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

D1.2 — *GDPR and Ethics Project Guidelines*

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	WP 1 - Project Management, Dissemination and Exploitation
Work package Leader	UvA
Deliverable No.	D1.2
Deliverable Title	GDPR and Ethics Project Guidelines
Lead Beneficiary	KUL
Type of Deliverable	Report
Dissemination Level	Public
Due Date	30/06/2023

Document Information	
Delivery Date	27/06/2023
No. pages	25
Version | Status	2.0 | Final
Deliverable Leader	KUL
Internal Reviewer #1	Kelly Mastoraki (CEF)
Internal Reviewer #2	Gergely Acs (BME)

Quality Control	
Approved by Internal Reviewer #1	30/05/2023
Approved by Internal Reviewer #2	03/06/2023
Approved by Work package Leader	26/06/2023
Approved by Quality Manager	26/06/2023
Approved by Project Coordinator	26/06/2023

List of Authors

Name(s)	Partner
Lead Author: Daniela Spajić	KUL
Contributors: Maja Nišević (supervisor), Anton Vedder (PI)	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
05/05/2023	0.1	Daniela Spajić (KUL)	Created the document and the initial version of its content
08/05/2023	0.2	Maja Nišević, Anton Vedder (KUL)	Internal review
24/05/2023	0.3	Daniela Spajić (KUL)	Adapted to project template
26/05/2023	0.4	Maja Nišević (KUL)	Internal review
30/05/2023 03/06/2023		Kelly Mastoraki (CEF), Gergely Acs (BME)	Review by CEF and BME
12/06/2023	1.0	Daniela Spajić (KUL)	First completed version of the deliverable
26/06/2023		Francesco Regazzoni (UvA), Paolo Palmieri (UCC)	Review by Project Coordinator and Quality Manager
27/06/2023	2.0	Daniela Spajić (KUL)	Final version of the deliverable

Table of Contents

Acronyms and Abbreviations

DoA Description of Actions. 8

DPIA Data Protection Impact Assessment. 18

EDPB European Data Protection Board. 13, 20

EU European Union. 8-12

GA Grant Agreement. 8

GDPR General Data Protection Regulation. 8, 10

TEU Treaty on European Union. 14

WP29 Article 29 Working Party. 13, 18

1 Executive Summary

This deliverable, D1.2 GDPR and Ethics Project Guidelines, will serve Consortium partners as a guiding document on the fundamental legal and ethical principles pertinent to the SECURED project.

First, it outlines relevant norms and obligations established under the General Data Protection Regulation (GDPR) as the main data protection framework in the EU. In particular, this deliverable presents the scope of application of the GDPR (Section 3) including:

- The relevant definitions on data processing, controller-ship/processor-ship, and personal data
- The GDPR principles
- The legal grounds building the basis for the processing of personal data
- The rights of the data subject
- The data protection impact assessment
- The principles of data protection by design and by default
- The obligation to notify in case of a personal data breach

Furthermore, this deliverable delivers an overview of the elementary principles in medical ethics (Section 4). As a first step, this section will introduce the relationship between law and ethics in order to provide Consortium partners with a basic understanding of the similarities and differences between the two of them. Afterwards, the section will outline the four main biomedical principles developed by Beauchamp and Childress, as these are widely accepted in philosophy and ethics.

1.1 Related Documents

- Grant Agreement (GA) Project 101095717 - SECURED; Description of Action (DoA) Annex 1

2 Introduction

This document provides some basic, yet essential information about the scope and definitions of the General Data Protection Regulation as the primary data protection legislation at the EU level. Furthermore, it offers an overview of the fundamental principles in medical ethics. The document is an informal information document for SECURED partners, seeking to help understand the issues discussed in the deliverables that will follow later in this project.

2.1 Structure of the Document

The main part of this document is divided into two segments, i.e., the legal and ethical part. The following section (Section 3) summarizes relevant norms established under the General Data Protection Regulation, including selected definitions, principles, and obligations. Afterwards, the ethics section (Section 4) introduces the fundamental ethical principles established in biomedical ethics. The last section (Section 5) provides the final conclusion.

3 General Data Protection Regulation

3.1 Scope of application

The General Data Protection Regulation[1] (hereinafter referred to as "GDPR") lays down the rules regarding the protection of natural persons with regard to the processing of their personal data and rules relating to the free movement of personal data.[2] To this end, the regulation protects the fundamental rights and freedoms of individuals with regard to their right to the protection of personal data[3], and is applicable to any processing of personal data, regardless of whether it is wholly or partly conducted by automated means[4]. This technology-neutral approach as foreseen by the EU legislator seeks to make the data protection legislation fit for the digital age. Partners should thus remember, whenever personal data are collected or processed, to secure the privacy of the individual's personal data and their personal sphere.

