protocols.” [26] In the context of ENACT, the non-discrimination is highly connected to the right to access information. As established by the

[25] Arnadóttir, O. M. (2002). **Equality and Non-Discrimination under the European Convention on Human Rights.** Brill .
[26] ECtHR. **Rasmussen v. Denmark,** 28 November 1984, p. 29.

Open Data Directive[27], public actors must ensure non-discriminatory conditions for the re-use of public sector information[28]. However, as it will be further explored in the future versions of this Report, ENACT will manage different datasets, including some that may contain information that require a more controlled or even restricted access. This does not automatically breach the right to non-discrimination, since "Article 14 does not prohibit all differences, but only those differences based an identifiable, objective or personal characteristic, or "status", by which individuals or groups are distinguishable from one another."[29].

So, it is possible that throughout the development of the project, there might be a level of discrimination between the users of the ENACT's knowledge hub. These distinctions will be based solely in aspects related to the information, meaning that only restricted information will not be accessible for all the users, and this will only take place when a proportionate reason applies (e.g., national or public security), following the understanding of the Law Enforcement Agencies (LEAs) and experts that will contribute to the project. In this sense, the eCtHR already established that "[b]ecause of their direct knowledge of their society and its needs, the national authorities are in principle better placed than the international judge to appreciate what is in the public interest on social or economic grounds, and the Court will generally respect the legislature's policy choice unless it is "manifestly without reasonable foundation"[30]. Thus, ENACT will follow this understanding, while respecting the right to non-discrimination.

## 3.2 Access to information

The right to access to information is seen as a means to achieve other objectives, especially the right to freedom of expression, since one must be able to receive information to formulate their own opinions. So, the right to freedom of information is a core principle of democracy.[31] Article 19 of the UDHR establishes that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".

In the same sense, the ECHR sets under the right to freedom of expression[32] that "[t]his right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." Nonetheless, the following Article 10(2) limits the right to freedom of expression and access to information setting that:

> "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the

[27] 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.
[28] Recital 20 of the Open Data Directive.
[29] ECtHR. **Khamtokhy and Aksenchik v. Russia**, 24 January, 2017, p. 64.
[30] ECtHR. **Carson and Others v. The United Kingdom**. 16 March 2010. P. 61.
[31] Blanke, H.-Josef., & Perlingeiro, Ricardo. (Eds.). (2018). **The Right of Access to Public Information: An International Comparative Legal Survey** (1st ed. 2018.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-55554-5
[32] Article 10(1) of the ECHR.

> protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

With the same text as the ECHR, the Charter sets the right to freedom of expression and information in its Article 11. However, the right to access information, in the European level, is completed by a different provision. As a close connection to the Open Data Directive, Article 42 of the Charter establishes that "[a]ny citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to documents of the institutions, bodies, offices and agencies of the Union, whatever their medium". This provision allows a bigger oversight over the activities of national authorities, reaffirming the role of transparency in democracy and in the protection of fundamental rights.[33]

ENACT aims to ensure and positively affect the right to information, making already produced knowledge more accessible to different stakeholders. Limitations to the right to freedom of information will only be established whenever there is a legitimate aim (see 3.1), especially in the interests of national security, public safety, or for the prevention of disorder or crime, as long as these restrictions are prescribed by law are necessary in a democratic society[34]. Also, as already highlighted by the eCtHR "while there is no doubt that the public may be interested by a wide range of subjects, this fact alone cannot suffice to justify confidential information about these subjects being made public"[35].

So, ENACT will work on finding proportionality between providing and reinforcing the right to information and transparency and the observation of criteria of confidential information, also considering the requirements for limitation of any fundamental right or freedom (lawfulness, respect of the essence of rights, necessity and proportionality)[36]. (see 3.4) For this, the ethical partner (KUL), will be involved in the oversight of the uploaded information in the Knowledge Repository, checking when data is classified as restricted without a reasonable justification and if data that should be restricted is not flagged as such. In the next versions of this report the interplay between this classification and content moderation and the FCT Security Taxonomy will be further developed.

ENACT faces an obstacle. A variety of sources are used for outputs development. ENACT, however, has no management power towards these sources. In case the project receives any request regarding access to information, it will not be necessarily possible to provide access to the full content of the material added to the Knowledge Repository. For instance, in case of media and news material where a paywall is placed, ENACT will not provide access to the full content to not go against the policies in place. The same goes for other materials, such as research results, that also do not follow an open access policy. The project, however, will respond to requests of access to information by providing the direct link to the source of the observation. Whenever ENACT receives a request for accessing information, this will be evaluated and responded within a month since the day the project receives the information.

---

[33] Blanke, H.-Josef., & Perlingeiro, Ricardo. (Eds.). (2018). **The Right of Access to Public Information: An International Comparative Legal Survey** (1st ed. 2018.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-55554-5

[34] ECtHR. **Goodwin v. The United Kingdom.** 27 March 1996.

[35] ECtHR. **Halet v. Luxembourg.** 14 February 2023. P. 144.

[36] Article 52(1) of the Charter

Finally, it is crucial to notice that following the RRI approach, the ENACT knowledge hub will have a space for receiving suggestions of content and for the possibility of engagement with different actors of society, including the viability of receiving requests to access information classified as restricted.

## 3.3 Privacy

The fundamental right to privacy was first autonomously described still in 1890, with the right to be left alone. So, since the beginning of the discussion about the right to privacy, the *erga omnes* effects of this right were supported by the comprehension of the importance of having control over the private space[37]. With the development of the concept of privacy, it was put into a contextual connotation, bringing light into the understanding that the right to privacy brings the need for negative and positive obligations to ensure that the individual may maintain the control over their own information.

Although the right to privacy was explicitly referred in Article 12 of the UDHR[38], in European laws, the right to privacy was understood as the right to respect for private life.[39] So, in the EU level, privacy is not mentioned neither in the Charter or in the ECHR. In the Charter, privacy is foreseen in Article 7, which mentions that "Everyone has the right to respect for his or her private and family life, home and communications". Even without mentioning the word privacy, Article 8 of the ECHR is a truly relevant provision, since while protecting the right to respect for private and family life, already sets limits to this right, providing the requirements for situations that will allow the interference to said right:

1. Everyone has the right to respect for his private and family life, his home and his correspondence;
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The legal provision establishes that for an interference to someone's privacy, it must: (i) be in accordance with the law; (ii) pursue a legitimate aim; and (iii) be proportionate to the aim pursued[40]. The right to privacy, then, protects the individual of any illegitimate interference to their private land, family life, home or communication. Negative consequences of an action interfering with someone's private life must be proven by the right's holder, which includes an initiative that affects someone's privacy without complying with the requirements established in Article 8 of the ECHR.

---

[37] Warren, S. D.; Brandeis, L. (1890). The Right to Privacy. **Harvard Law Review**, vol. IV, no. 5, 1890.
[38] Article 12 of the UDHR: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.".
[39] European Union Agency for Fundamental Rights. (2018). **Handbook on European Data Protection Law**. Luxembourg. Publications Office of the European Union.
[40] ECtHR, Press Unit. (2022). **Factsheet – Mass surveillance**. September 2022. Available in: https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

No specific interference with privacy is initially foreseen by the proposed activities in ENACT. However, some interference to data protection is planned. Considering privacy's close connection with data protection, the requirements established by Article 8(2) ECHR must be observed whenever there is processing of personal data in ENACT, especially taking into account that the mentioned article is used as a basis for the eCtHR evaluating the legitimacy of data protection issues. This need for compliance is even clearer when one notices that the requirements established in Article 8 of the ECHR are remarkably similar to the ones mentioned in the Charter for any interference to fundamental rights[41] (see 3.4).

## 3.4 Data protection

Although currently it is commonly understood in Europe that the right to privacy and the right to data protection are autonomous rights, this was not the case in older instruments. Formerly, data protection was not understood as an essential fundamental right since the risks of data processing were minor. Processing was not automatic, and the amount of data collected and maintained by each entity was not so relevant. However, this idea is continuously changing with the establishment of the information society and information economy, which bring different risks to individuals. From this understanding, previously instruments were reinterpreted so that the right to privacy would also embrace the right to data protection.

In an international level, for example, the UN does not recognize personal data protection as a fundamental right, only mentioning privacy in Article 12 of the UDHR[42], unlike the Treaty on the Functioning of the European Union (TFEU) which stipulates data protection as a separate and autonomous right as further detailed below. However, a Special Rapporteur on the right to privacy was established, which included the impact of new technologies, and a non-binding resolution focusing on limiting intelligence surveillance and companies' abuse on the use of technologies and personal data was adopted[43].

For the CoE the case-law of the European Court of Human Rights (eCtHR) played an imperative role for the understanding that the Article 8 of the ECHR[44] also covers data protection. And, although not subject to the overview of the eCtHR, the Convention 108[45] was also crucial for the establishment of data protection as an autonomous fundamental right. Relevant principles[46] are provided by this Convention such as: (i) quality of data; (ii) fairness; (iii) necessity and (iv) minimization. This regulatory framework already makes a distinction

[41] Article 52(1) of the Charter.
[42] Article 12 of the UDHR: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.".
[43] European Union Agency for Fundamental Rights. (2018). **Handbook on European Data Protection Law**. Luxembourg. Publications Office of the European Union.
[44] Article 8 of the ECHR, Right to respect for private and family life: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.".
[45] CoE. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**Convention 108**).
[46] Article 5 of Convention 108.

between sensitive data[47], bringing a higher level of protection to this category, and also establishes the need for establishing measures for guaranteeing the data security[48].

