Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

D2.5 — *Legal and ethical framework and analysis*

Funded by
the European Union

Grant Agreement Nr. 10109571

Project Information

Project Title	Scaling Up Secure Processing, Anonymization and Generation of Health Data for EU Cross Border Collaborative Research and Innovation		
Project Acronym	SECURED	**Project No.**	10109571
Start Date	01 January 2023	**Project Duration**	36 months
Project Website	https://secured-project.eu/		

Project Partners

Num.	Partner Name	Short Name	Country
1 (C)	Universiteit van Amsterdam	UvA	NL
2	Erasmus Universitair Medisch Centrum Rotterdam	EMC	NL
3	Budapesti Muszaki Es Gazdasagtudomanyi Egyetem	BME	HU
4	ATOS Spain SA	ATOS	ES
5	NXP Semiconductors Belgium NV	NXP	BE
6	THALES SIX GTS France SAS	THALES	FR
7	Barcelona Supercomputing Center Centro Nacional De Supercomputacion	BSC CNS	ES
8	Fundacion Para La Investigacion Biomedica Hospital Infantil Universitario Nino Jesus	HNJ	ES
9	Katholieke Universiteit Leuven	KUL	BE
10	Erevnitiko Panepistimiako Institouto Systimaton Epikoinonion Kai Ypolgiston-emp	ICCS	EL
11	Athina-Erevnitiko Kentro Kainotomias Stis Technologies Tis Pliroforias, Ton Epikoinonion Kai Tis Gnosis	ISI	EL
12	University College Cork - National University of Ireland, Cork	UCC	IE
13	Università Degli Studi di Sassari	UNISS	IT
14	Semmelweis Egyetem	SEM	HU
15	Fundacio Institut De Recerca Contra La Leucemia Josep Carreras	JCLRI	ES
16	Catalink Limited	CTL	CY
17	Circular Economy Foundation	CEF	BE

Project Coordinator: Francesco Regazzoni - University of Amsterdam - Amsterdam, The Netherlands

Copyright

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 the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Deliverable Information

Work package	WP2 - Data Anonymization Research, Design and Assessment
Work package Leader	BSC
Deliverable No.	2.5
Deliverable Title	Legal and ethical framework and analysis
Lead Beneficiary	KUL
Type of Deliverable	Report
Dissemination Level	Public
Due Date	30/09/2023

Document Information

Delivery Date	29/09/2023
No. pages	51
Version | Status	1.0 | Final
Deliverable Leader	KUL
Internal Reviewer #1	Apostolos Fournaris (ISI)
Internal Reviewer #2	Kalliopi Mastoraki (CEF)

Quality Control

Approved by Internal Reviewer #1	25/08/2023 Apostolos Fournaris (ISI)
Approved by Internal Reviewer #2	27/07/2023 Kalliopi Mastoraki (CEF)
Approved by Work Package Leader	29/09/2023 Alberto Gutiérrez Torre (BSC)
Approved by Quality Manager	29/08/2023 Paolo Palmieri (UCC)
Approved by Project Coordinator	29/09/2023 Francesco Regazzoni (UvA)

List of Authors

Name(s)	Partner
Lead Author: Daniela Spajić	KUL
Contributors: Maja Nišević, Anton Vedder	KUL

The list of authors reflects the major contributors to the activity described in the document. The list of authors does not imply any claim of ownership on the Intellectual Properties described in this document. The authors and the publishers make no expressed or implied warranty of any kind and assume no responsibilities for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information contained in this document.

Revision History

Date	Ver.	Author(s)	Summary of main changes
15/05/2023	0.1	Daniela Spajić (KUL)	First draft input
29/05/2023	0.2	Daniela Spajić (KUL)	Adapted to project template
04/07/2023	0.3	Daniela Spajić (KUL)	First complete draft
09/07/2023	0.4	Maja Nišević, Anton Vedder (KUL)	Internal review
14/07/2023	0.5	Daniela Spajić (KUL)	Integration of internal review feedback
25/08/2023 27/07/2023		Apostolos Fournaris (ISI), Kalliopi Mastoraki (CEF)	Review by ISI and CEF
28/08/2023	0.6		Second complete draft
29/08/2023 29/09/2023		Paolo Palmieri (UCC), Francesco Regazzoni (UvA)	Review by Quality Manager and Project Coordinator
26/09/2023	1.0		Final deliverable

Table of Contents

Acronyms and Abbreviations **7**
1 Executive Summary **8**
1.1 Related Documents 8
2 Introduction **9**
2.1 Structure of the Document 9
3 Data laws **11**
3.1 Introduction: A European Strategy for Data 11
3.2 General Data Protection Regulation 11
3.2.1 Introduction 11
3.2.2 Definitions and other selected aspects 12
3.3 Data Governance Act 20
3.4 Regulation on a framework for the free flow of non-personal data 21
3.5 Forthcoming 23
3.5.1 Proposal for a Data Act 23
3.5.2 Proposal for a European Health Data Space 24
4 AI Governance **27**
4.1 Introduction: The EU's approach to artificial intelligence 27
4.2 HLEG AI Guidelines 27
4.3 Proposal for an AI Act 30
4.3.1 Current state of affairs 30
4.3.2 Scope of application and selected aspects 31
5 Cybersecurity **33**
5.1 Introduction: An EU Cybersecurity Strategy for the Digital Decade 33
5.2 Data security: the General Data Protection Regulation 33
5.2.1 Data protection by design and by default 33
5.2.2 Security of processing 34
5.2.3 Data breach 35
5.3 Network security: The Network and Information Security Framework 36
5.4 AI security 37
6 Health technology framework **39**
6.1 EU Medical Devices Regulation 39
6.2 Regulation on Health Technology Assessment 40
7 Research ethics and integrity **41**
7.1 Introduction 41
7.2 Principles in biomedical ethics 41
7.3 Declaration of Helsinki 42
7.4 Declaration of Taipei 43
8 Conclusions **45**
9 Main references **46**

Acronyms and Abbreviations

AI Artificial Intelligence. 27 ff., 30 ff.

CJEU Court of Justice of the European Union. 13 ff., 17

DA Data Act Proposal. 23

DGA Data Governance Act. 20-21

DoA Description of Actions. 8

EDPB European Data Protection Board. 15 ff., 19

EDPS European Data Protection Supervisor. 20

EHDS Proposal for a regulation of the European Health Data Space. 24 ff.

ENISA European Union Agency for Cybersecurity. 19, 37

EU European Union. 9 ff.

FFNPDR Regulation on a framework for the free flow of non-personal data. 21-22

GA Grant Agreement. 8

GDPR General Data Protection Regulation. 9, 11 ff.

HLEG AI High-Level Expert Group on Artificial Intelligence. 27 ff.

IVDR In Vitro Diagnostic Regulation. 39

MDCG Medical Devices Coordination Group. 39

MDR Medical Devices Regulation. 39

NIS Network and Information Security. 36 ff.

UNCRC The United Nations Convention on the Rights of the Child. 18

WHO Word Health Organisation. 29

WMA World Medical Association. 42-43

WP Work Package. 9

WP29 Article 29 Working Party. 13, 15

1 Executive Summary

The SECURED project focuses on creating an EU cross-border health data collaboration system enabling data providers, researchers and innovators to produce new AI-based data analytics solutions. In realizing the project's objectives, the SECURED project must comply with the relevant legal and ethical requirements. This deliverable outlines the relevant moral and legal framework, including hard law (i.e., EU laws and regulations) and soft-law (i.e., recommendations, guidelines and other international instruments pertinent to the project), for the guidance of the consortium through relevant ethical and legal rules. The overview will cover frameworks related to data protection and privacy, AI, cybersecurity and medical devices. Additionally to the pertinent legal frameworks, the SECURED project must conform to relevant ethical principles to protect the interests of the individual and society. These can sometimes overlap but also differ from the legal provisions since the law does sometimes not foresee all ethical outcomes. Besides, this report will cover substantial research of other relevant acts, including guidelines (e.g., AI HLEG Ethics Guidelines on Trustworthy AI) and jurisprudence.

1.1 Related Documents

- Grant Agreement (GA) Project 101095717 - SECURED; Description of Action (DoA) Annex 1
- SECURED Deliverable D1.2 GDPR and Ethics Project Guidelines

2 Introduction

This deliverable, entitled D2.5 “Legal and ethical framework and analysis”, forms part of Work Package (WP) 2, Task 2.5, and is due at M9. This report aims to provide early guidance to the Consortium partners while raising awareness among the partners on relevant legislation and ethical considerations pertinent to the SECURED project.

This deliverable complements the first overview provided in deliverable D1.2 “GDPR and Ethics Project Guidelines” at M6, which introduced the relevant definitions concerning the General Data Protection Regulation (GDPR) and which should be considered for this deliverable. To recapitulate, the GDPR sets out the multiple obligations for data controllers and processors, in particular rules regarding the following:

- Implementation of the data protection principles (Article 5 GDPR)
- Processing of personal data and special categories of personal data based on an adequate legal basis as provided in Article 6 and 9 GDPR, respectively (both for training the algorithm and its final production).
    - Safeguards and derogations concerning the processing of special categories of personal data according to Article 9(2) GDPR for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89 GDPR).
- Ensuring and maintaining the data subject’s rights laid down in Articles 12-22 GDPR, which are:
    - Right to information
    - Right to access
    - Right to rectification
    - Right to erasure (also known as the right to be forgotten)
    - Right to restriction of processing
    - Right to data portability
    - Right to object
    - Right not to be subject to automated decision making
- Establishment of controller-processor contracts where needed (Article 28 GDPR)
- Keeping records of processing activities (Article 30 GDPR)
- Implementation and maintenance of technical and organizational measures (Article 32 GDPR)
- Conduct of Data Protection Impact Assessment (Articles 35 and 36 GDPR)
- Duty to report data breaches to national authorities and the data subject (Articles 33 and 34 GDPR)

In addition to D1.2, the deliverable D2.5 will provide a more detailed overview of the relevant definitions presented in D1.2 by providing further insight into selected pertinent aspects for the SECURED project. It gives a broader perspective considering the applicable provisions and rules within and beyond the GDPR. Thereby, D2.5 will build an essential ground for future developments by setting out a high-level overview of selected legal conditions and ethical aspects at the European Union (EU) level. As the project progresses, these guidelines will be further developed with D5.4 “Evaluation and implementation of legal and ethical requirements”, by M24 and D4.6 “Legal Validation and Recommendation report” by M36.

2.1 Structure of the Document

The following section provides an overview of the main legal and ethical frameworks in light of the project's objectives. As the SECURED project will (at least at the early stages) encompass the processing of personal health

data, Section 3 pays attention to the privacy and data protection framework and outlines selected aspects relevant to the project. Furthermore, this section considers other data laws related to data sharing and data governance that are essential to satisfy the project's promise. Section 4 provides a topical overview of the current policy developments concerning artificial intelligence at the EU level. Furthermore, it outlines the ethical guidelines building the basis for the ongoing policy discussions and drawn up by the High-Level Expert Group, a group of experts established by the European Commission. Section 5 illustrates the most relevant legal and policy sources concerning (cyber)security. Section 6 focuses on relevant frameworks regarding medical devices and health technologies. Finally, Section 7 maps a set of research ethics and integrity principles to support ethical research practices.

3 Data laws

3.1 Introduction: A European Strategy for Data

The development of the SECURED Innohub Platform and techniques encompasses data collection, processing and sharing. These are supported and based on a strong legal framework regarding data protection, safety and cybersecurity, which is essential to create citizens' trust in data-driven inventions.[1] With that in mind, the European Commission has developed a European strategy for data in order to foster the data economy in the EU whilst protecting the fundamental rights and freedoms of citizens, which are at the core of the European society.

The European strategy for data aims to increase the availability of personal data and non-personal data for the use and re-use of data and to prosper data governance. This can potentially improve several sectors, such as health and well-being, environment and public services across the EU. Data is of particular importance for developing personalized medicine, allowing care providers to address the patients' needs more individually. It also builds the fundament for developing new products in a data-agile health economy.[2]

Against this background, it must be kept in mind that the handling and processing of patient data are accompanied by a complex set of rules and principles which operate at different jurisdictional levels (e.g., national, EU, European, International) and sectors (e.g., medical care and confidentiality, research). In healthcare, the right to privacy and data protection is shaped by various hard-law and soft-law frameworks, for example, such as the European Convention on Human Rights[3], the Council of Europe's Convention for the Protection of Individuals concerning the automatic processing of personal data[4], but also national data protection laws and medical confidentiality legislations. While acknowledging that all these frameworks are relevant to the handling and processing of (personal) data, the following chapters are selective in that they provide an overarching view of the frameworks and obligations. The following sections will highlight relevant provisions and frameworks for the handling of personal data, health data and non-personal data in the SECURED project.

3.2 General Data Protection Regulation

As introduced in the preceding deliverable D1.2 " GDPR and Ethics Project Guidelines", the General Data Protection Regulation (GDPR) is the primary EU legislation on data protection, meaning the protection of an individual's personal data in the context of data processing. With that in mind, this section again stresses the importance of the GDPR and its relevance to the SECURED project. The following sections will, therefore, first introduce the aim of the GDPR and then provide further information on selected aspects that are essential to keep in mind for this project.