3.2 Definitions

The GDPR encompasses various key terms and definitions laid down in Article 4 of the regulation. These terms and definitions are essential, as they determine the conditions under which the GDPR applies. The following sections will illustrate the most important notions and provide further explanations about these.

3.2.1 Data processing

Data processing in general

The GDPR applies to *any* processing of personal data, regardless of the purpose for which it is processed. Article 4(2) GDPR defines the term "processing" as follows:

> "'*processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"

Data processing consequently covers any operation performed on personal data, whilst not being limited to the collection, alteration, or the other actions as enlisted above.

Data processing cross-border

Where data processing takes place across EU countries, the GDPR provides a complementary definition which it refers to as "cross-border processing". To identify whether the processing activity at issue constitutes cross-border processing, two elements need to be generally considered: Whether cross-border processing takes place will depend on where the data processing takes place (i.e., if it is carried out in one or more EU countries) and its effective outreach (i.e., if it is (likely) to affect data subjects in multiple EU countries). More specifically, the GDPR considers two types of scenarios as cross-border processing, which means according to Article 4(23) GDPR either:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.
[2] Article 1(1) GDPR.
[3] Article 1(2) GDPR.
[4] Article 2(1) GDPR.

The processing of personal data which takes place **in the context of the activities of establishments in more than one Member State** of a controller or processor in the Union where the controller or processor is established in more than one Member State;[5]	**or**	The processing of personal data which takes place **in the context of the activities of a single establishment** of a controller or processor in the Union **but which substantially affects or is likely to substantially affect data subjects in more than one Member State**.[6]

Whilst the GDPR determines the rules regarding the processing of personal data for all EU Member States, national laws may further specify the rules of the GDPR. Besides, in the event of cross-border processing, national supervisory authorities are obliged to cooperate with the aim to ensure the consistent application of the regulation. To this end, the GDPR has introduced the so-called "one-stop-shop", which is a mechanism ensuring the cooperation between the lead national data protection authority of the data controller and the other supervisory authority as the contact point for the data subject concerned.[7]

3.2.2 Data controller, data processor, joint controller

The GDPR differs between three types of processing actors, namely data controllers, joint controllers and data processors. These roles are mutually exclusive, meaning that a stakeholder can be either a data controller or a data processor. Which role one inherits will depend on the particular circumstances of the case. The following table will provide a general overview as to how these roles differ from one another. Thereinafter, further explanation regarding their respective roles will be provided.

	Overview
Data controller	The data controller determines the purpose(s) and means of the processing, meaning the *why* and *how* data are processed.
Joint controller	Joint controllers (two or more) determine the purpose(s) and means of the data processing jointly. Whenever there are joint controllers, there must be a binding agreement which determines the joint controllers' respective roles.
Data processor	The data processor processed the data *on behalf of* the data controller, following their instructions. Whenever a data controller shares personal data with the data processor, there must be a binding agreement which regulates what the data processor does with the shared data.

Data controller

As per Article 4(7) GDPR, *data controller* is any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of persona data". They are

[5] Article 4(23)(a) GDPR.
[6] Article 4(23)(b) GDPR.
[7] See Article 60, Recital 127 GDPR.

responsible for the processing activities taking place and, hence, must also be able to demonstrate that the data processing is conducted in accordance with the GDPR.[8] This encompasses furthermore the responsibility to ensure the implementation of appropriate technical and organizational measures whilst taking into account the nature, scope, context, and purpose of the data processing activity as well as the risks of varying likelihood and severity for the rights and freedoms of the data subject.[9] These technical and organizational measures have to be reviewed and updated if necessary when personal data is being processed.[10]

Joint controller

Joint controllers can be recognized based on their involvement in the decision-making regarding the processing operation. Specifically, the regulation foresees that where multiple controllers (i.e., two or more) determine the purposes and means of the processing jointly, they should be regarded as joint controllers.[11] Joint controllers must determine their respective responsibilities for compliance with the obligation in respect of the GDPR in a transparent manner. Transparency shall be created by means of an arrangement between the joint controllers unless, and in so far as, the responsibilities of each controller are determined by EU or national law.[12] This is particularly, but not exclusively, important with regard to the exercising of the data subject's rights and the providing of adequate information to the data subjects according to Articles 13 and 14 GDPR. Such an arrangement must subsequently duly reflect the respective roles and relationships of the controllers vis-à-vis the data subjects.[13]