More recently, in 2018, a modernised protocol for Convention 108 was developed, with provisions closely related to modern society's need, commonly known as Convention 108+.[49] This new protocol complements the list of principles, mentioning, for example, the need for transparency actions from the data controllers[50], additionally establishing a list of rights of the data subject[51]. It is worth also highlighting the more detailed provision regarding the role of supervisory authorities in the data protection system[52]. Other international bodies also have an active and relevant role in the data protection ecosystem, as the Organisation for Economic Cooperation and Development (OECD), which has published different studies and guidelines on the domain of data protection.

In a European level, history developed differently. Since the 1970s States have put into force specific data protection norms, understanding the potential risks that the organized processing of personal information could arise, forming the first generation of data protection laws[53]. From this understanding, the need for a general norm on data protection became clear[54], making space for the creation of the Directive 95/46/EC[55]. This Directive represents an initial effort for a bigger harmonization of the level of data protection in Europe. Nonetheless, the mentioned Directive was replaced by the GDPR in 2018.

After this initial legislative movement, personal data became part of some of the most relevant norms of the EU, here mentioned: the Treaty on the Functioning of the European Union (TFEU)[56] and of the Charter. In the first, data protection is established by Article 16, which states that "Everyone has the right to the protection of personal data concerning them". In the latter, Article 8 of the Charter reaffirms the autonomous right to personal data protection in Article 8, which establishes that:

1. Everyone has the right to the protection of personal data concerning him or her;
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified;

[47] Article 6 of Convention 108.
[48] Article 7 of Convention 108.
[49] CoE. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (**Convention 108+**)
[50] Article 5(4)(b) and Article 8 of Convention 108+.
[51] Article 9 of Convention 108+.
[52] Article 15 of Convention 108+.
[53] Doneda, Danilo. (2019). O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco.
[54] Mendes, Laura Schertel. (2014). **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva.
[55] European Union. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 23 November 1995.
[56] European Union. (2012). **Consolidated version of the Treaty on the Functioning of the European Union**. 26 October 2012.

3. Compliance with these rules shall be subject to control by an independent authority.

It is crucial to understand that the data protection framework does not intend to prohibit the data flow but aims on ensuring that the data subject has control over the use of their data. So, reaffirming the non-absolute perspective of the right to data protection, the Article 8 above already sets rules for a legitimate processing of data, these being: (i) fairness; (ii) specific purpose; (iii) consent or another legitimate legal basis.

Past the specific requirements of processing data protection in the Charter, ENACT should also consider the generic rules set for any interference to fundamental rights. Article 52(1) of the Charter stipulates:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

This means that any activity from ENACT that may limit a fundamental right must:

- Be in accordance with the law;
- Respect the essence of the fundamental rights and freedoms;
- Be proportionate and necessary to the general interest or to protect the rights and freedoms of others.

## 3.5 Misuse

According to the Cambridge Dictionary, misuse is “to use something in an unsuitable way or in a way that was not intended".[57] On the context of research, misuse can be understood as the use of research results for unethical purposes, such as terrorist or criminal activities or against human rights, safety of people, animals or the environment.[58]Following the European Commission Guidance Note on Potential misuse of research, identifying potential misuse entails considering any possible misuse, evaluating the risks associated with the planed research and possible unethical or malevolent ways which the research and its results could be used.[59]

ENACT foresees different types of results, namely: flash and analytical reports, stakeholders map, and knowledge repository and structured knowledge base. In this topic, considerations

[57] Cambridge dictionary. **Misuse**. Online. Retrieved from: https://dictionary.cambridge.org/dictionary/english/misuse

[58] VLIR (2022). **Guidelines for Researchers on Dual Use and Misuse of Research.** Retrieved from: https://vlir.be/wp-content/uploads/2022/10/VLIR-Dual-Use-2022-EN.pdf

[59] European Commission. (2021). **Guidance note – Potential misuse of research**. EU Grants: Potential misuse of research: V2.0. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf

about possible misuse of all of these outputs will be drawn. As the project evolves, new evaluations can be brought to the table and, if necessary, mitigation measures should be added. As ENACT's goals involve the promotion and dissemination of knowledge in the FCT domain, facilitating the access of already developed knowledge, and appointing to trends and gaps, the evaluation will evaluate if the project's results could be used for other, incompatible purposes.

### 3.5.1 Stakeholders map

ENACT's Stakeholders map support and facilitate a networking environment for all pillars of the project, with a specific focus on the **networking** pillar. D4.1 details the functioning of this output, explaining that ENACT "will neither connect with every single stakeholder nor absorb as many as possible under its direct constituency. Its strategy is to connect the project with the main, and already existing, Knowledge Hubs and organisations from the FCT ecosystem."[60]

As further detailed in the following sections, the public version of the stakeholders map[61] does not contain any direct personal data, portraying information about legal persons only. Under an evaluation of possible misuses, two main risks were already mapped: (1) identification of individuals by combining information presented in the ENACT's stakeholders map, revealing personal information; and (2) facilitating the mapping of entities and persons involved in the FCT domain, facilitating possible attacks, in a broad manner.

Regarding the first risk, it is relevant to highlight that ENACT already implemented mitigation measures to avoid the direct offering and processing of personal information. No direct identifier of a person is provided in the stakeholders map. While it is the project's role to mitigate the further incompatible use of the information provided, ENACT cannot be hold responsible for all further use of the information, including to identify individual persons. Considering that this risk was mapped during the second cycle of the project, new mitigation measures must be put into place to clarify the limits imposed to further use of the information presented in the map.

In the same sense, the second possible misuse follows a similar idea. Either way, aiming to dimmish these risks, ENACT is working with publicly available information and the classification into the categories is made in a broad manner. Similarly to the first risk, new mitigation measures must be put into place to clarify the limits imposed to further use of the information presented in the map.

### 3.5.2 Knowledge repository and Structured Knowledge Base (SKB)

As detailed in D4.1, "ENACT's observatories will collect, classify, aggregate, curate and process information pertinent to each observatory in a Structured Knowledge Base (SKB) and appropriately disseminate them to interested parties through a dedicated Knowledge Repository (KR). Although the terms may be used interchangeably in some occasions, it is important to clarify and distinguish the two terms. To this end, the Structured Knowledge Base (SKB) pertains to the classified and processed outputs of ENACT's Research Pillar and its

[60] ENACT. **D4.1 Network methods and tools**.
[61] ENACT. **ENACT FCT Stakeholder Map and Structured Knowledge Base.** Retrieved from: https://enact-eu.net/enact-fct-stakeholder-map/

observatories, while the Knowledge Repository (KR) is the digital container in which the SKB will reside."[62]

One must consider the possibility of unethical or non-compliant tools being aggregated and further disseminated in the ENACT's knowledge repository. A risk connected to this possibility emerges as an user could understand that a tool or observation featured in the knowledge repository is recommended or endorsed by the project. This is not the case. ENACT does not intend to present or provide an assessment of compliance or readiness from any of the tools or observations added to the knowledge repository. In reality, the project intends to further disseminate results and illustrate the current state of the market without making specific assessments on readiness and compliance of any of the observations. To mitigate this risk, more clarification on the matter must be provided. This possible risk was highlighted by the EAB in its first report (D11.1). To mitigate it, a note will be implemented into ENACT's website to highlight that the observations added to the SKB should not be understood as endorsed by the project and that no assessment of readiness or compliance was done by the project.[63] Any responsibility towards the use of any technology displayed is solely for the developers or deployers of said solutions.

The same considerations apply for AI technologies that may be classified under the unacceptable risk category of the AI Act.[64] Article 5 of this Regulation prohibits certain practices, which some could be relevant to the FCT sector. Also, projects prior to the AI Act could have developed technologies that are now prohibited by this norm. ENACT is not making a specific analysis of the compliance of the observations and tools portraited in the SKB, including no specific assessment of compliance with the AI Act is performed. From this, the same considerations listed above should be considered in the AI Act context.

Currently, the SKB does not count with any specific classification on the ethical readiness or legal compliance of the observations there added. The partners are, nonetheless, evaluating the viability of adding dedicated classifications to translate these information. In either case, this will not change the responsibility of the ENACT project.

### 3.5.3 Flash and Analytical Reports

Flash reports are results of summaries of observations collected and classified for the composition of the knowledge repository. Analytical reports, on the other hand, are in-depth research reports performed either by ENACT partners or by external specialists. Considerations on misuse of these Reports follow a similar rationale from the Knowledge Repository and the SKB, since the reports originate from the content present in these instruments. As pointed out, ENACT must clarify that the dissemination of any content does not translate into endorsement and should not be read as such. Also, no specific evaluation on the ethical readiness or legal compliance of the observations is provided until the moment.

---

[62] ENACT. D4.1 Network methods and tools.
[63] ENACT. **ENACT FCT Stakeholder Map and Structured Knowledge Base.** Retrieved from: https://enact-eu.net/enact-fct-stakeholder-map/
[64] European Commission (2024). **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).** OJEU, 12.7.2024.

However, the Analytical Reports may be an important opportunity to develop further research on these matters.

### 3.5.4 Dual-use considerations

Dual-use results are those that may be used for both civil and military purposes. For this, ENACT understands the lack of a common definition of 'dual use; in the context of R&D support, what creates certain challenges.[65] ENACT's results do not raise specific concerns on possible dual-use, with risks more connected to the idea of misuse as presented in the previous topics. Because of this, no specific considerations or mitigation measures are foreseen at the moment for ENACT's results.