3.2.1 Introduction

The GDPR's goal is twofold: whilst the protection of fundamental rights and freedoms of national personal regarding the processing of personal data is an essential objective, it also seeks to facilitate the free movement of personal data.[5]

[1] European Commission, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European strategy for data COM/2020/66 final (hereinafter "A European Strategy for Data"), p. 1.
[2] Ibid., p. 1-2.
[3] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
[4] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108.
[5] Article 1 GDPR.

This piece of legislation sets out the legal requirements for personal data processing, including the legal obligations for data controllers and processors (e.g., companies, hospitals, research institutes, physicians, et cetera) and the rights of the data subjects (e.g., patients, citizens). The GDPR specifies in its provisions the territorial scope, which states that the GDPR applies to the processing of personal data by processors and controllers with an establishment in the European Union.[6] However, this is not the only scenario, and the GDPR may also apply to data controllers and processers established outside the EU. If the data controller or processor is not established in the EU, the GDPR still applies if the data processing operations are related to the offering of goods to data subjects in the EU or to the monitoring of their behavior (if such monitoring takes place in the EU).[7]

As a regulation, the GDPR is directly applicable in all EU Member States, but it does not replace or preclude the applicability of national legislation. Notably, the GDPR specifies explicitly that Member States are allowed to maintain or introduce further conditions and limitations with regard to the processing of data concerning health.[8] Consequently, diverging implementations of the regulation may exist among Member States and consortium partners are advised to check the applicable requirements, if necessary, with the responsible national Data Protection Authority.

3.2.2 Definitions and other selected aspects

The following sections elaborate on selected aspects that could become relevant for partners in the SECURED project. Especially the concepts of personal data and special categories of personal data are important as they trigger the application of the GDPR. In light of the project's goal, also the concepts of anonymization and pseudonymization will be discussed in order to raise the SECURED partners' understanding on this matter. Afterwards, a dedicated section outlines various legal bases that partners may rely on for their data processing activities. Finally, since SECURED solutions encompass the development or use of multi-party computation, synthetic data generation and federated learning techniques, data protection-related implications arising from these privacy enhancing techniques will be discussed.

3.2.2.1 Personal data

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[9] The GDPR introduces a broad concept of “personal data”. Personal data refers to “any information relating to an identified or identifiable natural person”, i.e., the data subject.[10] An identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier (e.g., a name, an identification number, location data, an online identifier).[11] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[12]

[6] Article 3(1) GDPR.
[7] Article 3(2) GDPR.
[8] Article 9(4)(a and b) GDPR.
[9] Article 2(1) GDPR.
[10] Article 4(1) GDPR.
[11] Article 4(1) GDPR.
[12] Recital 26 GDPR.

By doing so, the GDPR takes a risk-based approach to determine whether a person is identifiable.[13] The concept of "identifiability" is crucial for controllers and processors when distinguishing between anonymous and non-anonymous (hence, personal) data. Anonymization and pseudonymization techniques must be implemented adequately. Both concepts differ in that the latter (pseudonymous data) constitutes personal data and is thus subject to the scope of the GDPR, whereas truly anonymized data is not.[14] Given their particular importance, the understanding of both concepts is pivotal:

> ***Anonymisation*** is the process in which personal data is rendered anonymous.[15] According to EU law, more specifically the GDPR, anonymous data is "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[16] A dataset including personal data may encompass direct and indirect identifiers, enabling identifying an individual or making them identifiable. Direct identifiers contain specific information with reference to an individual (e.g., name or ID number). At first glance, an indirect identifier may not expose an individual but may do so individually or in combination with other indirect identifiers allowing for re-identification.[17] For data to be truly anonymous, an individual is no longer identifiable. Examples of anonymization techniques are randomization and generalization. However, whether the anonymization techniques are robust must be assessed case by case. Circumstances can change, and newly evolving techniques and practices might revert the anonymization process in the future.[18] The opinion of the Article 29 Working Party (WP29) may provide further guidance on anonymization techniques.[19]
>
> ***Pseudonymisation*** is not the same as anonymization. According to the GDPR, pseudonymisation is "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the personal data are not attributed to an identified or identifiable natural person".[20] Pseudonymous data can, therefore, in combination with additional information enable the identification of the individual, which is why pseudonymous data is still personal data. Examples of pseudonymization techniques are, for instance, encryption, hash function, tokenization.

Both concepts are essential to the anticipated development of the SECURED tools, aiming to develop privacy-friendly solutions. However, determining when a person is identifiable can be challenging when it is unclear from whose perspective the risk of (re-)identification should be determined. As stated above, recital 26 requests to consider various factors in order to determine "all the means reasonably likely to be used" (e.g., costs and time) and takes the view of the controller or another third person into account.

In this context, two court decisions should be mentioned as these are significant for assessing the identifiability of a data subject. Specifically, the court argued in favor of the so-called "relative approach", according to which the assessment of whether the data at issue is anonymous or pseudonymous is context-depended.

> In the case, ***Breyer v. Bundesrepublik Deutschland***[21]*,* the Court of Justice of the European Union (CJEU) issued a judgment dealing with the concept of "identifiability" in relation to the Data Protection Directive[22],

[13] See Article 29 Working Party, „Opinion 05/2014 on Anonymisation Techniques", Adopted on 10 April 2014, p. 6-7, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
[14] See ibid., p. 10; also see recital 26, Article 4(5) GDPR.
[15] EDPS, "10 Misunderstandings related to anonymization", <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>.
[16] Recital 26 GDPR.
[17] EDPS, "10 Misunderstandings related to anonymization", p. 2, <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>.
[18] Ibid, p. 10.
[19] Article 29 Working Party, „Opinion 05/2014 on Anonymisation Techniques", Adopted on 10 April 2014, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
[20] Article 4(5) GDPR.
[21] CJEU, Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 19 October 2016.

the predecessor of the GDPR. In the case at stake, the CJEU established that dynamic IP addresses constitute personal data if a party has the "legal means" to make an individual "identifiable". The CJEU did not consider pseudonymization as such, but it suggested that the meaning of "identifiability" is broad.[23] Therefore, if a person has the "legal means" to obtain the additional information which enables the identification of an individual related to the IP address, then the IP address is personal data. Such legal means can be considered a means reasonably likely to identify a natural person.

The CJEU reaffirmed the relative approach to the concept of personal data in a recent judgement in ***SRB v. EDPS***[24]. The general court of the CJEU stressed the importance of the legal means to access the additional information to re-identify an individual once again and the need to take the position of the data recipient into account when assessing the means reasonably likely to be used. The decision was issued with regard to Regulation (EU) 2018/1725[25], which governs the protection of individuals regarding the processing of their personal data by EU institutions and bodies. Still, it would also be relevant for the GDPR as both legislations share the exact definition of personal data.[26] Whether the decision will be subject to appeal remains to be seen.

It is important to note that the assessment of when data can be considered fully anonymised is subject to debate at the European level. Again, recital 26 GDPR considers such data anonymous "which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used (such as singling out), either by the controller or by another person to identify the person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify someone, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[27] More importantly, sharing anonymised data with the public comes with a higher burden to guarantee that it is impossible to re-identify a person and that it remains anonymous over time.[28]

SECURED partners are therefore advised to be mindful of the challenges arising concerning the concept of anonymization. This is important as the processing of personal data, including pseudonymous data, must comply with the GDPR principles and legal bases. Furthermore, it should be highlighted that the process of anonymization, meaning when personal data are being anonymized, is an action involving personal data processing and which must fulfil a legal basis to be compliant with the GDPR.

[22] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995.
[23] D Kelleher, "In Breyer decision today, Europe's highest court rules on definition of personal data", 19 October 2016, IAPP, <https://iapp.org/news/a/in-breyer-decision-today-europes-highest-court-rules-on-definition-of-personal-data/>.
[24] CJEU, Case T-557/20, SRB v. EDPS, 26 April 2023.
[25] 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, PE/31/2018/REV/1, OJ L 295.
[26] D Spajić, "Anonymous vs. pseudonymous data: the CJEU reaffirms the relative approach to the concept of personal data", CiTiP Blog, 26 April 2023, <https://www.law.kuleuven.be/citip/blog/anonymous-vs-pseudonymous-data-the-cjeu-reaffirms-the-relative-approach-to-the-concept-of-personal-data/>.
[27] Recital 26 GDPR.
[28] M Finck, F Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, Volume 10, Issue 1, February 2020, pages 11–36, <https://doi.org/10.1093/idpl/ipz026>.

3.2.2.2 Special categories of personal data

Special categories of personal data are more sensitive due to the risks their processing poses concerning an individual's fundamental rights and freedoms. Article 9(1) GDPR enlists the following data as special categories of personal data:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions, religious or other beliefs, including philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data processed for the purpose of uniquely identifying a person;
- Data concerning health;
- Data concerning a person's sex life or sexual orientation.

Article 4(15) GDPR adopts a broad interpretation of the notion of ***data concerning health***, encompassing all "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". The CJEU[29] confirmed the wide interpretation of the term "data concerning health" in order to include all data pertaining to the past, current or future health status.[30] Recital 35 GDPR provides some further examples regarding data concerning health, covering, for instance, any information on medical history, treatments, et cetera, independent of its source (e.g., physician, hospital, medical device). It could include any information that may be collected in an administrative context during the registration for healthcare provision, but also a number, symbol or particular assigned to a natural person to uniquely identify a person for health purposes. According to the Article 29 Working Party (WP29), the predecessor of the European Data Protection Board (EDPB), concluded that information, such as the fact that someone has a broken leg, wears glasses or contact lenses, a person's intellectual and emotional capacity (IQ), constitutes data about the health status of a person.[31]

Genetic data "means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".[32] The notion covers particularly "chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained".[33]

The categorization of these data types is significant for determining the legal grounds. The legal bases for processing special categories of personal data are laid down in Article 9 GDPR, whereas the processing of (i.e., regular personal data) personal data can be legitimized based on Article 6 GDPR. Special categories of personal data are subject to higher protection, as their processing result in higher risks for the data subject. Article 9(1) GDPR, therefore, generally prohibits the processing of such data types. However, exceptions to the prohibition may apply (Article 9(2) GDPR).

Against this background, it should be noted that data processing and sharing concerning health and genetic data is subject to different governance models and national laws. Member States may introduce special conditions and

[29] CJEU, Case C-101/01, Lindqvist, 6 November 2003, para. 50.
[30] See also recital 35 GDPR.
[31] Article 29 Working Party, Annex to Letter from the WP29 to the European Commission, DG CONNECT on mHealth, p. 2, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>.
[32] Article 4(13) GDPR.
[33] Recital 34 GDPR.

limitations regarding the processing of genetic data and data concerning health.[34] Different legal bases may apply depending on the aim for which the data is processed, such as patient care, cross-border access to and sharing of data, or the re-/use of data for scientific research. Hereinafter, some of the main provisions of the GDPR that could become relevant in the SECURED project will be outlined, namely explicit consent, consent of children and scientific research:

- ***Explicit consent:*** Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[35] From this definition, four crucial elements can be retrieved for obtaining valid consent: *free, specific, informed* and *unambiguous.* Additionally, if special categories of personal data are processed, consent must also be *explicit* according to Article 9(2)(a) GDPR.[36] The following sections will outline the main features of the five elements of explicit consent:

    - *Freely given*: This requirement implies that the data subject must have a real choice and control when consenting to the data processing without having to fear possible negative consequences. Consequently, the data subject must be able to refuse or withdraw his or her consent at any time.[37] The notion also takes into account a possible imbalance between the data controller and the data subject, so that it needs to be assessed whether a different legal basis may be more appropriate. For instance, recital 43 indicates that public authorities can unlikely rely on consent. The EDPB suggests that a power imbalance might also exist in the medical setting when a clinical trial participant is not in good health or belongs to a socially or economically disadvantaged group.[38]

    - *Specific*: The element of specificity requires that consent must be given concerning one or more specific purposes, whereby the data subject is required to have a real choice in relation to each of these purposes. The need for specific consent has to be seen in relation to the principle of purpose limitation as embedded in Article 5(1)(b) GDPR, serving as a safeguard against broadening purposes. The condition of "specific" requires an "opt-in"-approach for data subjects to give specific consent for a particular purpose.[39]

    - *Informed*: In line with the transparency principle, data subjects must be provided with clear information to make an informed decision. The information (in accordance with Articles 13 and 14 GDPR) must be provided prior to obtaining consent. Where consent is obtained to process or share data including multiple controllers, the EDPB highlights that these should be named. Articles 13 and 14 GDPR also require controllers to provide a complete list of recipients or categories of recipients, including processors.[40]

    - *Unambiguous*: When consenting, data subjects must indicate their wishes unambiguously. It requires a statement or clear affirmative act. A clear affirmative act encompasses a deliberate action through a written or oral statement. Silence, inactivity, or pre-ticket "opt-in"-boxes cannot be viewed as an indicator of consent.[41]

[34] See Article 9(4) GDPR.
[35] Article 4(11) GDPR.
[36] Article 9(2)(a) GDPR.
[37] EDPB, "Guidelines 05/202 on consent under Regulation 2016/679", Version 1.1, Adopted on 4 May 2020, p. 7-8, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
[38] EDPB, "Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))", p. 6, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf>.
[39] EDPB, "Guidelines 05/202 on consent under Regulation 2016/679", Version 1.1, Adopted on 4 May 2020, p. 13-15, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
[40] Ibid., p. 15-16.
[41] Ibid., p. 18.

- *Explicit*: Finally, to process sensitive data such as data concerning health, consent also has to be explicit. The notion "explicit" relates to how the data subject expresses his or her consent, requiring that individuals make an express statement of approval (e.g., a written statement, filling in an electronic form, sending an email, using an electronic signature). Although oral statements can suffice to obtain explicit consent, it may be challenging to proof when in need to provide evidence.[42]

- ***Consent of children:*** The GDPR established additional protection mechanisms for vulnerable people. A specific area of concern in the GDPR is the consent obtained with regard to children's data. Article 8 GDPR creates additional obligations for the protection of children in terms of their personal data. More specifically, where consent is given in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. However, the processing of data from children below 16 years should only be lawful if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.[43] The GDPR offers some flexibility regarding the age limit as Member States can provide a lower age. Nonetheless, the age cannot be below 13 years.[44] Subsequently, Article 8 applies where the following two requirements are fulfilled:

  - The processing is based on consent as per Article 6(1) GDPR, and
  - The processing is related to the offer of information society services directly to a child.

  The protection of children in relation to their personal data is vital as they may be less aware of the risks, consequences, safeguards and rights.[45] According to recital 38, this protection should apply in particular where their data is processed for marketing purposes or user profiles when using services offered to children. The term "in particular" shows that the protection is not limited to marketing or profiling. It encompasses the collection of personal data regarding children in a wider sense.[46] The EDPB refers in its guidelines on consent also to European jurisprudence. To this end, the CJEU decided that "information society services" encompass contracts and other services which are conducted or transmitted online.[47] The GDPR borrows the definition of the term "information society service" from Article 1(1)(b) Directive (EU) 2015/1535[48]. According to Annex I of the Directive (EU) 2015/1535, "medical examinations or treatments at a doctor's surgery using electronic equipment where the patient is physically present" should not be considered as an "information society service". However, other medical services might fall nonetheless under this definition.

  The question of whether a child can provide valid consent depends on their maturity level. Whilst not interfering with the rules laid down in national contract laws, the Article 29 Working Party argued that children should be asked when data is processed about them, as the right to data protection protects the child directly and not their representatives.[49] Article 12(1) and recital 58 GDPR embed a similar consideration.

[42] Ibid., p. 20-21.
[43] Article 8(1) GDPR.
[44] Article 8(1) GDPR.
[45] Recital 38 GDPR.
[46] EDPB, "Guidelines 05/202 on consent under Regulation 2016/679", Version 1.1, Adopted on 4 May 2020, p. 25-26, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
[47] Ibid., p. 26-27, referring to CJEU, Case C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, 2 December 2010, para. 22 and 28.
[48] See Article 4(25) GDPR, referring to Article 1(1)(b) Directive (EU) 2015/1535.
[49] E Kosta, "Article 8 Conditions applicable to child's consent in relation to information society services", in: C Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic), <https://doi.org/10.1093/oso/9780198826491.003.0037>, referring to Article 29 Working Party, "Opinion 01/2012 on the data protection reform proposals", Adopted on 23 March 2021, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.

In light of the specific protection children merit, "any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand"[50].

Other international policy documents, such as the UN Convention on the Rights of the Child (UNCRC) or the Council of Europe guidelines[51], suggest 18 as "the age of majority" without considering it a hard threshold.[52] Rather, the "evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present convention."[53] With regard to the right of children, the UNCRC considers that "[no] child shall be child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home"[54].[55] Concerning the processing of genetic data or data related to the child's mental or physical health, the Council of Europe specifies that states should ensure that processing of such special categories of data shall be only allowed where appropriate safeguards are laid down in law.[56]

- ***Scientific research:*** The notion of scientific research is not legally defined in the GDPR. Recital 159 stipulates that "the processing of personal data for scientific research should be interpreted in a broad manner". The derogations in regulation provisions for the processing of data concerning health and genetic data for scientific research have arguably caused legal uncertainty due to the deviating implementation throughout the European countries. However, the EDPB argues that the concept of "scientific research" should "not be stretched beyond its common meaning", understanding research as "a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice".[57] Article 89(1) GDPR requires the implementation of appropriate safeguards (e.g., data minimization, anonymisation) where the data processing activities for research are based on other legal bases than consent, such as for the further data processing according to Article 5(1)(b) GDPR, or for the processing of personal data or special categories of personal data according to Article 6(1)(e) or (f), or Article 9(2)(j), respectively. Suppose consent is used as the legal basis for the purpose of conducting research. In that case, consent for the data processing must be differentiated from other types of consent (e.g., consent for the provision of healthcare, consent as a procedural obligation according to the regulation on clinical trials[58]).[59] Regarding data processing activities, recital 33 GDPR provides some flexibility regarding the concept of consent obtained for scientific research. Recital 33 does not disregard or revoke the consent requirements enshrined in the GDPR. Still, it acknowledges that "[it] often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to consent to certain areas of scientific research when in keeping with recognised

[50] Recital 58 GDPR.
[51] Council of Europe, "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.
[52] See, for instance, Section 1 Council of Europe Guidelines, ibid.
[53] Article 5 UNCRC, UN Convention on the Rights of the Child accessible here: <https://www.unicef.org.uk/wp-content/uploads/2016/08/unicef-convention-rights-child-uncrc.pdf>; similarly also: Council of Europe, "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", para. 2 on p. 12, para. 28 on p. 16, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.
[54] Article 16 UNCRC.
[55] E Kosta, 'Article 8 Conditions applicable to child's consent in relation to information society services', in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic), https://doi.org/10.1093/oso/9780198826491.003.0037, accessed 28 June 2023.
[56] Council of Europe, "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", para. 32 on p. 17, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.
[57] EDPB, "Guidelines 05/202 on consent under Regulation 2016/679", Version 1.1, Adopted on 4 May 2020, p. 25-26, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, p. 30.
[58] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, p. 1 (Clinical Trial Regulation).
[59] EDPB, "Guidelines 05/202 on consent under Regulation 2016/679", Version 1.1, Adopted on 4 May 2020, p. 30, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." It thus allows for loosening the "specificity"-requirement to the extent that the purpose "may be described at a more general level". However, in light of the strict requirements for the processing of sensitive data, the application of recital 33 will be subject to more rigid interpretation and requires high scrutiny.[60]

To sum up, data controllers and processors must determine an appropriate legal basis according to the purpose of the envisioned data processing activity and comply with data protection principles. When processing special categories of personal data, attention must be paid to domestic rules. SECURED partners are therefore advised to consult regarding their national legislations prior to any envisaged data processing activity.

3.2.2.3 Privacy enhancing techniques

The SECURED project's objective is the creation of a one-stop collaboration hub (i.e., the SECURED Innohub) that creates a secure and trusted environment for decentralized, cooperative processing, including secure multi-party computation techniques, synthetic data generation, data anonymization and an anonymization assessment. The previous section outlined the legal considerations for assessing anonymity in the GDPR and relevant case law. Beyond that, account should be taken of possible challenges and debates related to other privacy-enhancing processing techniques. These are legally closely connected to the concept of (non-)personal data and subsequently to the question regarding the applicability of the GDPR. With that in mind and considering the SECURED project's goals, the following sections will elaborate on some legal considerations in relation to multi-party computation, synthetic data, and federated learning.

- ***Multi-party computation:*** In its recommendation 01/2020, the EDPB considered the deployment of multi-party computation as an "effective supplementary measure" for transferring data internationally.[61] Multi-party computation, in general terms, enables multiple entities to process data jointly without revealing their data to each other.[62] This technique shall allow stakeholders to share "data insights while keeping the data itself private".[63] However, as long as personal data is used, for example, to store data, the GDPR applies.[64] Furthermore, it seems unclear whether this technique anonymizes or pseudonymizes.[65] ENISA, for instance,

[60] Ibid., p. 30.
[61] K Koerner, "Multiparty computation as supplementary measure and potential data anonymization tool", 27.10.2021, <https://iapp.org/news/a/multiparty-computation-as-supplementary-measure-and-potential-data-anonymization-tool/>; EDPB, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", Version 2.0, Adopted on 18 June 2021, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>.
[62] See EDPB, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", p. 32-33, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>; see also: ENISA, "Data Pseudonymisation: Advanced Techniques and Use Cases", 28.01.2021, p. 23, <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.
[63] K Koerner, "Multiparty computation as supplementary measure and potential data anonymization tool", 27.10.2021, <https://iapp.org/news/a/multiparty-computation-as-supplementary-measure-and-potential-data-anonymization-tool/>.
[64] A Treiber, D Müllmann, T Schneider, I Spiecker genannt Döhmann (2022) Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. In Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES'22). Association for Computing Machinery, New York, NY, USA, 69–82, p. 73, <https://doi.org/10.1145/3559613.3563192>.
[65] See, for instance, L Helminger, C Rechberger (2022) Multi-Party Computation in the GDPR. In: Schiffner, S., Ziegler, S., Quesada Rodriguez, A. (eds) Privacy Symposium 2022. Springer, Cham. <https://doi.org/10.1007/978-3-031-09901-4_2>.

refers to multi-party computation as a pseudonymization technique as a privacy-by-design measure.[66] At last, although the multi-party computation technique may secure the input data, there seems to be a risk that the generated output may reveal personal information if the input data is personal data.[67] Under these circumstances, personal data would have been transmitted and exposed.

- ***Synthetic data generation:*** Synthetic data is often referred to as "fake data" or "artificial data", as it is artificially created. At the same time, it maintains the statistical properties of a person's original data. Synthetic data generation has thus been regarded as an effective anonymization technique.[68] However, in the discussion regarding the creation and use of synthetic data, scholars have challenged the conception that synthetic data constitutes "fake data" or "artificial data", terms which typically imply that synthetic data are non-identified data.[69] Despite this opposing view, there is a general concern at what point synthetic data are personal or non-personal along the spectrum. The European Data Protection Supervisor (EDPS) thus suggests that privacy assurance assessments should be conducted in order to evaluate to what extent data subjects can be identified.[70]

- ***Federated learning:*** Finally, using federated learning has received significant interest as a privacy-preserving data-sharing solution. The general idea behind federated learning is that the algorithm is sent to various entities to train the model on the dataset without sharing the actual data. While federated learning has the potential to maintain an individual's privacy, it does not exempt from the application of the GDPR. For instance, if a developer sent a model to a hospital in order to develop an algorithm based on patients' health record data, then this processing activity would run on the patients' health data.[71] Using personal data and sensitive data for the training of algorithms must hence comply with the requirements and obligations under the GDPR. Furthermore, attention must be paid particularly to the data minimization principle, as only such personal data that is truly necessary to achieve the purpose of the processing should be accessed.[72]

Data anonymization is a complex undertaking which requires careful and ongoing (re-)evaluation of the circumstances according to state-of-the-art techniques. As the SECURED project seeks to develop multiple data anonymisation tools, these techniques must be reviewed with the necessary scrutiny.

3.3 Data Governance Act

The Data Governance Act[73] (DGA) is a legislation that seeks to foster data availability by increasing trust in data sharing and overcoming technical obstacles related to data reuse. The regulation entered into force on 23 June 2022 and will become applicable from September 2023 onwards. It supports the establishment of European data spaces for

[66] See ENISA, "Data Pseudonymisation: Advanced Techniques and Use Cases", 28.01.2021, p. 23, <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.
[67] L Helminger, C Rechberger (2022) Multi-Party Computation in the GDPR. In: Schiffner, S., Ziegler, S., Quesada Rodriguez, A. (eds) Privacy Symposium 2022. Springer, Cham. <https://doi.org/10.1007/978-3-031-09901-4_2>.
[68] CA Fontanillo López, A Elbi, "On synthetic data: a brief introduction for data protection law dummies", European Law Blog, 22.09.2022, <https://europeanlawblog.eu/2022/09/22/on-synthetic-data-a-brief-introduction-for-data-protection-law-dummies/>.
[69] Ibid., referring also to T Stadler, B Oprisanu, C Troncoso, "Synthetic Data – Anonymisation Groundhog Day", 31st USENIX Symposium, <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>.
[70] EDPS, "Synthetic data", <https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en>.
[71] Li Q et al. (2021) A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection. arXiv:1907.09693v7
[72] EDPS, "Federated Learning", <https://edps.europa.eu/press-publications/publications/techsonar/federated-learning_en>.
[73] 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), PE/85/2021/REV/1, OJ L 152.

various sectors, including, but not limited to, the healthcare sector. In terms of the regulation's subject matter, the act sets out rules for:

- The re-use of certain data types held by public bodies;
- A notification and supervisory framework for data intermediation services;
- A framework for voluntary registration of entities collecting and processing data for altruistic purposes;
- A framework for the creation of a European Data Innovation Board.[74]

The regulation applies to data, which is defined in a broad manner. Specifically, according to Article 2(1) DGA, data means "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording". Thereby, the regulation includes personal data[75] and non-personal data[76] into its scope of application.