As the Structured Knowledge Base and the Reports may feature observations and tools that present a dual-use, the note to be added in the website page on the knowledge repository should also emphasise this notion. Additionally, links to relevant materials on the matter, such as the VLIR Guidelines for Researchers on Dual Use and Misuse of Research[66] and the European Commission Guidance, will also be added. [67] ENACT must clarify that portraying and disseminating any information does not translate into endorsement and the project holds no responsibility for the observations presented.

In the future, the project will evaluate if adding new categories into the SKB to highlight possible dual-use risks is viable and increases the potential of this result. Such solution may also translate to further details on possible dual-use risks also on the Reports produced by or for the project. For this, ENACT partners are currently discussing ways to use the EU's list of dual-use technologies,[68] alongside NATO STO considerations on the matter,[69] to find ways to highlight dual-use potential of observations added.

# 4 Data Protection Framework

In a data-driven society and economy, knowledge became one of the most relevant assets one may have. Data are interesting assets for various business models, especially considering that they are easy to transfer (with various ways of interoperability) and non-rivals, which allow them to be explored for different purposes by various entities.[70]

Processing of personal data is not one of ENACT's main activities. However, some personal data may be processed for the creation of the Knowledge Hub. Beyond the considerations

---

[65] European Commission. (2024). **White paper on options for enhancing support for research and development involving technologies with dual-use potential.**
[66] VLIR (2022). **Guidelines for Researchers on Dual Use and Misuse of Research.** Retrieved from: https://vlir.be/wp-content/uploads/2022/10/VLIR-Dual-Use-2022-EN.pdf
[67] European Commission. (2021). **Guidance note – Potential misuse of research**. EU Grants: Potential misuse of research: V2.0. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf
[68] European Union. (2024). Commission delegated regulation (EU) 2024/2547 of 5 September 2024 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items. 2024/2547. **OJEU**, 7.11.2024. L series.
[69] E.g., NATO. (2023). **Science & Technology Trends 2023-2043.** Across the Physical, Biological, and Information Domains. Volume 2: Analysis.
[70] Toffler, A. (2012). **O futuro do capitalismo: a economia do conhecimento e o significado da riqueza no século XXI**. São Paulo: Saraiva.

already mentioned and that will be considered and implemented throughout the development of the project, ENACT will also consider the whole EU Data Protection Framework when developing the project since the right to data protection is a fundamental right protection by European and international law. For developing a legally and ethically compliant tool, ENACT should observe the new findings on case-law regarding data protection, which shows that several and different types of information can bring into light individual aspects of a person, which would make it a personal data. So, it is crucial to consider specific norms about the use of personal data, especially the General Data Protection Regulation (GDPR)[71] and the ePrivacy Directive[72]. Also, considering the specific focus of the project on FCT, the Law Enforcement Directive (LED)[73] must also be taken into account, which establishes rules of processing personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, having a direct connection with ENACT. Nonetheless, considering that ENACT already developed a Data Management Plan (D1.2, submitted in M03), this Report will focus on the use of personal data for the results of ENACT, without further developing guidelines to be considered by partners when handling personal data, since this was already addressed in the project.

Additionally, the EU legal framework also comprehends that not only personal data is relevant for today's society. So, rules aiming for the maximum exploitation of the information already produced have been put into force in the European jurisdiction, with the goals to increasing the economic potential of the single market and to maximize the fundamental rights and freedoms. As this directly interacts with ENACT's goals, legal provisions on the topic of data will be evaluated and embedded in the project, considering the principles, rules and good practices already established in this domain, especially the Regulation on the Free-Flow of

[71] European Union. (2016). 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**). 4 May 2016.

[72] European Union. (2002). **ePrivacy Directive**. 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). 12 July 2002, updated version of 19 December 2009.

73 European Union. (2016). 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 (**Law Enforcement Directive**). 4 May 2016.

Non-Personal Data[74], the Open Data Directive[75], the Data Governance Act[76], and the Data Act[77].

In this initial assessment, the most relevant legal provisions will be highlighted, in connection with the first mapped interferences with ENACT's activities. However, as an introductory report, the conclusions here presented will be revisited and updated in the following versions of this Deliverable, with more specific considerations regarding the risks and mitigation measures related to ENACT.

## 4.1 The General Data Protection Regulation (GDPR)

As briefly presented (see 3.4), the GDPR was a very relevant normative that entered into force aiming a more harmonized EU approach to the fundamental right to data protection. Repelling the previous Directive, the Regulation brought a general and universalist approach to the topic, with the goal of maintaining the protection of personal data of EU citizens even in a data-driven international world and economy.[78]

In this context, the GDPR follows an *ex-ante* approach, meaning that personal data processing activities are prohibited unless the data subject provides their consent or there is another legal legitimate base for said treatment[79]. Article 6 of the GDPR presents an exhaustive list of legal bases for processing data, mentioning that personal data can only be processed if the data subject provides their consent, or if the processing is necessary for:

- The performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Compliance with a legal obligation to which the controller is subject;
- In order to protect the vital interests of the data subject or of another natural person;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- The purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and

[74] European Union. (2018). 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 (**Regulation on the Free-Flow of Non-Personal Data**). 28 November 2018.
[75] European Union. (2019). 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 (**Open Data Directive**). 26 June 2019.
[76] European Union. (2022). 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**). 3 June 2022.
[77] European Union. (2023). Regulation of the European Parliament and of the Council on Harmonised rules on fair access to and use of data (**Data Act**). 9 November 2023.
[78] Bennett, Colin; e Raab, Charles D. (2018). **Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective.**
Limberger, Têmis. (2019) Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco.
[79] Mendes, Laura Schertel. (2014). **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva.

freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Rules set by the Regulation apply horizontally and vertically to both private and public actors processing personal data. In this sense, the concept of processing is very broad, including any activity with personal data (e.g., collection, sharing, retaining, or exclusion)[80].

Another way of guaranteeing that the GDPR has a scope as broad as relevant, the Regulation adopted a very inclusive concept of personal data. Article 4(1) of the GDPR establish that personal data should be understood as "any information relating to an identified or identifiable natural person ('data subject'); 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 identity of that natural person".

Even though the Regulation already follows an expensive definition of data protection, the case-law has confirmed that several information should be considered as personal data as from the possibility of identifying someone. For example, the Court of Justice of the European Union (CJEU), already decided that dynamic IP addresses constitute personal data. The Court interpreted identifiability in a broad manner by stating if a controller holding information about a person has legal means to obtain from another party extra information that enables the organisation to identify the individual, then the data should be considered as personal[81]. So, it is necessary to reflect beyond he data in the hands of one controller, but also consider possible interactions of the organisation. In a more recent decision, the CJEU reaffirmed the relative approach to the concept of personal data[82]. This means, that "it is not required that all the information enabling the identification of the data subject must be in the hands of one person".[83] This case, T-557/20, is currently under appeal and the future decision is highly anticipated. Any future relevant understandings shall be considered in ENACT. So, it is crucial to develop a case-to-case analysis of each data processing activity and used datasets to verify if personal data is being handled, what is being considered by ENACT.

Nonetheless, the GDPR has a limitation on its material scope, namely anonymised data. Anonymous information should be understood as data not related to an identified or identifiable person, or to personal data that went through an anonymisation procedure that the data subject is no longer identifiable[84]. For understanding if a person is identifiable, one should consider all the reasonable means to be used by any party to identify the individual.[85] Anonymisation is different from pseudonymisation, since the last considers any the measures

---

[80] Article 4 (2) of the GDPR.
[81] CJEU. (2016). Case C-582/14. **Patrick Breyer v. Bundesrepublik Deutschland**. 19 October 2016.
[82] Spajic, Daniela. (2023). Anonymous vs. pseudonymous data: the CJEU reaffirms the relative approach to the concept of personal data. **CiTiP blog.** Available at: https://www.law.kuleuven.be/citip/blog/anonymous-vs-pseudonymous-data-the-cjeu-reaffirms-the-relative-approach-to-the-concept-of-personal-data/
[83] CJEU. (2023). Case T-557/20. **SRB v. EDPS**. 26 April 2023, referring to CJEU. (2016). Case C-582/14. **Patrick Breyer v. Bundesrepublik Deutschland**. 19 October 2016.
[84] Recital 26 of the GDPR.
[85] Recital 16 of 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. 21 November 2018.

that lead to the impossibility of the personal data being "attributed to specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[86]

GDPR also finds limitation in its material scope for specific purposes. According to Article 2(2) of the Regulation, it does not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty of the European Union (TEU);
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The last exception is relevant to ENACT, since the results of the project are foreseen to be used for combating criminal offences. For this reason, not only the GDPR, but also the LED will be analysed and considered in the project, guaranteeing that the various purposes of ENACT are evaluated. Also in this matter, it is relevant to notice that the GDPR establishes thar processing personal data relating to criminal convictions and offences or related security measures "shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority"[87].

As a principle-based Regulation, the GDPR establishes the following principles that should be observed in all personal data processing activities:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and Confidentiality
- Accountability

Additionally, by the understanding that the self-determination of any individual relies on them having effective control over their personal data. For ensuring this, the GDPR lists a non-exhaustive list of rights to be observed by controllers[88]:

- Right to information;
- Right of access;
- Right to rectification;
- Right to erasure ("right to be forgotten")

[86] Article 4(5) of the GDPR.
[87] Article 10 of the GDPR.
[88] Articles 12 to 22 of the GDPR.