As the DGA seeks to improve the conditions for data sharing, data intermediaries will play an important role. Especially ***data altruism organisations*** are a specific type of data intermediaries foreseen under the DGA and will foster the sharing of personal and non-personal data for altruistic purposes, such as scientific research. A crucial goal of such organisations will be the creation of data repositories.[77] In order to support trust and the availability of data for altruistic purposes, the DGA introduces a new tool, the so-called ***data altruism consent form***.

Under the DGA, the data altruism consent form is a mechanism that shall facilitate the *voluntary* sharing of data by data holders as well as by individuals. According to Article 25 DGA, the European Commission shall adopt implementing acts for establishing and developing a European data altruism consent form. The DGA defines ***data altruism*** in Article 2(16) DGA as:

> "*the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest*".

At the time of writing, legal uncertainties exist with regard to the data altruism consent form and its development remains to be followed. This is, in particular, the case as the DGA refers to the GDPR in terms of the concept of consent as a legal basis for the processing of personal data (Article 6(1)(a) GDPR) and special categories of personal data (Article 9(2)(a) GDPR). Individuals should be able to give and withdraw their permission at any time.[78]

3.4 Regulation on a framework for the free flow of non-personal data

The Regulation on a framework for the free flow of non-personal data in the European Union[79] (FFNPDR) became applicable on 28 May 2019 and promotes the free flow of data across Europe and IT systems in Europe by setting out

[74] Article 1(1)(a-d) DGA.
[75] Article 2(3) DGA refers to Article 4(1) GDPR for the definition of personal data.
[76] According to Article 2(4) DGA, non-personal data means data other than personal data.
[77] Recital 46 DGA.
[78] See recital 50 DGA, and Article 25(3) DGA.
[79] 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, PE/53/2018/REV/1, OJ L 303.

rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.[80] It applies to ***non-personal data***, meaning other than personal data[81], and thereby ensures a comprehensive approach concerning the free movement of all data within the EU.[82] The FFNPDR incorporates three distinctive features:

- Member States are prohibited from imposing data localisation requirements unless this is in the interest of public security and proportionate;
- The regulation creates a cooperation mechanism enabling competent authorities to exercise data access rights; and
- It seeks to motivate the industry to establish a self-regulatory code of conduct regarding the change of service providers and the porting of data.[83]

Against this background, it might not always be clear which provisions apply when personal data and non-personal data are present in mixed datasets. Health data can be included in mixed datasets. This could be the case, for instance, in electronic health records or mobile health applications.[84] Dividing between the personal and non-personal data parts in datasets can become blurry, especially through rapid technological developments. The FFNPDR took this into account: Where the data set contains personal and non-personal data, the FFNPDR clarifies that the regulation applies to the part of the data set containing the non-personal data. This requires that both (personal and non-personal) datasets are not inextricably linked. When both datasets are inextricably linked, meaning that separating the two would be impossible or be considered to be economically inefficient or technically unfeasible, then the GDPR shall apply.[85] On this note, the Commission has published guidance on the interaction between the FFNPDR and the GDPR in alignment with Article 8(3) FFNPDR.[86]

The FFNPDR applies primarily to the processing of non-personal data in the EU. However, it may constitute a valuable instrument for SECURED partners when identifying the concepts of "personal data" and "non-personal data", as well as the applicability of the FFNPDR and GDPR in relation to mixed datasets.

[80] See Article 1 FFNPDR.
[81] See Article 3(1) FFNPDR.
[82] European Commission, "Free flow of non-personal data", <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>.
[83] Communication From The Commission To The European Parliament And The Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN>.
[84] Ibid..
[85] Article 2(2) FFNPDR; ibid..
[86] Communication From The Commission To The European Parliament And The Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN>.

3.5 Forthcoming

This section provides an overview on forthcoming legal frameworks that are currently discussed at the EU level. In particular, attention will be paid to the proposal for the so-called "Data Act" and the European Health Data Space. Both drafts are currently subject to debate at the EU level and aim to foster the availability of data.

3.5.1 Proposal for a Data Act

The proposal for a regulation on harmonised rules on fair access to and use of data (Data Act)[87] is a draft legislation which was adopted on 23 February 2022 and aims to foster the Commission's goal of a thriving data economy. The measures laid down in the proposed regulation will complement the Data Governance Act. While the Data Governance Act sets out provisions for creating processes and structures to make data available, the Data Act (DA) seeks to determine who can gain value and under which requirements.[88] By doing so, the Data Act pursues to maximise the access to and use of data created through IoT-devices by consumers and businesses.[89] In its current form, once enforced, the regulation would encompass an array of connected devices, including medical and health devices.[90] It applies to manufacturers, suppliers, data holders, data recipients, public sector bodies and Union organisations, and providers of data processing services.[91]

Data, under the Data Act proposal, is widely defined, encompassing "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording"[92], while derived or inferred data should not be considered to be within the scope of the legislation[93]. It lays down provisions on making data available by creating rules on data sharing between business to consumer, business to business, and business to government. The proposal is a complex framework envisioning to govern multiple different themes that are pertinent to research, such as:[94]

- Facilitate access and use to data from consumers and businesses by implementing access obligations on businesses in case of exceptional needs or public interest;
- Enable the switching between cloud and edge service in order to provide access to competitive and interoperable data processing services;
- Support the development of interoperability standards for data to facilitate the use between sectors and to remove data sharing barriers across domain-specific European Data Spaces.[95]

In healthcare, a noteworthy feature of the data act proposal concerns the data sharing obligation to be created in the context of business-to-government data sharing. Chapter 5 of the data act proposal introduces the notion "exceptional need", which obliges businesses to share data essentially in response, prevention or recovery of a public

[87] Proposal for a Regulation Of The European Parliament And Of The Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.
[88] European Commission, "Data Act", <https://digital-strategy.ec.europa.eu/en/policies/data-act>.
[89] Chapter II Data Act.
[90] EDPB-EDPS (2022) Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Adopted on 4 May 2022, p. 2, 3 and 8; see also recital 14 Data Act.
[91] Article 1(2)(a-e) Data Act proposal.
[92] Article 2(1) Data Act proposal.
[93] Recital 14 Data Act proposal.
[94] European Commission, Directorate-General for Research and Innovation, Eechoud, M., Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research, Publications Office of the European Union, 2022, p. 32, <https://data.europa.eu/doi/10.2777/71619>.
[95] Ibid., p. 32; see also explanatory memorandum, data act proposal.

emergency.[96] Besides, the Data Act foresees an extended right to data portability, allowing users to share their data with third parties by having their non-personal data ported.[97] How this right will apply in practice in relation to the data portability right enshrined in the GDPR (and the European Health Data Space proposal) remains to be seen.[98] It is worth following the legislative developments as this regulation could become relevant within the SECURED project, for instance, where partners would become data holders as defined under the regulation.

The Data Act proposal, if adopted, will lay out rules on the sharing of data between businesses, businesses and consumers, and businesses and governments. For instance, the proposal foresees obligations for private entities who qualify as data holders to make data available to governmental bodies (such as public health entities). Also, the Data Act seeks to implement an (in comparison to the GDPR) extended right to data portability, allowing users to share their non-personal data. However, considering that the text is still a provisional draft, it remains to be seen how the act and its rules will be enforced.

3.5.2 Proposal for a European Health Data Space

On 3 May 2022, the European Commission adopted the proposal for a Regulation on the European Health Data Space (EHDS).[99] In light of the aim to establish common European Data Spaces across different fields, this draft constitutes the first piece of legislation that targets the creation of a European Data Space in a specific domain, i.e., the healthcare sector.

3.5.2.1 Introduction

The provisions on the secondary use of data concerning health data will have to change due to a new proposal that is currently subject to discussion, namely the proposal for a Regulation on the European Health Data Space (EHDS)[100]. The EHDS aims to foster easier sharing of and access to health data stored on electronic health data records. By doing so, the proposal does not merely seek to enhance better healthcare delivery but also to foster the further use of the data collected for healthcare provision for processing activities such as medical research, healthcare innovation, or personalized medicine.[101] The current EHDS proposal refers to the former as the primary use of health data, and the latter as the secondary use of health data.

Some of the mechanisms are intended to foster the availability and sharing of health data are data altruism, to enhance the data subject's right to data portability and to promote interoperability between electronic health record systems.[102] Thereby, the EHDS proposal complements various existing and forthcoming EU legislations, including, amongst other things, the GDPR, MDR, DGA, NIS Directive or the proposed Data Act.[103] For instance, in comparison to the GDPR, the EHDS proposal seeks to provide more specific rules for the processing of health data (i.e., electronic health record data) in the medical sector. It also foresees the establishment of a mandatory cross-border infrastructure enabling the primary use and for the secondary use of electronic health data.[104] By providing new essential conditions for the data altruism consent form, the DGA also provides generic requirements for the

[96] See Article 15 and recital 58 Data Act proposal.
[97] Article 5 Data Act proposal.
[98] D Spajic, T Lalova-Spinks, "The broadening of the right to data portability for IoT products: Who does the Act actually empower?", p. 27-31, in: C Ducuing, T Margoni, L Schirru (eds.), "CiTiP Working Paper Series – White Paper on the Data Act Proposal", 26 October 2022, <https://www.law.kuleuven.be/citip/en/Publications/citip-whitepaperdataact.pdf>.
[99] Proposal for a Regulation Of The European Parliament And Of The Council on the European Health Data Space COM/2022/197 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>.
[100] Proposal for a Regulation Of The European Parliament And Of The Council on the European Health Data Space COM/2022/197 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>.
[101] Ibid., explanatory memorandum, p. 2.
[102] Ibid., explanatory memorandum, p. 3-4.
[103] Ibid., explanatory memorandum, p. 3.
[104] Ibid., Article 1(2)(a-b).

facilitation of the secondary use of data without focusing on the healthcare sector. Similarly, the proposal for a Data Act seeks to foster data portability which can possibly include health data but, again, without putting this specific data type into its focus.[105]

At the time of writing, the EHDS proposal is structured across eight chapters. Chapter I sets out provisions on the subject matter and scope of application, whereas chapter II creates rights and mechanisms substituting the data subject's rights offered under the GDPR. Chapter III regulates the implementation of a mandatory self-certification scheme for electronic health record systems related to interoperability and security. Chapter IV focuses on the rules on the secondary use of electronic health record data for, for instance, research, patient safety, policy making and more. Chapters V and VI lay down measures for building national capacities for the development of the European health data space and the establishment of a European health data space board, respectively. Chapter VII enables the European Commission to implement delegated acts with regard to the European health data space. Finally, chapter VIII includes provisions on cooperation and penalties. The following section will provide an overview of selected definitions and requirements under the current EHDS proposal, whilst bearing in mind that the framework may be subject to changes.

3.5.2.2 Scope of application and selected aspects

The EHDS proposal applies, amongst other things, to manufacturers and suppliers of electronic health record systems and wellness applications placed on the market and put into service.[106] It also applies to data controllers and processors established in the Union who are processing the electronic health data of EU citizens.[107] In general, this framework sets out provisions for the placing on the market, making available on the market or putting into service of electronic health records systems and lays down rules and mechanisms to support the ***primary and secondary use of electronic health data***.[108]

The primary use of electronic health data is defined as

> "*means the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services*"[109].

The secondary use of electronic health data means

> "*the processing of electronic health data for purposes set out in Chapter IV of this Regulation. The data used may include personal electronic health data initially collected in the context of primary use, but also electronic health data collected for the purpose of the secondary use*"[110].

Both definitions have been subject to discussion and as the framework is still a draft, the text and its definitions may be altered. Overall, with the aim of unleashing the potential of health data, the regulation fosters control over one's health data, for instance, through an enhanced right to data portability. According to the proposal, individuals should be able to transmit their electronic health data, including inferred data, in a secured manner irrespective of the legal basis that builds the ground for the processing of the electronic health data[111]. However, while this right should apply to all health data stored on electronic health records, individuals should also be able to select what data they want or do not want to share.[112] To facilitate this right and the sharing of patient data among health professionals, the interoperability of electronic health data needs to be ensured.[113] To this end, the EHDS proposal suggests providing

[105] Ibid., explanatory memorandum, p. 4-5.
[106] Article 1(3)(a) EHDS proposal.
[107] Article 1(3)(b) EHDS proposal.
[108] See Article 1(2) EHDS proposal, in particular Article 1(2)(lit. b-e) EDHS proposal.
[109] Article 2(2)(d) EHDS proposal.
[110] Article 2(2)(e) EHDS proposal.
[111] Recital 12 EHDS proposal.
[112] Recital 13 EHDS proposal.
[113] Recital 16 EHDS proposal.

healthcare professionals with adequate means (e.g., the deployment of portals for health professionals) for introducing and using such data.[114]

Furthermore, the increased use and sharing of health data for better healthcare services, research and innovation should be enabled through a consistent and trustworthy set-up.[115] The regulation creates strict requirements for researchers, industry and other institutions to access such data. They will have to submit a data access application to so-called health data access bodies, which will be set up in every EU Member State and which will be connected to the EU-infrastructure for the secondary use of data (HealthData@EU).[116] Article 34 EHDS proposal defines purposes for which electronic health data can be processed for secondary use, such as public interest in the area of public and occupational health[117], education or teaching activities in the health or care sector[118], or scientific research related to health or care sectors[119]. Access will only be possible for the purpose indicated in the application.[120] Health data access bodies should provide electronic health data in an anonymous form if the purpose can be achieved with such data.[121] Also, the mechanism of data altruism established under the Data Governance Act will support the secondary use of health data.[122] In conclusion, as the EHDS proposal seeks to create (forthcoming) rules for the use and reuse of data in healthcare, this framework may be particularly relevant to the SECURED project once transposed.

The overall objective of the European Health Data Space proposal is to facilitate the primary and secondary use of electronic health record data. Furthermore, it pursues to establish mandatory cross-border infrastructure for the primary and secondary use of electronic health data and introduces specific rights for data subjects (such as the right to access electronic health data or to receive an electronic copy as per Article 3 (1 and 2) EHDS proposal). While the draft promises to be pertinent to the SECURED project due to its aim to enable the primary and secondary use of health data, the framework is still in the proposal stage and may be subject to change before being approved.

[114] Recital 16 EDHS proposal.
[115] European Commission, "European Health Data Space", <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en>.
[116] European Commission, "European Health Union: A European Health Data Space for people and science", press release, 3 May 2022, <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711>; see also Articles 36, 37, 45 EHDS proposal.
[117] Article 34(1)(a) EHDS proposal.
[118] Article 34(1)(d) EHDS proposal.
[119] Article 34(1)(e) EHDS proposal.
[120] Article 44(1) EHDS proposal.
[121] Article 44(2) EHDS proposal.
[122] See Article 40 EHDS proposal.

4 AI Governance

4.1 Introduction: The EU's approach to artificial intelligence

The Commission strives to achieve excellent innovation aligned with people's trust, safety and fundamental rights consistently throughout the EU. Especially in the field of medicine, artificial intelligence (AI) has great potential to support care providers in clinical decision-making and diagnostic accuracy by improving the review of radiological images or the analysis of medical data, thereby creating benefits for patients and improving the healthcare system.[123] Considering the benefits that AI can bring to healthcare and other sections, the European strategy for artificial intelligence was launched in April 2018 and has experienced rapid developments since then. At the EU level, the initial work towards implementing an AI framework commenced with the establishment of the High-Level Expert Group on AI (HLEG).[124] In 2018, 52 experts joined forces to support the European Commission in transposing the EU Strategy on Artificial Intelligence. This cooperation resulted in the creation of the HLEG ethics guidelines for Trustworthy AI[125], which has been the steering ethics guidance on AI within the EU. The coordinated plan on AI put forward by the Commission aims for the strategic alignment between the European Commission, Member States, Norway and Switzerland in order to prevent fragmentation across the EU and create a resilient economy.[126] Furthermore, the Commission recently put forward the first draft of the legislation, i.e., the AI Act, that governs the use and development of AI. By implementing these two pillars, the EU seeks to accelerate the potential that trustworthy AI can bring and to tackle the safety risks of this new technology by tacking a human-centric approach that puts the human first.[127]

4.2 HLEG AI Guidelines

The HLEG developed the following definition of AI, which considers AI as a technology and a scientific discipline and sets the basis for the identification of a framework for achieving the creation of trustworthy AI:

> *"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*
>
> *As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning,*

[123] European Commission, ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence COM(2021) 205 final, ANNEX, p. 40-41, <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.
[124] AI Act, explanatory memorandum, p. 8.
[125] High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", 8 April 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
[126] European Commission, "Coordinated Plan on Artificial Intelligence", <https://digital-strategy.ec.europa.eu/en/policies/plan-ai#:~:text=The%20key%20aims%20of%20the,AI%20policy%20to%20avoid%20fragmentation.&text=The%20Coordinated%20Plan%20on%20Artificial%20Intelligence%202021%20Review%20is%20the,global%20leadership%20in%20trustworthy%20AI.>.
[127] Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - Fostering a European approach to Artificial Intelligence COM/2021/205 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN>.

scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).”[128]

There are three core elements relevant to enable the creation of trustworthy AI, namely that AI systems must be lawful, ethical and robust:[129]

- *Lawfulness:* AI-driven systems have to comply with relevant legal frameworks throughout its entire lifecycle;
- *Ethical:* AI has to respect ethical values and principles;
- *Robustness:* AI systems have to be technically robust while considering their social environment in order to prevent harm to citizens.

The foundation of trustworthy AI is the acknowledgement of mainly four ethical principles, namely respect for human autonomy, the prevention of harm, fairness and explainability.[130] As the HLEG's aim is to go beyond a list of ethical principles in its ethics guideline[131], the expert group set up multiple criteria to provide guidance, particularly on the last two mentioned core elements for the realisation of trustworthy AI, i.e., facilitating ethical and robust AI.[132] In a nutshell, the experts established the following seven requirements (composed of technical and non-technical methods) that trustworthy AI should fulfil:

Ethics principles of the HLEG	
Human agency and oversight:	Users of AI should be able to make informed choices and autonomous decisions. AI systems should support users in this, facilitate fundamental rights and secure an individual's autonomy and decision-making. Human oversight ensures that human autonomy is guaranteed. Where fundamental rights are at risk, the impact on the fundamental rights should be assessed.[133]
Technical robustness and safety:	AI-driven systems need to be developed in a way that prevents unexpected and unintentional harm, also when changes are made later on in the system. Obviously, securing AI systems against malicious attacks is essential. They should also be secured through safeguards in case of a fallback. A high accuracy level is fundamental when human lives are affected. Where inaccurate outcomes are unavoidable, the likelihood of such errors should be indicated. AI results should be reliable and reproducible.[134]
Privacy and data governance:	Privacy and data protection must be secured throughout the AI lifecycle. The quality of the data and their integrity must be ensured. This is particularly necessary in terms of social bias, inaccuracies, and other errors and needs to be tackled before the training commences. Data protocols determining under which conditions and by whom data can be accessed should be implemented.[135]

[128] High-Level Expert Group on Artificial Intelligence, “A Definition of AI: Main capabilities and disciplines”, 8 April 2019, p. 6, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
[129] Ibid., p. 2.
[130] Ibid., p. 8.
[131] High-Level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, 8 April 2019, p. 2, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
[132] Ibid., p. 2.
[133] Ibid., p. 15-16.
[134] Ibid., p. 16-17.
[135] Ibid., p. 17.

Transparency:	The data sets and processed applied to facilitate AI-decisions should be documented in order to make them and the reasons building the ground for the decisions traceable and transparent. Both technical processes and human decisions should be explainable so that it enables humans to understand and trace decisions. When humans are interacting with an AI system, this should be made clear.[136]
Diversity, non-discrimination, and fairness:	To avoid direct or indirect prejudice or discrimination, unfair bias in training and operational data sets must be prevented. AI-systems should be inclusive and accessible for everyone (irrespective of age, skills, etc.) through user-centric designs. Stakeholder participation at various stages should be anticipated.[137]
Societal and environment well-being:	The development, deployment and use of AI systems should be sustainable and environmentally friendly in light of a possibly adverse impact on resources and energy consumption. The societal impact, e.g., on people's well-being, democracy, or society overall, must be observed.[138]
Accountability:	AI systems should be auditable in terms of the algorithm, data and design process. It must be guaranteed to report on actions and decisions and to reply to the results thereof. Potential trade-offs and tensions (that cannot be avoided) should be tackled in a methodological way using the state of the art. Mechanisms to facilitate redress in terms of unfair effects must be implemented.[139]

It is important to note that these conditions should not be considered as an exhaustive checklist. The HLEG clarifies that tensions between various ethical principles and requirements can occur, and thus, stakeholders need to be thoughtful about this. They are required to "[c]ontinuously identify, evaluate, document and communicate these trade-offs and their solutions".[140] It is also necessary to communicate openly both capabilities and limitations of the AI system at stake.[141] The HLEG published an Assessment List for Trustworthy AI (ALTAI)[142] for self-assessment with the intention to help evaluate if an AI-tool complies with the abovementioned requirements for trustworthy AI.

Additionally, also other organisations have drafted guidelines for the use and development of responsible AI. One of these are the ethics guidelines created by the World Health Organisation (WHO), which put forward six ethical principles that are specifically adapted to the use of AI in the healthcare setting, using the widely accepted ethical principles by Beauchamp and Childress as a foundation.[143]

Following ethics principles is an essential foundation for SECURED partners when developing ethical AI-tools. The Ethics guidelines on Trustworthy AI can provide helpful assistance in making AI more "trustworthy". However, SECURED partners must take into account that it is not enough to consider the identified principles as an exhaustive list that enables just to "check the box". Rather, possibly arising tensions need to be acknowledged, evaluated and addressed.

[136] Ibid., p. 17.
[137] Ibid., p. 18-19.
[138] Ibid., p. 19.
[139] Ibid., p. 19-20.
[140] Ibid., p. 3.
[141] Ibid., p. 2-3.
[142] High-Level Expert Group on Artificial Intelligence, "Assessment List for Trustworthy AI (ALTAI) for self assessment", 17 July 2022, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.
[143] See: WHO, "Ethics and governance of artificial intelligence for health", 28 June 2021, <https://www.who.int/publications/i/item/9789240029200>; see also: SECURED deliverable D1.2 GDPR and Ethics Project Guidelines.

4.3 Proposal for an AI Act

In 2021, the European Commission published a proposal for a Regulation on Artificial Intelligence, also known as the Artificial Intelligence Act or AI Act[144]. Artificial Intelligence (AI) is a rapidly evolving technology bringing about a wide array of societal benefits for patients and the healthcare system. The proposal is built upon the values of the European Union and its fundamental rights whilst seeking to foster the development of AI-based solutions in the Union market.[145] The goal of this proposal is to provide a horizontal regulatory approach to AI by providing the minimum requirements that are necessary to tackle risks and issues in relation to AI-driven technologies. This approach allows for a proportionate risk-based and flexible legal framework that supports the creation of AI without unnecessary restrictions. Furthermore, the principle-based pre-requisites laid down in the proposal secure the citizens' fundamental rights and freedoms.[146]

4.3.1 Current state of affairs

The proposal for an AI Act was first presented by the European Commission in April 2021. It is evolving swiftly and is currently subject to negotiations by the co-legislators, the European Parliament and the Council.[147] The Council adopted its position in December 2022. In May 2023, in parliament, the Internal Market Committee and the Civil Liberties Committee published their amendments to the proposal for an AI Act of the European Commission. The MEPs suggested amendments, for instance, regarding the classification of high-risk areas, including harm to people's health and safety and the list of bands on intrusive and discriminatory uses of AI systems (e.g., in relation to real-time biometric identification systems in publicly accessible spaces, indiscriminate scraping of biometric data from social media or CCTV material, and others).[148] Whilst the final text still needs to be agreed upon, this deliverable also takes note of the latest version of the AI Act at the time of writing, namely the AI Act proposal as amended by the Parliament on 16 May 2023[149].

The proposal for an AI Act is closely related to other legislative initiatives under the EU strategy for data, such as the Data Governance Act[150] or the Open Data Directive[151]. Together, they are mechanisms to promote trust for the pooling and (re-)use of data essential for creating data-driven and high-quality AI systems.[152]

---

[144] Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>.

[145] AI Act, ibid., explanatory memorandum.

[146] AI Act, ibid., explanatory memorandum.

[147] European Parliament, "Legislative Train Schedule – Proposal for a Regulation on a European approach for Artificial Intelligence In "A Europe Fit for the Digital Age" <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence>.

[148] European Parliament, "AI Act: a step closer to the first rules on Artificial Intelligence", press release, 11.05.2023, <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>.

[149] European Parliament, "DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts" (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)), Version 1.1, 16/05/2023,
<https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf>.

[150] 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) PE/85/2021/REV/1, OJ L 152.

[151] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) (Open Data Directive) PE/28/2019/REV/1, OJ L 172.

[152] AI Act, explanatory memorandum, p. 5.

4.3.2 Scope of application and selected aspects

The AI Act sets out harmonized rules for the *market placement, putting into service and use of AI* in the European Union.[153] It lays down specific prohibitions of certain AI practices[154] and conditions for AI systems which create high risks to the health, safety, or fundamental rights of individuals. Whether an AI system is to be classified as high risk depends on the intended purpose of the AI system (Chapter 1). Furthermore, the legislative framework sets out legal requirements for high-risk AI systems with regard to data and data governance (Chapter 2) and a set of obligations (Chapter 3). The act applies to operators of AI systems, encompassing providers, users or deployers[155], authorized representatives, importers and distributors of AI systems.[156]

The creation of a clear definition of AI is critical and has been subject to many debates, resulting in changes thereof throughout the legislative train. The proposal established by the European Commission in April 2021 provided a definition of an AI system seeking to be as technology-neutral as possible in view of future AI developments and techniques.[157] In the latest public text from December 2022, the Council of the European Union adjusted the text, which defines AI systems as a

> "*system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts*"[158].