- Right to restriction of processing;
- Right to data portability;
- Right to objection;
- Right to not be subject to automated decision-making, including profile.

Important to notice that the mentioned rights may only be restricted by law when specific interests are at stake[89]:

(i) national security;
(ii) defence;
(iii) public security;
(iv) 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;
(v) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
(vi) the protection of judicial independence and judicial proceedings;
(vii) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(viii) a monitoring, inspection or regulatory function connected to the exercise of official authority in the cases referred to in point (i) to (v) and (vii);
(ix) the protection of the data subject or the rights and freedoms of others;
(x) the enforcement of civil law claims.

This list is exhaustive[90], but may have relevance to some actions in ENACT, especially considering that some processed data will be classified as restricted. So, limitation of access to personal data should only be in place in case one of the purposes listed above are in place.

Following the consideration established in the DMP, whenever ENACT faces a request of exercise of data subjects' rights, the project must timely reply with the due information. Details on the procedure and who to contact for the exercise of data subjects' rights will be available in the project's website.[91]

### 4.1.1 Data cycle

Considering that personal data might be processed, an essential step for the compliance of the ENACT project and results is to determine and examine the data cycle. The data processing activities developed internally in ENACT were already mapped in a detailed manner in the Data Management Plan v1 (D1.2)[92] submitted in M03. As an exercise of further analysis in this report, a summary of the data cycle taking into account the DMP is presented below:

[89] Article 23(1) of the GDPR.
[90] EDPB. (2020). **Guidelines 10/2020 on restrictions under Article 23 GDPR,** Version 2.0.
[91] ENACT. https://enact-eu.net/about/
[92] ENACT. (2023). D1.2 – Data Management Plan v1.

**Table 1. Overview of the data processing activities**

| | |
|---|---|
| **Data assets** | Project results, practitioner reports, public databases, policy papers and updates, news and media, scientific literature, consultation results (including interviews and questionnaires), and events reports. |
| **Processing purposes** | Guarantee the quality of the information displayed in the knowledge hub to provide relevant evidence-based support to the decision makers of the EU Research &Innovation ecosystem, in particular the Fight against Crime and Terrorism |
| **Controller** | During the duration of the project, the consortium should be considered as the data controller. In this stage, it is not possible to determine who shall be considered as the controller of data in future further development of ENACT hub outside of the scope of the research project. |
| **Processor(s)** | In this stage, it is not possible to determine |

Finally, it is relevant to point that no data subject will be subjected to automated decision-making procedures in ENACT, which already mitigates the risks of the data processing activities taking place in the project.

## 4.1.2 GDPR and ENACT

### *4.1.2.1 Personal data processing for the project's goals and results*

After the considerations regarding the GDPR, it is relevant to understand the specific implications of this framework to ENACT. It is central to understand that processing personal data will not be part of ENACT's main activities since the knowledge acquired and processed will be based mainly in non-personal data. Nonetheless, it is possible that some inputs that will feed the knowledge hub do contain personal data (e.g., name of authors, policy makers, interviews, questionnaires) or that personal data can be found via the combination of data sources. So, it is possible that ENACT handles mixed datasets, meaning, datasets that contain both personal and non-personal data. The handling of mixed datasets is closely related to the Regulation of free flow of non-personal data (see 4.7), so a holistic approach with considerations of all the applicable rules must be developed in ENACT.

To this end, a continuous data mapping of the inputs used in the Knowledge Hub must take place. In case a personal data is processed, then the activity must comply with the GDPR rules, with clear observation of the data protection principles and a framework that allows the exercise of rights by the data subjects. In the latter versions of this report, more specific risks and mitigation measures may arise considering a closer evaluation of the datasets being used by ENACT.

In case high risks to the rights of freedom of natural persons arise from future personal data activities in ENACT, a Data Protection Impact Assessment (DPIA) should be incorporated in the later versions of this Deliverable, assessing the risks and mitigation measures in place to guarantee the observation of the fundamental right to data protection.

### *4.1.2.2 Personal data processing for internal activities*

Additionally, it is important to differentiate the data that will be used directly for the project goals and results (e.g., data that will feed the knowledge hub) from the data that is relevant

for the project internal activities (e.g., contact list of partners for communication purposes). The latest, intra-project data, will be handled in a compliant manner following the description of actions established in the Data Management Plan (D1.2, submitted in M03) and also published in a policy privacy in the project's website[93]. Thus, what has been presented in this Deliverable focuses on the use of data for the results of the project (the knowledge hub).

Finally, it is important to highlight that non-EU partners members of the consortium remain bound by the GDPR, especially considering data processing activities involving data subjects in the EU. On this, we highlight that ENACT counts with a partner based in the UK. While, as mentioned, the partner is bounded by the GDPR, it is also important to mention that currently a temporary adequacy decision was provided for international data transfers between the UK and the EU, confirming an adequate level of protection also under the UK regulation on personal data.[94]

## 4.2 ePrivacy Directive

Complementing the provisions set by the GDPR (and the previous Data Protection Directive), the ePrivacy Directive lays down rules for the electronic communications sector. Understanding that the confidentiality of communication is one of the ramifications of human rights[95], the Directive establishes that surveillance is, in principle, prohibited[96], while the free movement of data and the communication ecosystem is compatible with the essence of fundamental rights, as long as some limits are observed[97]. As a Directive, this legislative piece must be transposed in the EU Member States national law, and unlike the GDPR, the ePrivacy Directive does not have a general scope of application, focusing on data processing activities in the electronic communication sector.

Communication, in this context, should be understood as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communication network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.”[98].

The ePrivacy Directive only covers traditional telecommunication services[99] and the scope of the norm does not include “activities concerning public security, defence, State security

[93] ENACT. https://enact-eu.net/about/
[94] ”Both adequacy decisions last until 27 December 2025. This date reflects a 6-month extension to the original end date. This extension has been adopted by the European Commission to allow for an assessment of the new legal framework in the UK under the Data (Use and Access) Act.“
ICO. **Adequacy.** Retrieved from: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/.
[95] Recital 3 of the ePrivacy Directive.
[96] European Union Agency for Fundamental Rights. (2018). **Handbook on European Data Protection Law**. Luxembourg. Publications Office of the European Union.
[97] Article 1(1) of the ePrivacy Directive.
[98] Article 2(d) of the ePrivacy Directive.
[99] European Union Agency for Fundamental Rights. (2018). **Handbook on European Data Protection Law**. Luxembourg. Publications Office of the European Union.

(including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law"[100].

With these initial considerations, it is understood that the ePrivacy Directive, as is, does not affect directly the ENACT project. Only minor rules related to a possible hosting service may apply (e.g., the need to collect the consent for cookies). In those cases, considering the fact that the Directive is *lex specialis*, in case of an apparent conflict between the Directive and the GDPR, the first should apply.

## 4.3 Law Enforcement Directive (LED)

Considering that personal data processing for certain purposes, including the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties fall outside of the scope of the GDPR, as already mentioned, a different and autonomous legal normative was approved in parallel with the General Regulation. This complementary piece of legislation is commonly known as Law Enforcement Directive (LED), which sets rules regarding personal data processing handled by authorities for the mentioned purposes. Since it is a Directive, the provisions must be transposed in the EU Members national legislations. Nonetheless, only the Directive will be considered in the context of the project, since it already embraces the main aspects of the topic and it is a European result.

LED adopts a number of similar definitions as the ones set by the GDPR (e.g., personal data, processing, processor). In the same sense, the principles laid down by the Directive[101] are also closely related to the ones foreseen in the GDPR, being them:

- Lawfulness and fairness;
- Transparency;
- Purpose limitation (personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes);
- Minimisation (personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed);
- Accuracy;
- Storage limitation (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 they are processed)[102];
- Data security (processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures);
- Categorisation[103].

[100] Article 1(3) of the ePrivacy Directive.
[101] Article 4 of the LED.
[102] Additionally, Article 5 of the LED establishes that "Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed".
[103] Article 6 of the LED: "Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects (…)"

Another interesting and related provision is Article 20, which defines that whenever needed and or possible, data protection by-design and by-default should be implemented in processing activities under the scope of the LED, which will take place in ENACT.

On the topic of data subjects' rights, the LED establishes a high level of discretionary power to Member States, since Article 18 limits data subjects' rights while making space for heterogenous transpositions into national legislations.[104] Nonetheless, the LED lists various rights, namely:

- Right to information[105];
- Right of access[106];
- Right to rectification or erasure of personal data and restriction of processing[107];

Even though ENACT is a project aimed and designed for LEAs and their employees, the project does not foresee any creation, collection or any processing activity involving personal data that would fall under the scope of the LED. On one hand, the personal data that might be revealed from the project's goals and results are not connected to any of the activities under the LED. By building knowledge hubs, ENACT is disseminating already accessible knowledge, not acting directly for any specific law enforcement activity. ENACT's goals are more connected with networking, knowledge distribution, and effective use of already available information. Even in the case of the stakeholders map, the purpose for the processing activity is connected to networking and promotion, not law enforcement. On the other hand, the personal data processed for internal activities of the project are completely disconnected from the object regulated by LED. These processing activities are connected to administrative issues such as communication and payment. Personal data collected for these purposes will not be used for any goal connected to law enforcement activity. Thus, LED continues to be an essential norm for actors involved in the field of R&I for FCT. However, ENACT's activities do not fall under the scope of the Directive.

## 4.4 Erro! A origem da referência não foi encontrada.The Open Data Directive

After several amendments in the Directive 2003/98/EC on the re-use of public sector information and evaluating the need for updating the Directive 213/37/EU with the same topic, in 2019 the Open Data Directive entered into force. Discouraging exclusivity arrangement while promotive access to information, the Directive goals include maximizing the use of information for economic and social development, even highlighting the importance of data for new technologies such as artificial intelligence (AI).

With similar goals to the Regulation on the free flow of non-personal data, the Open Data Directive brings a broader scope of application, including not only documents processed by public sector organisations, but also vast information maintained by public undertakings and

[104] European Parliament (2022). **Assessment of the implementation of the Law Enforcement Directive**. Authors: Vogiatzoglou, Plixavra; Marquenie, Thomas. Online report available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf
[105] Article 13 of the LED.
[106] Articles 14 and 15 of the LED.
[107] Article 16 of the LED.

research data resulting from public funding. On this, Article 1 of the Directive establish a detailed list of documents to which the Directive does not apply, including documents protected by intellectual property rights, and documents with sensitive data for the protectional national security, defence, or public security, and with statistical or commercial confidentiality. In the categorization of restricted and publicly available information, ENACT must consider the provisions of this Article as a relevant way of moderating data.

On this, it must be better understood how the results of ENACT will be classified, since research data is defined by the Open Data Directive as "documents in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results;"[108]. So, various outcomes of ENACT project will fall in this concept, which must observe the provisions of the Article 10 of the Directive:

1. Member States shall support the availability of research data by adopting national policies and relevant actions aiming at making publicly funded research data openly available ('open access policies'), following the principle of 'open by default' and compatible with the FAIR principles. In that context, concerns relating to intellectual property rights, personal data protection and confidentiality, security and legitimate commercial interests, shall be taken into account in accordance with the principle of 'as open as possible, as closed as necessary'. Those open access policies shall be addressed to research performing organisations and research funding organisations;
2. Without prejudice to point c) of Article 1(2), research data shall be re-usable for commercial or non-commercial purposes in accordance with Chapters III and IV, insofar as they are publicly funded and researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository. In that context, legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights shall be taken into account.

Another important concept brought by the Directive is the definition of open data as it follows, since it reinforces the principles of data open-by-design and open-by-default, which are part of several provisions of the Directive, reinforcing the idea that data should be as open as possible [109]:

> Open data as a concept is generally understood to denote data in an open format that can be freely used, re-used and shared by anyone for any purpose. Open data policies which encourage the wide availability and re-use of public sector information for private or commercial purposes, with minimal or no legal, technical or financial constraints, and which promote the circulation of information not only for economic operators but primarily for the public, can

[108] Article 2(9) of the Open Data Directive.
[109] Recital 16 of the Open Data Directive

> play an important role in promoting social engagement, and kick-start and promote the development of new services based on novel ways to combine and make use of such information. Member States are therefore encouraged to promote the creation of data based on the principle of 'open by design and by default', with regard to all documents falling within the scope of this Directive. In doing so they should ensure a consistent level of protection of public interest objectives, such as public security, including where sensitive critical infrastructure protection related information are concerned. They should also ensure the protection of personal data, including where information in an individual dataset does not present a risk of identifying or singling out a natural person, but when that information is combined with other available information, it could entail such a risk.

Other principles are also embedded in the Directive, as the ones highlighted:

- Non-discrimination between re-users, including for cross-border re-users. Comparable re-users must have similar rights, regardless of being public or private entities, except for differentiated charging in specific cases[110];
- Non-exclusivity, except for the provision of a service in the public interest and with a limited duration[111];
- Interoperability in a machine-readable format, especially for high-value datasets[112];

As a Directive, the norms set by the legal instrument must be transposed into national law of the Member States, which has been a slow process. That is one of the reasons why initiatives like ENACT are so relevant, since, as already mentioned, they broadcast the importance of the re-use of information, especially when held by the public sector, research performing organisations and research funding organisations. Even though each partner of the project has a different nature (e.g., private and public entities), ENACT is considered as a public interest research project as a whole. Thus, ENACT's results should be made as open as possible, following the ideas of possibilities of re-use of information and Open Data.

To already apply certain provisions brought by the Open Data Directive, initial considerations shall be drawn to each of the main outputs of the project. First, regarding the SKB and the Knowledge Repository, ENACT is solely using publicly available information to construct its outputs. Nevertheless, as already mentioned, the access to the full content of certain observation may be blocked by licenses or paywalls, for example. ENACT will not be able to guarantee the full access to each one of the observation, otherwise it could infringe copyrights and specific policies. Nevertheless, as highlighted before, ENACT will reply to any request of access to information providing as much information as possible about each observation, including a direct link to the source of the content.

In the same sense, the Flash and Analytical Reports developed by the project will all be open access. Exploring the SKB, the Reports will allow for a different presentation of the observations in context. All the reports will be available in the project's website and are available for further use. Limitations only apply to secondary uses incompatible with

[110] Recital 46 and Article 11 of the Open Data Directive.
[111] Article 12 of the Open Data Directive.
[112] Article 14 of the Open Data Directive.

fundamental rights, values and freedoms. Exactly the same applies for the Stakeholders Map. This tool contains solely publicly available information, and the data provided in the Map should not be used for incompatible purposes, including the identification of individuals.

Finally, ENACT produces both public and restricted Deliverables. After the first period review and engagement with the EAB, in the cases of restricted Deliverables, a brief summary highlighting challenges and mitigation measures presented in the documents will be added to the project's website and will be available for all.

## 4.5 The Data Governance Act (DGA)

A human-centric approach in the developing of technologies, with the observation of European values and rights in the digital world are central for the establishment of the European Strategy for data. By understanding that maximizing the use of data is a need for achieving greater purposes as security, economic development, and effective public services, the EU has been working on different initiatives to promote safe and trusted data sharing and re-use of data, by increasing data availability and interoperability[113]. Two legislative pieces are already in force playing a vital role in for the achievement of the goals of this Strategy, namely: (i) the Data Governance Act (DGA); and (ii) the Data Act. While the DGA complement the Open Data Directive, the Data Act focus on open data for the private sector[114].

The DGA plays a vital role in the reinforcement of the common European Data Spaces, bringing rules for voluntary data sharing and data availability for the flow of information involving public and private entities. The Regulation sets[115]:

- Conditions for the re-use, within the Union, of certain protected categories of data held by public sector bodies;
- The framework for data intermediation services (data intermediaries);
- The framework for entities involved in data availability for altruistic services;
- The establishment of a European Data Innovation Board.

At the moment, the most relevant provisions of the DGA are related to the expansion of the principles already set by the Open Data Directive, aiming for wider use of public sector data. That is why the Chapter II of the DGA both sets rules for the re-use of protected data that falls outside of the scope of the Open Data Directive and implements a scenario to facilitate the cross-border transfers of data.[116] Considering that ENACT will handle both research data and also information controlled by the public sector, provisions related to the use of said categories of data are of high relevance to the project. However, the Regulation adopts an unclear language that still needs better addressing in concrete cases[117].

---

[113] European Commission. (2020). Communication from the Commission the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. **A European Strategy for data**. 19 February 2020.
[114] Katulić, T., Musa, A., & Lončar, D. (2023). Understanding some of the open data challenges to data protection in the developing European legal framework**. Central European Conference on Information and Intelligent Systems**, 35–41.
[115] Article 1 of the DGA.
[116] Baloup, J. *et al*. (2021). **White Paper on the Data Governance Act**. CiTiP Working Paper series.
[117] Baloup, J. *et al*. (2021). **White Paper on the Data Governance Act**. CiTiP Working Paper series.

Article 5 of the DGA occupies a central role in this system, setting conditions for the re-use of data[118], which shall be further observed by ENACT both on making data available as well as requesting data for the purposes of the project. While requesting data, partners should keep in mind that, in a more detailed provision than the Open Data Directive, the DGA establishes that[119]:

> In order to facilitate and encourage the use of data held by public sector bodies for the purposes of scientific research, public sector bodies are encouraged to develop a harmonised approach and harmonised processes to make that data easily accessible for the purposes of scientific research in the public interest. That could mean, inter alia, creating streamlined administrative procedures, standardised data formatting, informative metadata on the methodological and data collection choices and standardised data fields that enable the easy joining of data sets from different public sector data sources where relevant for the purposes of analysis. The objective of those practices should be to promote the publicly funded and produced data for the purposes of scientific research in accordance with the principle of 'as open as possible, as closed as necessary'.

Another relevant aspect to be considered is that "the exchange of data, purely in pursuit of their public tasks, among public sector bodies in the Union or between public sector bodies in the Union and public sector bodies in third countries or international organisations, as well as the exchange of data between researchers for non-commercial scientific research purposes, should not be subject to the provisions of this Regulation concerning the re-use of certain categories of protected data held by public sector bodies" [120], so ENACT or some of the research activities developed in the project may not be under the scope of the Regulation.

The relevance of comprehending scientific research activities inside the project gains even more relevance with the broad understanding of scientific research purposes set down by the DGA as "any type of research-related purpose regardless of the organization or financial structure of the research institution in question, with the exception of research that is being conducted by an undertaking with the aim of developing, enhancing or optimizing products or services". By the understanding that ENACT will have two different relevant relationships with the re-use of data (one when requesting data to public sector authorities or bodies or other scientific research initiatives, and the other when providing data for the re-use of it), these considerations must be assessed in a case-by-case definition, with further development in the future phases of the project. Additionally, the same considerations provided in the previous topic (4.4) also apply to each output in relation to the DGA. Finally, under the DGA, it is important to highlight that ENACT is applying the FAIR practices and principles to the project's results, especially to the SKB. This will facilitate the data re-use and is compatible with the ideas of interoperability for re-use.