Thereby, the Council of the European Union narrowed down the definition of AI compared to the original draft by the Commission, now focusing on systems created through machine learning, logic- and knowledge-based approaches.[159] Against that background, the European Parliament adopted a report in May 2023, suggesting a definition that is closer oriented and aligned with the notions of other international organizations, in particular the Organization for Economic Co-operation and Development (OECD).[160] Subsequently, the members of the European Parliament voted in May 2023 for the following definition[161]:

> "*a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments."*[162]

---

[153] Article 1(2) AI Act.
[154] Article 1 AI Act.
[155] The version adopted by the European Parliament suggests to replace the term "user" with "deployer", see Article 3(4) and (8) AI Act as adopted by the European Parliament.
[156] Article 3(8) AI Act.
[157] AI Act, explanatory memorandum, p. 12. The original draft defines an artificial intelligence system in Article 3(1) AI Act as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"
[158] Article 3(1) AI Act as adopted by the Council of the European Union, 25 November 2022 (Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>).
[159] Council of the EU, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", press release, 6 December 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>.
[160] Recital 6 AI Act as adopted by the European Parliament, <https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf>.
[161] See European Parliament, Legislative Train Schedule, Proposal for a Regulation on a European approach for Artificial Intelligence – In "A Europe Fit for the Digital Age", <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence>.
[162] Article 3(1) AI Act as adopted by the European Parliament, p. 137.

It becomes clear that, whilst the development of the AI Act is moving forward quickly, so are the changes related to the definitions and conditions laid down in the text of the AI Act. It is therefore essential to follow the developments regarding the AI Act proposal.

The AI Act proposal provides harmonized provisions regarding the market placement, putting into service and use of AI in the EU. It contains, amongst other things, prohibitions of certain AI practices and rules for AI systems creating high risks to the health, safety, or fundamental rights of individuals. If approved, the AI Act could become relevant for SECURED solutions incorporating AI-driven systems. Following these rules will then become vital to establish trust in AI.

5 Cybersecurity

5.1 Introduction: An EU Cybersecurity Strategy for the Digital Decade

In December 2020, the EU's cybersecurity strategy for the digital decade was presented by the European Commission together with the high representative of the Union for foreign affairs and security policy.[163] The cross-sectoral interdependences created through connected devices and information systems are increasing and so are the needs to secure vulnerabilities to cyberattacks that arise in the digital ecosystem. This holds particularly true for critical infrastructures such as hospitals, online services or devices that encompass sensitive personal data or industrial secrets.[164] Thus, the security of digital tools and network and information systems need to be improved and made "cyber-ready" in order to minimize their vulnerability to malicious cyber-attacks. This also enhances people's trust in digital transformation and the protection of their fundamental rights and freedoms. Cybersecurity awareness and hygiene are consequently pivotal elements for the functioning of the economy and society in the digital age.[165] While the European Commission is working on multiple initiatives, such as a European cybersecurity certification scheme under the EU Cybersecurity Act, particularly the framework on the security of Network and Information Systems (NIS) builds the heart of the single market for cybersecurity.[166] Besides, the GDPR covers specific provisions addressing security regarding the processing of personal data. The following section will illustrate relevant rules concerning (cyber-security) for the SECURED project.

5.2 Data security: the General Data Protection Regulation

The GDPR encompasses various legal obligations that concern security regarding the processing of personal data. A vital aspect thereof is the implementation of appropriate technical and organizational measures, constituting safeguards against accidental loss, unauthorized disclosure, et cetera. The following section will provide further information on three crucial conditions embedded in the GDPR concerning data security, namely the principle of data protection by design and by default according to Article 25 GDPR, the security of processing according to Article 32 GDPR, and the obligation to notify in case of a personal data breach according to Articles 33 and 34 GDPR.

5.2.1 Data protection by design and by default

The first deliverable, D1.2 GDPR and Ethics Project Guidelines, introduced the principle of data protection by design and by default already in order to highlight the importance of the adequate implementation of this rule from the very beginning of this project.

The principle of ***data protection by design***, which is embedded in Article 25 GDPR, necessitates that data controllers employ organisational and technical safeguards into the technological architecture and design for the processing of personal data, facilitating GDPR compliance and subsequently also the effective protection of the individual's rights and freedoms[167] at the early stage (as the data collection) throughout the data processing lifecycle. This means, for instance, that the technological architecture should be designed in a way that only relevant and necessary amounts of

[163] European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.
[164] Joint Communication To The European Parliament And The Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>.
[165] Ibid., p. 2-4.
[166] Ibid., p. 5, 8-9.
[167] EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", Version 2.0. Adopted on 20 October 2020, p. 4 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>.

personal data should be collected and processed, which secures compliance with the data minimisation principle.[168] The implementation of this principle follows a risk-based approach, for which the data controller needs to consider the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks and severity for rights and freedoms of natural persons posed by the processing activity.[169] These measures should be taken into account already at the time when determining the means for the data processing as well as at the time of processing.

The principle of ***data protection by default*** is a term stemming from computer science. It relates to the controller's choices regarding pre-existing and preselected configuration values or processing options employed in the processing systems (e.g., service or device, software applications).[170] This principle is specifically dedicated to ensuring the implementation of the data minimisation principle.[171] Consequently, the data controller should choose default processing settings and options that are restricted to the collection, processing and storing of personal data that is actually necessary with a view to the lawful purpose. It is, therefore, essential to determine the specific and legitimate purpose prior to the collection and processing of the personal data. [172] These considerations also need to be accounted for in the implementation of organisational measures, for instance, by defining data access rights to employed personnel according to their particular role and access needs.[173]

In conclusion, the design and operation of software and hardware components are not the only relevant components. Also, procedural and organisational measures, such as business strategies, internal policies, or training of the personnel, are relevant to enforce the data subject's rights and freedoms effectively. There is no uniformly applicable method that can be applied in order to guarantee compliance with data protection by design and by default conditions. The controller must assess, based on the circumstances at issue, what measures are appropriate to secure the data subject's rights. The measures and safeguards have to be developed in a way that they are robust and that the controller can implement further measures to scale to any increase in risk.[174]

5.2.2 Security of processing

Article 32 GDPR is closely related to the principle of integrity and confidentiality laid down in Article 5(1)(f) GDPR and the principles of data protection by design and by default (Article 25 GDPR). The wording thus coincides (especially) with the latter provision. In particular, Article 32(1) GDPR states that

> "*[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*."

Article 32(2) GDPR requires controllers and processors to pay particular attention to specific types of risks when assessing the level of security of data processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Nonetheless, the conduct of a risk assessment, i.e. the data protection impact assessment (DPIA) according to Article 35 GDPR, is not limited to these risk categories. The DPIA must consequently take all possibly occurring risks into account and has to be carried out prior to any data processing activity.[175]

[168] Ibid.; see also Article 25(2) GDPR.
[169] See Article 25(1) GDPR.
[170] EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", Version 2.0. Adopted on 20 October 2020, p. 11-12 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>.
[171] Ibid., p. 12.
[172] Ibid., p. 11.
[173] Ibid., p. 12.
[174] Ibid., p. 7.
[175] See again SECURED deliverable D1.2 GDPR and Ethics Project Guidelines, p. 18.

The provision specifies some of the measures which are deemed to be appropriate for securing the processing of personal data as per Article 32 GDPR. These measures are, amongst other things:

- Pseudonymisation and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[176]

Besides, adherence to an approved code of conduct according to Article 40 GDPR or an approved certification mechanism according to Article 42 GDPR could be used as an element to demonstrate compliance with the pre-requisites laid down in Article 32(1) GDPR.[177]

5.2.3 Data breach

In deliverable D1.2, we already introduced the relevant provisions, particularly Articles 33 and 34 GDPR, applicable in case of a personal data breach. According to the GDPR "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[178] Given its importance, the table below shall remind on the obligation to notify the supervisory authority and the data subject affected by the breach:[179]

Notification to the supervisory authority, Article 33	Communication to the data subject, Article 34
• When a personal data breach occurs, the controller must notify the personal data breach to the supervisory authority competent in accordance with Article 55 GDPR. • The notification should take place without undue delay and not take longer than 72 hours after having become aware of it. Notifications that were not made within 71 hours shall be accompanied by the reasons for the delay. • Data processors who are on notice of a data break must notify the responsible controller without undue delay after becoming aware of said breach. • The notification shall contain a description at least of the information referred to in Article 33(3)(a-d) GDPR.	• If a data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate said breach to the data subject. • The communication to the data subject shall take place without undue delay. • The communication must inform the data subject in a clear and plain language. • The communication shall contain a description of the nature of the data break and contain at least the information and measures referred to in Article 33(3)(lit. b, c, and d) GDPR.

[176] Article 32(1)(a-d) GDPR.
[177] Article 32(3) GDPR.
[178] Article 4(12) GDPR.
[179] See SECURED deliverable D1.2 GDPR and Ethics Project Guidelines, p. 21.

5.3 Network security: The Network and Information Security Framework

The Network and Information Security (NIS) Directive[180], which came into force in 2018, is the first EU legislation laying down cybersecurity requirements with the aim of achieving a high common level of cybersecurity across the EU. The directive seeks to achieve this objective through particularly two components: first, the implementation of minimum cybersecurity requirements, and second, the establishment of cybersecurity notifications for operators of essential services and digital service providers. Which organizations are identified as operators of essential services may be defined differently across Member States. Organisations falling under the definition will have to transpose adequate security measures and comply with the obligation to notify relevant national authorities in case serious incidents occur. For instance, various EU Member States identify healthcare providers such as hospitals as operators of essential services. Furthermore, cloud service providers are key digital service providers which have to comply with the security and notification prerequisites. Therefore, both types of organisations will have to take account of the NIS Directive and the relevant national laws implementing it. However, the transposition of the first EU cybersecurity legislation has shown to carry with it challenges, causing fragmented implementation across countries.[181] To address the constant rise in cyber-attacks and security threats to network and information systems[182], the European Commission has put forward a proposal amending the currently applicable NIS Directive - i.e., the NIS2 Directive.

The NIS2 Directive[183], updating the existing cybersecurity framework, came into force on 16 January 2023, and EU Member States now have 21 months (until 17 October 2024) to transpose its measures and provisions into domestic law. The directive aims for minimum harmonisation, enabling Member States to adopt or maintain provisions which ensure a higher level of cybersecurity if such provisions are consistent with obligations set out it Union law.[184] The aim of the NIS2 Directive is to:[185]

- lay down obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single point of contact and computer incident response teams (CSIRTs);
- implement cybersecurity risk-management measures and reporting obligations for critical sectors or entities;[186]
- transpose rules and obligations on cybersecurity information sharing;
- set down supervisory and enforcement obligations on Member States.

In comparison to the initial NIS Directive, the NIS2 Directive aims to boost cyber-resilience through:

- Expanding the coverage of sectors and services by eliminating the differentiation between operators of essential services and digital service providers, which is replaced by a size-cap rule;[187]
- Preparedness of Member States by being suitably equipped through, e.g., computer security incident response teams (CSIRTs) and NIS authorities;

[180] 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) OJ L 194.
[181] European Parliament "The NIS2 Directive: A high common level of cybersecurity in the EU", 08.02.2023, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333>.
[182] See Definition of Article 6(1) NIS2 Directive.
[183] 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 (NIS 2 Directive), PE/32/2022/REV/2, OJ L 333, 27.12.2022.
[184] Article 5 NIS2 Directive; Member States are also able to identify entities which where operators of essential services under the NIS Directive as essential entities under the NIS2 Directive (See recital 17 NIS2 Directive).
[185] Article 1(2)(a-d) NIS2 Directive.
[186] See Article 1(2)(b) NIS2 Directive, referring to entities of a type referred to in Annex I and II as well as to critical entities as defined under Directive (EU) 2022/2557.
[187] Recital 6 and 7 NIS2 Directive; .

- Cooperation between Member States through cooperation groups set up for strategic cooperation and information exchange;
- Cultural security awareness in all economically and societal relevant sectors relying on ICT, such as healthcare, digital infrastructure, water, finance, energy and more.[188]

Having regard to the expansion of the scope of application of the NIS2 Directive, the framework now differentiates between ***essential and important entities*** in Article 3 NIS2 Directive, resulting in different levels of supervisory measures and enforcement regimes.[189] The classification into these two categories (i.e., essential and important) reflects the extent to which an entity is critical as well as its size.[190] Amongst other things, an entity of a type referred to in Annex I is essential if it exceeds the threshold for medium-sized enterprises[191].[192] Notably, the NIS2 Directive has added the health sector to its scope of application. The directive now explicitly encompasses healthcare providers[193] such as hospitals in Annex I, but also laboratories, entities conducting research and development activities of medicinal products, and more.[194]

Considering that the health sector constitutes a sector of high criticality according to Annex I, healthcare providers are thus obliged to transpose the security requirements under the NIS2 Directive. Both essential and important entities are required to notify its CSIRT or, where applicable, their competent authority about any incident that has a significant impact on the provision of their services without undue delay.[195] According to Article 23(3) NIS2 Directive, an incident shall be considered significant if "it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned"[196], or if "it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage"[197].

5.4 AI security

The security of AI-driven systems is not explicitly introduced in the EU's Cybersecurity Strategy for the Digital Decade.[198] However, its importance is not to be neglected. The European Union Agency for Cybersecurity (ENISA) has released multiple reports about cybersecurity and algorithms.[199] Considering that one of the SECURED use cases aims to develop medical images, ENISA's report discussing cybersecurity and privacy in AI-related to medical imaging diagnosis may be pointed out.[200] The report was published in June 2023 and focused, as the title suggests, on cybersecurity and privacy challenges in medical imaging diagnosis supported by AI. It identifies multiple aspects

[188] European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)", <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
[189] See Recital 15, Article 32 and 33 NIS Directive.
[190] Recital 15 NIS2 Directive.
[191] According to Article 3(1)(a) NIS2 Directive in conjunction with Article 2(1) of the Annex to Recommendation 2033/361/EC, medium-sized enterprises are entities which employ more than 50 employees and/or exceed 10 million Euro revenue. Small entities employ less than 10 persons and/or do not exceed 10 million Euro revenue. Large entities employ more than 250 employees and/or exceed 50 million Euro revenue.
[192] Article 3(1)(a) NIS2 Directive.
[193] According to Article 3(g) healthcare provider encompasses "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State".
[194] See Annex I, Nr. 5, NIS2 Directive; Annex II of the directive identifies also the manufacturing of medical devices and in vitro diagnostic medical devices as "other critical sector" (see Annex II, Nr. 5, lit. a NIS2 Directive).
[195] See Article 23 NIS2 Directive.
[196] Article 23(3)(a) NIS2 Directive.
[197] Article 23(3)(b) NIS2 Directive.
[198] Joint Communication To The European Parliament And The Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>.
[199] See ENISA, "Cybersecurity Challenges of Artificial Intelligence", <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>; also: ENISA, "Securing Machine Learning Algorithms", <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.
[200] ENISA, "Cybersecurity and privacy in AI - Medical imaging diagnosis", 7 June 2023, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.

relevant in this context, namely the assets, actors and their roles, relevant processes, AI algorithms and the requirements related to cybersecurity and privacy.[201] Both aspects, i.e., cybersecurity and privacy, are important. Yet, the balance between the two is sometimes hard to maintain and can result in certain trade-offs (e.g., in terms of accuracy).[202] Besides, in September 2022, the European Commission put forward a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence, i.e., the AI Liability Directive.[203] By doing so, the Commission seeks to protect persons affected by damages caused by the involvement of AI systems.[204] The draft directive does not put forward concrete cybersecurity requirements. Rather, the proposal considers cybersecurity as a relevant aspect within the draft for certain types of AI systems, which shall be briefly mentioned to raise awareness of the importance of moderating cyber vulnerabilities.[205]

[201] ENISA (2023), ibid., p. 5.
[202] ENISA (2023), ibid., p. 20.
[203] Proposal for a Directive Of The European Parliament And Of The Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496>.
[204] European Commission, "Liability Rules for Artificial Intelligence", <https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en>.
[205] See, for instance, explanatory memorandum at page 3, or Article 4(2)(d) AI Liability Directive referring to the AI Act.

6 Health technology framework

6.1 EU Medical Devices Regulation

Intending to ensure the protection of patient's health and safety, the EU has put forward essential regulations, namely the In Vitro Diagnostic Regulation[206] (IVDR), which applies to in vitro diagnostic medical devices and the Medical Devices Regulation[207] (MDR). These frameworks set out fundamental safety requirements and IT measures for all medical devices. Particularly the MDR may become important as medical devices are, in general terms, any equipment or product intended to diagnose and treat medical conditions. Article 2(1) MDR defines a medical device more specifically as "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings" for one or more of specific medical purposes, such as diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease or other medical purposes enlisted in Article 2(1) MDR.

Software, in particular, can qualify as a medical device if the software is *intended* to be used, alone or in combination, for a purpose as specified in the medical devices regulation.[208] In order to be considered a medical device software, the product should fulfil the definition of software according to the Medical Devices Coordination Group's (MDCG) guidance[209] and the abovementioned definition of medical device as per Article 2(1) MDR. However, also software that does not meet the definition of the medical device can fall under the MDR if it is intended by the manufacturer to accompany the medical device as an accessory. The MDCG provides the following examples falling under such categories, such as software that directly controls a medical device (e.g., radiotherapy treatment software), that offers instant decision-triggering information (e.g., blood glucose meter software), or software that supports healthcare professionals (e.g., ECG software that allows better interpretation). Also, software intended to process, analyse, create or modify the patient's medical information can constitute medical device software. However, software for simple searches or with library functions would not meet the threshold to qualify as such devices.[210]

In light of the SECURED project's objective, it is worthwhile to provide a brief overview of relevant general safety and performance requirements for cybersecurity laid down in Annex I of the MDR:

- The operator must take into account national and EU legislations (e.g., GDPR);
- Physical security must be provided for the use of medical devices through security measures, such as regulated physical access (e.g., the use of badges or segregated and secured access controlled areas);
- Appropriate security controls must be transposed (e.g., using credentials for accessing software and devices, anti-malware software, firewall, only use of genuine non-illegitimate software).[211]

[206] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117, 5.5.2017.
[207] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No. 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC 2017, OJ L 117/1 (MDR).
[208] See Medical Device Coordination Group (MDCG) 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019, p. 6, <https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf>.
[209] Ibid..
[210] Ibid., p. 6.
[211] Medical Device Coordination Group (MDCG) 2019-16 Rev.1 Guidance on Cybersecurity for medical devices, December 2019, July 2020 rev.1, p. 21, <https://ec.europa.eu/docsroom/documents/41863>.

6.2 Regulation on Health Technology Assessment

The Regulation on Health Technology Assessment[212] (HTA) came into force in January 2022 and will be applicable after a delayed transition period of three years as of January 2025.[213] With this regulation, the EU legislator seeks to address the fragmented rules applicable to the assessment of health technologies in order to achieve harmonisation across Member States. The primary goal of the HTA is to offer policy-makers evidence-based information, allowing them to prepare policies that are effective and safe. Against this background, HTA bodies will review health technologies in order to evaluate the positive therapeutic as well as possible side-effects, the impact on citizens' life quality, and administrative means.[214] Health technology assessment is defined as "a multidisciplinary process that summarises information about the medical, social, economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner".[215] It is a scientific evidence-based process which enables competent authorities to evaluate the effectiveness of new or existing health technologies.[216] The HTA's goal is specifically to identify the added value of a health technology in comparison with other new or existing health technologies.[217] Examples of health technologies encompass medicinal products, medical devices or methods of medical prevention. The regulation sets out the conditions and methods for health technologies assessments throughout five chapters regulating: the general provisions (chapter I), the joint work on health technology assessment at the Union level (chapter II), the general rules for joint clinical assessment (chapter III), support framework (chapter IV), and the final provisions (chapter V).

[212] Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (2021) OJ 458/1.
[213] European Commission, Health Technology Assessment: Commission welcomes the adoption of new rules to improve access to innovative technologies, press release, 13.12.2021, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6771>.
[214] European Commission, "Health technology assessment – Overview", <https://health.ec.europa.eu/health-technology-assessment/overview_en>.
[215] Proposal for a Regulation Of The European Parliament And Of The Council on health technology assessment and amending Directive 2011/24/EU. COM/2018/051 final - 2018/018 (COD), p. 1; Article 2(5) Regulation on health technology assessment.
[216] Recital 2 Regulation on health technology assessment.
[217] Ibid.

7 Research ethics and integrity

7.1 Introduction

In the previous deliverable, D1.2, the four fundamental principles developed by Beauchamp and Childress[218] have been established as fundamental, given they often build the foundation for the creation of technology-related guidelines.[219] These can be helpful and provide guidance, especially where the law does not provide an answer.[220] The following section will thus recapitulate the common principles in biomedical ethics. Furthermore, this chapter will introduce two other guiding documents, namely the Declaration of Helsinki and the Declaration of Taipei. Both documents are relevant to the SECURED project since they provide guidance on ethical principles in relation to scientific research.

7.2 Principles in biomedical ethics

The four biomedical ethics principles developed by Beauchamp and Childress[221] are beneficence, non-maleficence, respect for autonomy, and justice:

- ***Beneficence***: The principle of beneficence foresees contributing actively to the well-being and welfare of others and protecting the rights and freedoms of others[222], e.g., by:
    - Protecting human safety and public interest (e.g., quality control and improvement measures).[223]
    - Assigning responsibility and fostering accountability (e.g., through ensuring human supervision when AI is used).[224]
- ***Non-maleficence***: This principle encompasses the obligation not to inflict harm on others and to abstain from creating risks to the detriment of others[225], e.g., by:
    - Implementing regulatory and cybersecurity prerequisites adequately.[226]
    - Securing the authenticity and integrity of data through a trusted access control mechanism.[227]
- ***Respect for autonomy:*** Respecting one's autonomy means respecting an individual's choices and not interfering with a person's decision-making process[228], e.g., by:

[218] TL Beauchamp, JF Childress (2013) Principles of Biomedical Ethics, 7th Edition.
[219] L Floridi et al. (2018) AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds & Machines 28, 689–707 <https://doi.org/10.1007/s11023-018-9482-5>.
[220] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in nontrusteD envirOnMents"', D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) <https://cordis.europa.eu/project/id/644371/results/de>.
[221] Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition.
[222] Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 202-205.
[223] WHO, "Ethics and governance of artificial intelligence for health", 28 June 2021, p. 26 <https://www.who.int/publications/i/item/9789240029200>.
[224] Ibid., p. 28.
[225] TL Beauchamp, JF Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 150-155.
[226] WHO, "Ethics and governance of artificial intelligence for health", p. 26 <https://www.who.int/publications/i/item/9789240029200>.
[227] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) 44 <https://cordis.europa.eu/project/id/644371/results/de>.
[228] TL Beauchamp, JF Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 103-107.

- Being transparent (e.g., it is not sufficient to merely convey general information to the patient, but it must be individualized. Tailored advice should be communicated to the patient through his or her doctor to allow them to understand how and for what reason their data are used throughout the AI or ML timespan.[229])

- ***Justice:*** The principle of justice requires to treat others fairly and provide equal and just opportunities to everyone[230], e.g., by:
  - Processing data in a way the patient would expect it (e.g., the use for the detection of a specific illness would be expectable, whereas possible negative effects could obviously not be considered as such.[231])
  - Protecting inclusiveness and equity (e.g., AI developers should be aware of and consider possible biases in terms of the design, implementation and use to prevent healthcare disparities).[232]

7.3 Declaration of Helsinki

The Declaration of Helsinki[233] is a statement of ethical principles to guide medical research involving human subjects, including research on identifiable human material and data. The declaration was adopted in 1964 by the World Medical Association (WMA), which is an international organization representing physicians, in order to guide physicians in the context of medical research. It is a non-binding guideline but provides essential ethical considerations, which have been in part codified in national legal frameworks. The WMA explicitly encourages others involved in medical research with human participants to consider the principles established.[234] The Declaration of Helsinki is to be read as a whole, and each of its paragraphs should be applied in consideration of all other relevant paragraphs laid down in the declaration.

The declaration establishes that it is the duty of the physician to promote and safeguard the health, well-being and rights of patients, which also includes those involved in medical research.[235] Even though progress in medicine relies on research that ultimately contains studies with human subjects, the primary purpose of such research must be to understand the cause and effects of diseases better and improve medical interventions whilst being safe, effective, accessible and qualitative.[236] To maintain and ensure such a standard, even the best-proven interventions must be continuously reassessed.[237] It is the duty of the physician involved in the research to protect the life, health, dignity, integrity, right to self-determination, privacy and confidentiality of personal information of research subjects.[238] The goal to create and learn new knowledge can never outweigh the interests and rights of the research subject.[239] Also, when the individual has given consent, the responsibility to protect the research subject remains always with the physician and other healthcare professionals.[240] Vulnerable individuals and groups should receive specific protection

[229] ENISA, "Cybersecurity and privacy in AI - Medical imaging diagnosis", 7 June 2023, p. 19, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.
[230] TL Beauchamp, JF Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 249-277.
[231] ENISA, "Cybersecurity and privacy in AI - Medical imaging diagnosis", 7 June 2023, p. 19, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.
[232] WHO, "Ethics and governance of artificial intelligence for health", 28 June 2021, p. 29 <https://www.who.int/publications/i/item/9789240029200>.
[233] WMA, Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>.
[234] See ibid., preamble, section 2.
[235] Ibid., section 4.
[236] Ibid., sections 5-6.
[237] Ibid., section 4.
[238] Ibid., section 9.
[239] Ibid., section 8.
[240] Ibid., section 9.

because they are more likely to be wronged or harmed.[241] Every precaution must be made to secure the privacy of the research participants and the confidentiality of their personal information.[242]

Research participants able to provide voluntary and informed consent must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study.[243] The individual must also be informed about the right to withdraw consent at any time without having to fear disadvantages. Special attention must be given to the specific information needs as well as the methods used to convey the information. Freely given informed consent should be preferably given in writing or otherwise formally documented and witnessed.[244] If the individual is incapable of giving consent, the physician must seek informed consent from the legally authorized representative. These individuals must not be included in a research study that has no likelihood of benefiting them unless it is intended to promote the health of the group represented by the potential subject.[245]

7.4 Declaration of Taipei

The Declaration of Taipei[246] was adopted by the World Medical Association (WMA) after the Declaration of Helsinki in consideration of the evolvement and digitisation of research. The Declaration of Taipei considers the potential that large collections of data and human specimens bring for the development of new research strategies and predictive models bring, whilst considering that databases also carry certain risks. It aims to achieve a balance between the rights of individuals regarding their participation in research, confidentiality and privacy rules while acknowledging the potential that health data brings as a powerful tool to increase knowledge. To this end, the declaration concludes that the risks in the use and potential misuse of health data and biobanks may not come from research. Rather, the risks seem to lie in the commercial, administrative, or political use of such data. As physicians are the primary custodians of confidential medical data, they feel an obligation towards those who entrust them with their information. In contrast to the Declaration of Helsinki, the Declaration of Taipei does not focus only on the medical setting but takes other interests, such as commercial, administrative and political ones, into consideration.[247] It is essentially divided into three parts, i.e., the preamble, the ethical principles, and governance.