---

[118] European Commission. (2022). **Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research.** Independent Expert Report written by Mirelle van Eechoud.
[119] Recital 16 of the DGA.
[120] Recital 12 of the DGA.

## 4.6 The Data Act

As a pillar of the European strategy for data, the Data Act is a Regulation that very recently entered into force (on 11 January 2024). With a strong focus on clouding services and the private sector, the Regulation addresses relevant topics for research activities[121]:

- Access obligations imposed on mainly businesses in case of exceptional (public interest) needs;
- Access to certain Internet of Things (IoT) data for users of connected products (including a clarification of the intellectual property status of IoT data);
- FRAND licensing for data access, with specific protections for SMEs;
- Switching of cloud service providers and associated data portability;
- Interoperability for data spaces.

The Data Act, similarly, to the other normative instruments already evaluated, adopts EU values throughout the whole document, especially the goal of increasing competitiveness and develop the European Single Market, while observing the principles of fairness, proportionality, accountability and transparency. Reaffirming the value of data, the Act considers different relationships in the data market: Business to Consumers, Business to Business, and Business to Government. Finally, while promoting data governance, including rules on data interoperability, the Data Act adopts a free-flow approach to data, in divergence to the property-data approach.[122]

In ENACT, initially, having the assessment of the Data Act, it is important to map which data sharing relationships will be established in the project. In a later phase, it is crucial to establish good practices in data interoperability in an accessible format to guarantee the free flow of data. Considering the research activities of ENACT and the proximity with public bodies, the Data Act, apparently, will be a subsidiary norm to be applied alongside the other legislative instruments already presented.

ENACT does not use or interact with IoT products and does not aim at creating a specific data space. Also, the project does not foresee any interaction with specific cloud services providers and data portability requirements and services. In the same sense, any of the research outputs will handle different license for data access. Considering the main research outputs (Flash and Analytical Reports, Stakeholder Map, and Knowledge Repository), the Data Act can serve as a guide or inspiration for measures for access, but do not impose any specific compliance measures to the project.

## 4.7 Mixed datasets

As already mentioned, mixed datasets can be understood as databases containing both personal and non-personal data. And, while compatible, applying the different regulations regarding personal data and non-personal data for the handling of mixed datasets may be challenging. However, the majority of datasets used nowadays consist of mixed datasets. As

[121] European Commission. (2022). **Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research.** Independent Expert Report written by Mirelle van Eechoud.
[122] CiTiP. (2022). **White Paper on the Data Act Proposal**. Ed. By Ducuing, Charlotte; Margoni, Thomas; Schirru, Luca.

an example of this category, the EC Guidance on handling mixed datasets[123] mentions "a research institution's anonymised statistical data and the raw data initially collected such as the replies of individual respondents to statistical survey questions", which may be observed in ENACT. This is not the only case where these datasets may be part of the project, hence the importance of following the inputs of the Knowledge Repository. So, following the EC Guidance and the legal provisions on the matter, the following system should apply:

- the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset;
- the personal data part of the dataset must consider that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data[124];
- when the non-personal data and the personal data parts are 'inextricably linked' (e.g., impossible to separate) the GDPR fully applies to the whole mixed dataset.

No controller is obliged to separate mixed datasets, especially because this may decrease the value of the information, may be technically not feasible, and the different systems of protection are compatible. So, if ENACT processes a small amount of personal data, one solution can be to separate the datasets, but also other comprehensive holistic solutions are in order.

Regarding portability or interoperability, it is central to understand how this notion plays different roles in personal data and in non-personal data. In the first, the data portability is a right established in the relationship between the data subject and the controller, ensuring that the individual may take their data to another provider without major issues. In the latter scenario, we encounter a business-to-business scenario for interactions. [125] This understanding is relevant and connected to possible requests of access and transfer of data that ENACT may receive.

The further application of the new Regulations set by the European Strategy for Data (DGA and Data Act) must always be aligned with the already established GDPR, for ensuring that the economic growth and exploitation of the European Single Market will continue to respect the fundamental rights, maintaining a crucial role on foreshowing the importance of this balance in the international community[126].

Since we are also analysing the impact of very recent and generic legislative initiatives, the future versions of this report are crucial for a better and further analysis of the impact of this complex legal framework in the ENACT project. This also considering that the regulatory framework is not focused on research activities, not addressing specific needs and scenarios

[123] European Commission. (2019). **Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union**. 20 May 2019.
[124] Article 1(3) of the GDPR.
[125] European Commission. (2019). **Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union**. 20 May 2019.
[126] Katulić, T., Musa, A., & Lončar, D. (2023). Understanding some of the open data challenges to data protection in the developing European legal framework**. Central European Conference on Information and Intelligent Systems**, 35–41.

of the international funded scientific research initiatives.[127] So, ENACT also intends to collaborate in the development of relevant recommendations for this still new complex regulatory framework.

## 4.8 AI Act

Understanding the risks and potential of AI technologies, the EU adopted the first binding general legal instrument regulating AI technologies, the AI Act. The official text was published in March 2024. Aiming for a broad, technology-neutral and future-proof concept, the AI Act, in its Article 3(1), defines AI system as a “machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;'.

The Regulation applies whenever you place on the market, put into service or use an AI system, or whenever you place on the market general-purpose AI. A scalonated applicability is foreseen, with most rules applying as of 2026. In either case, the AI Act left certain activities out of its scope, including non-professional purposes or use of AI tools for scientific research and development. ENACT, as a research project, can enjoy the last category and does not carry any specific compliance obligation. However, considering the AI Act as a good practices guide, the assessment will continue.

Aiming at preventing harms, the AI Act adopted a risk-base approach, targeting systems that present higher risks to society. With this, stakeholders involved in AI systems development and use must assess beforehand the risks carried out by the system and the possible purposes that can be achieved with said technology. The higher the possible risks, more obligations apply. To guarantee that this is translated in the full AI lifecycle, different obligations apply to different stakeholders, including the provider, the importer, and the deployer of the AI technology. Under the AI Act,[128] four categories of risk are drawn:

- Unacceptable risks, namely: harmful AI-based manipulation and deception, harmful AI-based exploitation of vulnerabilities, social scoring, individual criminal offence risk assessment or prediction, untargeted scraping of the internet or CCTV material to create or expand facial recognition databases, emotion recognition in workplaces and education institutions, biometric categorisation to deduce certain protected characteristics, and real-time biometric identification for law enforcement purposes in publicly accessible places (see Article 5 AI Act).
- High-risks: systems that bring serious risks to health, safety or fundamental rights, including remote biometric identification, biometric categorisation, emotion recognition; AI use-cases in law enforcement that may interfere with people's fundamental rights; AI solutions for the administration of justice and democratic processes (see Article 6 AI Act). Before placing these systems on the market, strict obligations must be observed, including clear and adequate information to the

[127] European Commission. (2022). **Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research.** Independent Expert Report written by Mirelle van Eechoud.

[128] European Commission. **AI Act.** Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

deployer, human oversight, risks assessment and mitigation measures, high level of cybersecurity and accuracy.

- Limited risks: whenever a limited risk is assessed, transparency requirements must be put into place (e.g., clarify if a user is interacting with a chatbot).
- Minimal or no risks: in this case, the AI technology can be used without any other restrictions besides the ones set by other laws (e.g., GDPR)

At the time of the first submission of D1.3, the AI Act had not yet been published and no specific considerations around AI were foreseen in the initial stage of the project. However, after the first periodic review and with considerations from the EAB, two points regarding AI deserve attention in ENACT.

First, even though the project does not develop any AI tool, during its first test implementation cycle (WP5), partners understood the value on using Large Language Models (LLMs), such as ChatGPT, to assist the classification of the observations. A preliminary assessment shows that this use can fall under the idea of deploying a limited risk AI practice. With this in mind and respecting the best practices involving AI governance, transparency measures to highlight the AI use were established, as detailed in D5.1[129]

Second, as briefly mentioned, ENACT mapped a new risk of disseminating AI tools that are not compliant with the AI Act or that fall under the classification of prohibited practices as defined in Article 5 of the Regulation. Currently, no specific measure or classification is in place to evaluate this. Nonetheless, partners are discussing the possibility of embedding these categories into the SKB in the future and to leverage from Analytical Reports to provide this evaluation. As highlighted in the section on Misuse Considerations (see 3.4), ENACT does not intend to assess the compliance of all specific AI tools highlighted in the project's outputs. This would be a disproportionate effort and outside of the scope of the project. The consortium, nevertheless, understands and is finding solutions to address the need for more clarity on this matter.

## 4.9 Summary of considerations on data governance

To facilitate the understanding of the data governance measures put in place to each of the project's outputs, the following table presents a summary of considerations on data governance.