The Declaration of Taipei lays down ethical considerations regarding health databases and biobanks which considers health research as a common good that is in the interest of individual patients as well as society overall.[248] It, therefore, believes that research and other health databases and biobank-related activities should contribute to the benefit of society, particularly public health interests.[249] Physicians have specific ethical and legal obligations as stewards ensuring the protection of the patient's information. The rights to autonomy, privacy and confidentiality entitle individuals to remain in control over their personal data and biological material.[250] Confidentiality is a crucial element in sustaining trust and integrity in health databases.[251] The collection, storage and use of data from participants capable of consent must be voluntary and collected for given research in line with the specific, free and

[241] Ibid., section 19.
[242] Ibid., section 24.
[243] Ibid., section 26.
[244] Ibid..
[245] Ibid, section 28.
[246] WMA, Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, 4 June 2020, <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/>.
[247] WMA, Declaration of Taipei – Research on Health Databases, Big Data and Biobanks, <https://www.wma.net/what-we-do/medical-ethics/declaration-of-taipei/>.
[248] Declaration of Taipei, section 5.
[249] Ibid., section 8.
[250] Ibid., section 9.
[251] Ibid., section 10.

informed consent set out in the Declaration of Helsinki.[252] If the data is stored in a health database for multiple and indefinite uses, consent is only valid if the individual has been adequately informed about the aspects considered in section 12 of the declaration, including the purpose of the health database or biobank, the risks and burdens of the data storage and collection, the rules of access to the data, et cetera.

In order to create trustworthy health databases and biobanks, these must be governed by internal and external mechanism, such as to protect the rights of individuals (protection of individuals), to maintain transparency, relevant information on databases should be available to the public (transparency), to consult and engage with individuals and their communities (participation and inclusion), to be accessible and responsive to all stakeholders (accountability).[253] All professionals who contribute to or work with health databases and biobanks must comply with adequate governance arrangements.[254] Such governance arrangements must include all elements enlisted in section 21 of the declaration, such as the purpose of the database, the nature of the health data stored, arrangements for the retention period and the destruction of the data or material, et cetera. Finally, health databases must be operated under the responsibility of appropriately qualified professionals who can assure compliance with the declaration.[255]

[252] Ibid., section 11.
[253] Ibid., section 20.
[254] Ibid., section 22.
[255] Ibid., section 23.

8 Conclusions

The objective of the present deliverable was to present the most relevant pieces of legislation applicable to the SECURED project. The deliverable looked into multiple legislative frameworks, including data protection and privacy, data governance, AI governance, cybersecurity, medical devices and health technologies, and, finally, research ethics and integrity. These chapters have provided a descriptive overview of the relevant legal and ethical frameworks, which will build the basis for the upcoming deliverable D5.4, due M24. The interim report will adopt an evaluative approach and focus on the legal challenges that may arise in the SECURED project. In the final phase of the project, a report on potential policy recommendations (D4.6) will be drafted to address the identified challenges and to support the regulatory transposition of cross-border sharing and the SECURED anonymisation techniques.

9 Main references

Legislation

- Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 (**Convention 108**).
- Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 (**ECHR**).
- 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 OJ L 194 (**NIS Directive**).
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, OJ L 172 (**Open Data Directive**).
- 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, PE/32/2022/REV/2, OJ L 333 (**NIS 2 Directive**).
- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995 (**Data Protection Directive**).
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (**AI Liability Directive**) COM/2022/496 final.
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (**Data Act**) COM/2022/68 final.
- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (**Artificial Intelligence Act**) and amending certain Union legislative acts - General approach, <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.
- Proposal for a Regulation Of The European Parliament And Of The Council on the European Health Data Space COM/2022/197 final (**EHDS**).
- Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, COM/2021/206 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>.
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No. 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC 2017, OJ L 117/1 (**MDR**).
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117 (**IVDR**).
- 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, PE/31/2018/REV/1, OJ L 295.
- 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, PE/53/2018/REV/1, OJ L 303 (**FFNPDR**).
- Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU (2021) OJ 458/1.

- 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**) PE/85/2021/REV/1, OJ L 152.
- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158 27.5.2014, p. 1 (**Clinical Trial Regulation**).

Case Law

- European Court of Justice, Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 19 October 2016.
- European Court of Justice, Case C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, 2 December 2010.
- European Court of Justice, Case T-557/20, SRB v. EDPS, 26 April 2023.
- European Court of Justice, Case C-101/01, Lindqvist, 6 November 2003.

Official Documents

- Article 29 Working Party, "Annex to Letter from the WP29 to the European Commission", DG CONNECT on mHealth, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf>.
- Article 29 Working Party, "Opinion 01/2012 on the data protection reform proposals", Adopted on 23 March 2021, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.
- Article 29 Working Party, „Opinion 05/2014 on Anonymisation Techniques", Adopted on 10 April 2014, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.
- Communication From The Commission To The European Parliament And The Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union COM/2019/250 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN>.
- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European strategy for data COM/2020/66 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.
- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - Fostering a European approach to Artificial Intelligence COM/2021/205 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN>.
- Council of Europe, "Guidelines to respect, protect and fulfil the rights of the child in the digital environment", Recommendation CM/Rec(2018)7 of the Committee of Ministers, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.
- EDPB, "Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))", <https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf>.
- EDPB, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", Version 2.0, Adopted on 18 June 2021, <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>.

- EDPB, Guidelines 05/202 on consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020, <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
- EDPB-EDPS (2022) Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Adopted on 4 May 2022, <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en>.
- ENISA, "Cybersecurity and privacy in AI - Medical imaging diagnosis", 07.06.2023, <https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis>.
- ENISA, "Cybersecurity Challenges of Artificial Intelligence", 15.12.2020, <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>.
- ENISA, "Data Pseudonymisation: Advanced Techniques and Use Cases", 28.01.2021, <https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases>.
- ENISA, "Securing Machine Learning Algorithms", 14.12.2021, <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.
- EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" Version 2.0. Adopted on 20 October 2020, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>.
- European Commission, "Coordinated Plan on Artificial Intelligence", <https://digital-strategy.ec.europa.eu/en/policies/plan-ai#:~:text=The%20key%20aims%20of%20the,AI%20policy%20to%20avoid%20fragmentation.&text=The%20Coordinated%20Plan%20on%20Artificial%20Intelligence%202021%20Review%20is%20the,global%20leadership%20in%20trustworthy%20AI.>.
- European Commission, "The EU's Cybersecurity Strategy for the Digital Decade", <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.
- European Commission, ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence COM(2021) 205 final, ANNEX, <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.
- European Commission, Directorate-General for Research and Innovation, Eechoud, M., Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2777/71619>.
- European Parliament, "DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", Version 1.1, 16/05/2023, <https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf>.
- High-Level Expert Group on Artificial Intelligence (HLEG), "Assessment List for Trustworthy AI (ALTAI) for self assessment", 17 July 2022, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.
- High-Level Expert Group on Artificial Intelligence, "A Definition of AI: Main capabilities and disciplines", 8 April 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
- High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", 8 April 2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
- Joint Communication To The European Parliament And The Council, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018>.

- Medical Device Coordination Group (MDCG) 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019, <https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf>.
- Medical Device Coordination Group (MDCG) 2019-16 Rev.1 Guidance on Cybersecurity for medical devices, December 2019, July 2020 rev.1, <https://ec.europa.eu/docsroom/documents/41863>.
- UNCRC, The United Nations Convention on the Rights of the Child, <https://www.unicef.org.uk/wp-content/uploads/2016/08/unicef-convention-rights-child-uncrc.pdf>.
- WHO, Ethics and governance of artificial intelligence for health, <https://www.who.int/publications/i/item/9789240029200>.
- WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, 6 September 2022, <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>.
- WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks, 4 June 2020, <https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/>.
- WMA, Declaration of Taipei – Research on Health Databases, Big Data and Biobanks, <https://www.wma.net/what-we-do/medical-ethics/declaration-of-taipei/>.

Other Sources

- A Treiber, D Müllmann, T Schneider, I Spiecker genannt Döhmann (2022) Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies. In Proceedings of the 21st Workshop on Privacy in the Electronic Society (WPES'22). Association for Computing Machinery, New York, NY, USA, 69–82, <https://doi.org/10.1145/3559613.3563192>.
- CA Fontanillo López, A Elbi (2022) On synthetic data: a brief introduction for data protection law dummies, European Law Blog, 22.09.2022, <https://europeanlawblog.eu/2022/09/22/on-synthetic-data-a-brief-introduction-for-data-protection-law-dummies/>.
- Council of the EU, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", press release, 6 December 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>.
- D Kelleher, "In Breyer decision today, Europe's highest court rules on definition of personal data", 19 October 2016, IAPP, <https://iapp.org/news/a/in-breyer-decision-today-europes-highest-court-rules-on-definition-of-personal-data/>.
- D Spajić (2023) Anonymous vs. pseudonymous data: the CJEU reaffirms the relative approach to the concept of personal data, CiTiP Blog, 26 April 2023, <https://www.law.kuleuven.be/citip/blog/anonymous-vs-pseudonymous-data-the-cjeu-reaffirms-the-relative-approach-to-the-concept-of-personal-data/>.
- D Spajic, T Lalova-Spinks, "The broadening of the right to data portability for IoT products: Who does the Act actually empower?", p. 27-31, in: C Ducuing, T Margoni, L Schirru (eds.), "CiTiP Working Paper Series – White Paper on the Data Act Proposal", 26 October 2022, <https://www.law.kuleuven.be/citip/en/Publications/citip-whitepaperdataact.pdf>.
- E Kosta, "Article 8 Conditions applicable to child's consent in relation to information society services", in: C Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic), <https://doi.org/10.1093/oso/9780198826491.003.0037>.

- EDPS, “Federated Learning”, <https://edps.europa.eu/press-publications/publications/techsonar/federated-learning_en>.
- EDPS, “Synthetic data”, <https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en>.
- EPDS, “10 Misunderstandings related to anonymization”, <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>.
- European Commission, “Data Act”, <https://digital-strategy.ec.europa.eu/en/policies/data-act>.
- European Commission, “Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)”, <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>.
- European Commission, “European Health Data Space”, <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en>.
- European Commission, “European Health Union: A European Health Data Space for people and science”, press release, 3 May 2022, <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711>.
- European Commission, “Free flow of non-personal data”, <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>.
- European Commission, “Health technology assessment – Overview”, <https://health.ec.europa.eu/health-technology-assessment/overview_en>.
- European Commission, “Liability Rules for Artificial Intelligence”, <https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en>.
- European Commission, Health Technology Assessment: Commission welcomes the adoption of new rules to improve access to innovative technologies, press release, 13.12.2021, <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6771>.
- European Parliament “The NIS2 Directive: A high common level of cybersecurity in the EU”, 08.02.2023, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333>.
- European Parliament, “AI Act: a step closer to the first rules on Artificial Intelligence”, Press release, 11.05.2023, <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>.
- European Parliament, Legislative Train Schedule, Proposal for a Regulation on a European approach for Artificial Intelligence – In “A Europe Fit for the Digital Age”, <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence>.
- G Verhenneman, A Vedder, ‘WITDOM "empoWering prIvacy and securiTy in non- trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles’ (30 June 2015) <https://cordis.europa.eu/project/id/644371/results/de>.
- K Koerner, “Multiparty computation as supplementary measure and potential data anonymization tool”, 27.10.2021, <https://iapp.org/news/a/multiparty-computation-as-supplementary-measure-and-potential-data-anonymization-tool/>,
- L Floridi et al. (2018) AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds & Machines 28, 689–707 <https://doi.org/10.1007/s11023-018-9482-5>.
- L Helminger, C Rechberger (2022) Multi-Party Computation in the GDPR. In: Schiffner, S., Ziegler, S., Quesada Rodriguez, A. (eds) Privacy Symposium 2022. Springer, Cham. <https://doi.org/10.1007/978-3-031-09901-4_2>.
- Li Q et al. (2021) A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection. DOI: arXiv:1907.09693v7.
- M Finck , F Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, Volume 10, Issue 1, February 2020, <https://doi.org/10.1093/idpl/ipz026>.

- T Stadler, B Oprisanu, C Troncoso, ”Synthetic Data – Anonymisation Groundhog Day”, 31st USENIX Symposium, <https://www.usenix.org/conference/usenixsecurity22/presentation/stadler>.
- TL Beauchamp, JF Childress (2013) Principles of Biomedical Ethics, 7th Edition, Oxford University Press.