**Table 2. Summary of considerations on data governance**

| Research output | Considerations on Data Governance |
|---|---|
| Stakeholders Map | All non-personal data information is openly accessible. Re-use is possible, as long as compatible with fundamental rights, freedoms and values. Information from the Stakeholders Map should not be used in incompatible contexts and neither should be combined with other data for the identification of individuals. |
| Flash and Analytical Reports | All reports are publicly available on ENACT's website and can be further added to research repositories.<br>Tools and solutions mentioned in the report are not endorsed by ENACT. Users take full responsibility in engaging with the tools and must conduct their own assessments. |

[129] ENACT. **ENACT Network Methods & Tools v2.**

| | |
|---|---|
| Knowledge Repository and Structured Knowledge Base | Only publicly available information is added as part of the observations. This does not translate to endorsement. ENACT does not provide an assessment of compliance or readiness of the information and tools provided. Responsibility for the further use and deployment of these tools is completely to the user.<br>In case of requests of access to information, ENACT will provide as much information as possible, providing direct links to the sources of the data, within one month from the data of the request. Nevertheless, the project cannot guarantee the full access to information with licensing restrictions or under paywall.<br>Format of the data will be compatible with interoperability practices, facilitating the re-use of information for legal and ethical purposes.<br>In case any AI tool is used for the classification of observations, this will be clearly mentioned in the outputs. |
| Deliverables | Public Deliverables are published in ENACT's website. They can be added to other repositories (e.g., University Libraries). They follow an open license and can be re-used openly, following ethical and legal limitations.<br>Restricted Deliverables are not fully accessible. Nevertheless, a brief summary of the content of each restricted Deliverable will be added to the project's website. |

# 5 Cybersecurity

Cybersecurity is a central aspect for guaranteeing the quality and security of information, protecting fundamental rights and freedoms. For this, the EU provides a legal framework on cybersecurity as part of the EU Cybersecurity strategy.

This section will focus on the most relevant initiatives of this strategy, namely: the NIS2 Directive[130] and the Cybersecurity Act[131], and how they are connected to ENACT. This exercise will allow partners to understand the points of attention to be considered in ENACT, mapping potential risks and designing effective mitigation measures for them. ENACT is composed by partners with different natures, such as private and public entities, education institutions and law enforcement agencies. In their own activities, each entity must comply with specific cybersecurity requirements. These, however, will not be the focus of the present analysis. D1.3 will present an overview of the legal cybersecurity framework and highlight if any of the provisions apply directly to the research project, the consortium or the research results. If necessary, new assessments will be presented in future deliverables, depending on project's updates. Finally, cybersecurity provisions that are not mandatory for ENACT can serve as possible optional mitigation and security measures for guaranteeing the security of the project's outcomes.

## 5.1 NIS2 Directive

As the EU-wide cybersecurity legislation aims to increase the cybersecurity level in the EU via legal measures, new strategies and norms are being developed. Although the NIS2 Directive entered into force in 2023, the effects on repealing the Directive (EU) 2016/1148[132] will only start as of 18 October 2024[133], the same date in which the Members States are obliged to start applying the measures foreseen in the new Directive[134]. Considering the timing of ENACT, only the NIS2 Directive will be relevant for its activities, reason why it will be the focus of the current analysis.

The scope of the NIS2 Directive includes public or private entities mentioned in Annex I or II of the Directive that qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC[135] or exceed the requirements of this classification, and which provide their services or carry out their activities within the Union[136]. The Directive also applies to entities listed in Annex I or II regardless of their size as long as they fall under the situations

[130] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 OJ L 333 (NIS 2 Directive).
[131] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 OJ L 151 (Cybersecurity Act).
[132] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).
[133] Article 44 of the NIS2 Directive.
[134] Article 41 of the NIS2 Directive.
[135] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Available online at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF
[136] Article 2 of the NIS2 Directive.

listed in Article 2(2) of the NIS2 Directive. Entities that must comply with the mentioned Directive are categorized into two different groups: essential or important entities. Essential entities include[137]:

- entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;
- qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;
- providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;
- public administration entities referred to in Article 2(2), point (f)(i);
- any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);
- if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

The remaining entities that fall under the scope of the Directive and are not listed as essential entities should be considered as important entities[138]. Different rules apply to the different categories of entities, aiming for an increase in the cybersecurity standards in the EU, by ensuring[139]:

- Member States' preparedness, by requiring them to be appropriately equipped, for example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority;
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States;
- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Considering the foreseen results from ENACT, it is unlikely that the project will be considered as an essential entity. Actually, ENACT will not develop any tool or technology that would require full compliance with the NIS2 Directive. Different conclusions can emerge for specific activities developed by research partners members of the consortium but, as already mentioned, this assessment goes beyond the scope of the research project and each entity should comply to the applicable provisions accordingly. Nonetheless, some key aspects foreseen in the Directive will be considered in the development of the project as good practices, especially taking into account the relationship that will be established between the project and key digital service providers (e.g., cloud computing services) and the proximity of

[137] Article 3(1) of the NIS2 Directive.
[138] Article 3(2) of the NIS2 Directive.
[139] European Commission. **Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)**. Published online at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

the knowledge hub being constructed to the definition of “network and information system” established by Article 6 of the NIS2 Directive:

- electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;
- any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or
- digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

The security of network and information systems is defined as “ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems”[140].

Considering that entities that develop or administer network and information systems should foresee procedures for handling vulnerabilities[141], ENACT will implement security measures to guarantee the control of access of restricted information, monitoring suspicious actions and attempts of attacks to the system, considering the cybersecurity risk-management measures pointed by the NIS2 Directive. This should be done via technical, operational and organisational measures, aiming for smooth and continuous service providing activity, while also mitigating the impacts of a possible incident[142]. Measures put into place should be proportionate and appropriate to the entity’s: exposure to risks, size, likelihood of occurrence of incidents and their severity.[143]

Finally, it is also be considered that the NIS2 Directive acknowledges the GDPR, stating that this Regulation applies to any processing of personal data that also falls withing the scope of the Directive. So, the NIS2 Directive should not affect the activities of the competent authorities to monitor the compliance of entities with the applicable data protection and privacy law[144].

## 5.2 Cybersecurity Act

With a broader scope than the NIS Directive, the Cybersecurity Act applies to all organisations aiming for more homogenous and relevant cybersecurity approaches within entities, while raising awareness about the importance of cybersecurity for different stakeholders. For this aims, the Cybersecurity Act focuses on establishing a new and stronger mandate for the European Union Agency for Cybersecurity (ENISA) and on creating a European cybersecurity certification framework[145].

With this, ENISA has a crucial role in several areas, as: (i) capacity-building; (ii) knowledge and information; (iii) awareness-raising and education; (iv) research and innovation; (v)

[140] Article 6(2) of the NIS2 Directive.
[141] Recital 58 of the NIS2 Directive.
[142] Incident is defined in Article 6(6) of the NIS2 Directive as “an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems”.
[143] Article 21of the NIS2 Directive.
[144] Recital 14 of the NIS2 Directive.
[145] European Commission. **The EU Cybersecurity Act.** Available online at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

international and operational cooperation and (vi) promotion of cybersecurity certifications. In this context, ENISA's contributions are crucial for an organization within the EU to establish the best practices to be adopted for guaranteeing cybersecurity of its information and communication technology (ICT) systems. This body studies the relationship between cybersecurity requirements and different normatives (e.g., GDPR), further detailing the interactions between various norms of the legal and ethical framework. Thus, in ENACT, partners – especially the technical partners – should consider and implement the best practices set out by ENISA, allowing the development of the compliant-by-design knowledge hub.

Finally, in respect to the European cybersecurity certification framework is designed to verify that certain products, services, and processes, as identified in the EU's working program, adhere to specific security standards, ensuring the protection of data availability, authenticity, integrity, and confidentiality throughout their lifecycle. In this context, ENISA is tasked with developing draft cybersecurity certification schemes, upon request from the EC or EU Member States, with support from experts and close collaboration with relevant stakeholders. The certification scheme's security objectives include safeguarding processed data against breaches, ensuring access only by authorized individuals, identifying vulnerabilities, monitoring data access, and ensuring timely restoration of data availability. It also promotes security through default and design and requires up-to-date software and hardware. Certification schemes may assign assurance level", such as" "basic," "substantial" or "high," based on the associated risk level, considering the probability and impact of potential breaches.

# 6 Conclusions

Data handling will always carry numerous possibilities and risks, especially when involving personal data or in specific contexts as crime prevention and prosecution. In accordance, the results aimed by ENACT are clearly valuable for the FCT community, including for the stakeholders involved in R&I. Structured and accessible data brings several benefits for society, who may use the easily accessible knowledge to create solution that will improve economy, security or other societal issues. Nonetheless, for avoiding any disproportionate negative effects, one must consider the ethical and legal obligations set by the applicable framework. Rules established for data management, human rights and cybersecurity should not be understood as incompatible or as negative for the economic and technological development, but as instruments that aim to have continuous innovation while reaffirming fundamental rights and interests.

Following the RRI approach, ENACT aims to develop compliant by-design and by-default solutions in creating useful resources of information that will be translated into an accessible knowledge hub. This Deliverable introduces topics of attention that must be considered by partners to guarantee that ENACT's goals are achieved. For this, an introduction to the legal and ethical framework was presented, with focus on impacts on human rights, data management (including personal data protection), and cybersecurity. Additionally, it was also described how each norm is linked to the project and how some provision can be implemented, interpreted and can contribute to the results of the research.

However, it is important to note that this assessment is not static neither complete. New developments on the project may lead to different conclusions, which shall be presented in updated versions of the report. Nonetheless, still considering the RRI approach, the results here presented already allow a more critical reflection on possible obstacles or issues that the project may encounter, while also allowing a better understanding of the potential of using data for creating more knowledge.

# References

ALIGNER. **Fundamental Rights Impact Assessment – FRIA**, retrieved from: https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/

Arnadóttir, O. M. (2002). **Equality and Non-Discrimination under the European Convention on Human Rights.** Brill.

Baloup, J. *et al*. (2021). **White Paper on the Data Governance Act**. CiTiP Working Paper series.

Bennett, Colin; e Raab, Charles D. (2018). **Revisiting 'The Governance of Privacy': Comtemporary Policy Instruments in Global Perspective.**

Blanke, H.-Josef., & Perlingeiro, Ricardo. (Eds.). (2018). **The Right of Access to Public Information: An International Comparative Legal Survey** (1st ed. 2018.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-55554-5

Cambridge dictionary. **Misuse**. Online. Retrieved from: https://dictionary.cambridge.org/dictionary/english/misuse

CiTiP. (2022). **White Paper on the Data Act Proposal**. Ed. By Ducuing, Charlotte; Margoni, Thomas; Schirru, Luca.

CJEU. (2023). Case T-557/20. **SRB v. EDPS**. 26 April 2023.

CJEU. (2016). Case C-582/14. **Patrick Breyer v. Bundesrepublik Deutschland**. 19 October 2016.

Council of Europe. (1950). **European Convention on Human Rights.** 4 November 1950. Online version available at: https://www.echr.coe.int/documents/d/echr/convention_eng

CoE. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**Convention 108**).

Council of Europe. (2022). **Guide to the case-law of the European Court of Human Rights - Terrorism**. Published online at: https://www.echr.coe.int/documents/d/echr/Guide_Terrorism_ENG

DARLENE. (2022). **D7.4: Legal and ethical assessment** – 1st version.

Data Spaces Support Centre. (2023). **DSSC Glossary** – Version 1.0. Online Report. March 2023.

DEDA, **Poster**, retrieved from: https://deda.dataschool.nl/en/poster/.

DEDA, **Handbook**, retrieved from: https://deda.dataschool.nl/en/handbook/

Doneda, Danilo. (2019). **O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet**. 2ª ed. Indaiatuba, SP: Editora Foco.

ECtHR. **Rasmussen v. Denmark,** 28 November 1984.

ECtHR. **Goodwin v. The United Kingdom.** 27 March 1996.

ECtHR. **Carson and Others v. The United Kingdom**. 16 March 2010.

ECtHR. **Khamtokhy and Aksenchik v. Russia**, 24 January 2017.

ECtHR, Press Unit. (2022). **Factsheet – Mass surveillance**. September 2022. Available in: https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf

ECtHR. **Halet v. Luxembourg.** 14 February 2023

ENACT. (2023). D1.2 – Data Management Plan v1.
European Commission. **Proposal for an ePrivacy Regulation**. Available online at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

European Commission. **European Commission Pact for Skills Knowledge Hub.** Available at: https://pact-for-skills.ec.europa.eu/community-resources/knowledge-hub_en

European Commission. **Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)**. Published online at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Commission. **Free flow of non-personal data**. Available online at: https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

European Commission. **The EU Cybersecurity Act.** Available online at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

European Commission. (2019). **Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union**. 20 May 2019.

European Commission. (2020). Communication from the Commission the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. **A European Strategy for data**. 19 February 2020.

European Commission. (2021). **Guidance note – Potential misuse of research**. EU Grants: Potential misuse of research: V2.0. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf

European Commission. (2022). **Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research.** Independent Expert Report written by Mirelle van Eechoud.

European Commission. (2024). **White paper on options for enhancing support for research and development involving technologies with dual-use potential.**

European Commission (2024). **AI Act.** Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). OJEU, 12.7.2024.

European Commission. **AI Act.** Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Council. **Statement by the members of the European Council.** Informal meeting of the Heads of State or Government. Brussels, 12 February 2015. Available at: https://www.consilium.europa.eu/en/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/

European Council. (2023). **The EU's response to terrorism**. Available online at: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/.

European Council. (2024). **The EU's fight against organised crime**. Available online at: https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/#:~:text=The%20EU%20is%20taking%20action,on%20asset%20recovery%20and%20confiscation.

European Parliament Multimedia Centre. (2015). **Europol: fighting crime and terrorism in Europe**. Available online at: https://multimedia.europarl.europa.eu/en/video/europol-fighting-crime-and-terrorism-in-europe_N005-151130-001

European Parliament (2022). **Assessment of the implementation of the Law Enforcement Directive**. Authors: Vogiatzoglou, Plixavra; Marquenie, Thomas. Online report available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf

European Union. (1995). **Directive 95/46/EC** on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 23 November 1995.

European Union. (2002). **ePrivacy Directive**. 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). 12 July 2002, updated version of 19 December 2009.

European Union. (2012). **Charter of Fundamental Rights of the European Union**. 26 October 2012. Publication online available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT

European Union. (2012). **Consolidated version of the Treaty on the Functioning of the European Union**. 26 October 2012.

European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (**NIS Directive**).

European Union. (2016). 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**). 4 May 2016.

European Union. (2016). 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 (**Law Enforcement Directive**). 4 May 2016.

European Union. (2017). Proposal for a Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (**e-Privacy Regulation**). 10 January 2017.

European Union. (2018). **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. 21 November 2018.

European Union. (2018). 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 (**Regulation on the Free-Flow of Non-Personal Data**). 28 November 2018.

European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 OJ L 151 (**Cybersecurity Act**). 7 June 2019.

European Union. (2019). 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 (**Open Data Directive**). 26 June 2019.

European Union. (2022). 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**). 3 June 2022.

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 OJ L 333 (**NIS 2 Directive**). 27 December 2022.

European Union. (2023). Regulation of the European Parliament and of the Council on Harmonised rules on fair access to and use of data (**Data Act**). 9 November 2023.

European Union. (2024). Commission delegated regulation (EU) 2024/2547 of 5 September 2024 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items. 2024/2547. **OJEU**, 7.11.2024. L series.

European Union Agency for Fundamental Rights. **What are fundamental rights?** Publication online available at: https://fra.europa.eu/en/content/what-are-fundamental-rights#:~:text='Fundamental%20rights'%20expresses%20the%20concept,is%20used%20in%20international%20law.

FRANZKE, A. S.; MUIS, I.; SCHÄFER, M. T. (2021) 'Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands.' **Ethics and Information Technology,** 23:551-567.

ICO. **Adequacy.** Retrieved from: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/.

Katulić, T., Musa, A., & Lončar, D. (2023). Understanding some of the open data challenges to data protection in the developing European legal framework**. Central European Conference on Information and Intelligent Systems**, 35–41.

Limberger, Têmis. (2019) **Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu**. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco.

Mantelero, Alessandro. (2022). **Beyond Data – Human Rights, Ethical and Social Impact Assessment in AI**. T.M.C. ASSER PRESS, The Hague, The Netherlands.

Mendes, Laura Schertel. (2014). **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva.

NATO. (2023). **Science & Technology Trends 2023-2043.** Across the Physical, Biological, and Information Domains. Volume 2: Analysis.

Netherlands. **Impact assessment fundamental rights and algorithms**, retrieved from: https://www.government.nl/binaries/government/documenten/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms/fundamental-rights-and-algorithms-impact-assessment-fraia.pdf

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D., (2013). A framework for responsible innovation. **Responsible innovation: managing the responsible emergence of science and innovation in society,** 31, 27-50.

Rip, A. (2014). The past and future of RRI. **Life Sciences, Society and Policy** 10(1), 17.

Spajic, Daniela. (2023). Anonymous vs. pseudonymous data: the CJEU reaffirms the relative approach to the concept of personal data. **CiTiP blog.** Available at: https://www.law.kuleuven.be/citip/blog/anonymous-vs-pseudonymous-data-the-cjeu-reaffirms-the-relative-approach-to-the-concept-of-personal-data/

Sutcliffe, H. (2011). A report on responsible research and innovation. **MATTER and the European Commission.**

Taebi, B., Correlje, A., Cuppen, E., Dignum, M., & Pesch, U. (2014). Responsible innovation as an endorsement of public values: The need for interdisciplinary research. **Journal of Responsible Innovation***, 1*(1), 118-124.

The Bali High-Level Meeting on Knowledge Hubs. (2012). **Bali Communiqué 2012.**

Toffler, A. (2012). **O futuro do capitalismo: a economia do conhecimento e o significado da riqueza no século XXI**. São Paulo: Saraiva.

UK Research and Innovation. (2023). **Framework for Responsible Research and Information**. Available online at: https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/framework-for-responsible-innovation/#:~:text=Responsible%20research%20and%20innovation%20is,undertaken%20in%20the%20public%20interest.

United Nations. (1948). **Universal Declaration of Human Rights**. 10 December 1948. Online version available at: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

UNODC. Positive and negative obligations of the State. Available at: https://www.unodc.org/e4j/zh/tip-and-som/module-2/key-issues/positive-and-negative-obligations-of-the-state.html#:~:text=Negative%20obligations%20refers%20to%20a,by%20the%20corresponding%20negative%20obligation.

VLIR (2022). **Guidelines for Researchers on Dual Use and Misuse of Research.** Retrieved from: https://vlir.be/wp-content/uploads/2022/10/VLIR-Dual-Use-2022-EN.pdf

Von Schomberg, R. (2013). A vision of responsible research and innovation. In R. Owen, J.R. Bessant and M. Heintz (Eds.), **Responsible innovation: Managing the responsible emergence of science and innovation in society** , pp.51–74.

Warren, S. D.; Brandeis, L. (1890). The Right to Privacy. **Harvard Law Review**, vol. IV, no. 5, 1890.