Data processor

Finally, data controllers have to be distinguished from data processors. A *data processor* differs from a data controller in that a processor, including a natural or legal person, public authority, agency or other body, processes personal data *on behalf of* the controller.[14] A data processor is thus subject to the instructions of the data controller, as the latter is also responsible for the compliance of the processor. Consequently, a data controller can only use processors which provide sufficient guarantees to implement appropriate technical and organizational measures in a manner that the processing operation complies with the rules of the GDPR and that ensures the protection of the data subject's rights.[15] A processor can thus generally not engage another processor for the data processing operation, unless prior authorization was provided by the data controller.[16] The processing by a processor shall be governed by a contract or other legal act under national or EU law, binding the data processor with regard to the data controller. The contract or other legal act shall lay down the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller.[17] Article 28(3) GDPR specifies the requirements regarding the information that the contract or other legal act must stipulate (e.g., that the processor processes the data only on documented instructions from the controller, that he or

[8] Article 24(1) GDPR.
[9] Article 24(1) GDPR.
[10] Article 24(1) GDPR; Where proportionate in relation to the data processing activities, the measures shall include the implementation of appropriate data protection policies by the data controller (see Article 24(2) GDPR).
[11] Article 26(1) GDPR.
[12] See Article 26(1) GDPR.
[13] Article 26(2) GDPR; In any case, data subjects may exercise their data subject's rights against each of the controllers (see Article 26(3) GDPR).
[14] See Article 4(8) GDPR.
[15] See Article 28(1) GDPR.
[16] See Article 28(2) GDPR, which states that said authorisation must be a prior specific or general written authorisation of the data controller. Specifically in the case of a general written authorisation, the processor must inform the controller about any intended chances concerning the adding or replacing of other data processors. This approach allows the data controller to object to the addition or replacement of another processor.
[17] See Article 28(3) GDPR.

she ensures that the authorized persons are committed to confidentiality and makes available all necessary Information available to demonstrate compliance to the controller, et cetera)[18].

3.2.3 Personal data and special categories of personal data

Personal Data

The GDPR protects the processing of *personal data,* which is defined as "any information relating to an identified or identifiable natural person", i.e. the 'data subject'.[19] An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier. A couple of possible identifiers are, for instance:

- Name,
- Identification number,
- Location data,
- An online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [20]

The Article 29 Working Party (WP29), which is the predecessor of the European Data Protection Board (EDPB), emphasized that the notion of personal data was willfully formulated in a *broad manner* in order to grant sufficient protection to the data subject in relation to the processing of the data relating to them.[21] However, to not "overstretch" the notion of personal data[22], the WP29 provided guidelines[23] on the definition of personal data and defined four essential elements which are embedded in the legal definition of Article 4(1) GDPR provided earlier:

Four essential elements of personal data		
1	*Any information*	The term reflects the intention of the legislator for a wide interpretation regarding the notion of personal data. It covers objective information (e.g., the identification of substances in blood samples) and subjective information (e.g., assessments and opinions), regardless of whether it is true or proven.[24]
2	*Relating to*	The term shows the need for a relation or link between the information and the individual. For instance, the medical information contained in the patient's medical record is obviously related to the person's circumstances as a patient. However, more generally, an information relates to an individual if it is *about* the individual, regardless of any purpose.[25]
3	*Identified or identifiable*	A person is viewed as "identified" when he or she is "distinguished" as an individual from other group members through identifiers. Additionally, a person is considered "identifiable" when someone may

[18] See Article 28(3)(a-h) GDPR.
[19] Article 4(1) GDPR.
[20] See Article 4(1) GDPR.
[21] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data', Adopted on 20th June, WP 136, p. 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
[22] Ibid., p. 5.
[23] Ibid.
[24] Ibid., p. 6-9.
[25] Ibid., p. 9-10.

		not have been identified yet, but it is *possible* to do so. This may be the case directly, e.g., through one's name, or indirectly through ID numbers or telephone numbers. However, whether a person is identifiable will also depend on the case-specific circumstances. To determine whether a person is identifiable, *all the means likely reasonably to be used by the controller or any other person* to identify the individual at issue should be taken into account.[26] To ascertain whether means are reasonably likely to be used to identify the individual, all objective factors should be taken into account (e.g., the costs and the amount of time required for identification, the available technology at the time of processing, technological developments).[27]
4	*Natural person*	Subject to protection of the personal data processing are all *living* natural persons[28] residing within the European Union.[29] Hence, the data of deceased persons is not protected.[30] The protection of personal data must be secured by the data controller and data processor when processing personal data about an individual.

Special categories of personal data

Some personal data are more sensitive in nature and, thus, enjoy higher protection under the GDPR. The GDPR refers to these "sensitive" personal data as special categories of personal data. Special categories of personal data are data revealing

- one's ethnic origin,
- political opinion, religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data for the purpose of uniquely identifying a person,
- data concerning health, sex life, and sexual orientation.

[26] Ibid., p. 12-21.
[27] Recital 26 GDPR.
[28] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data', Adopted on 20th June, WP 136, p. 21-24 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>; As per recital 27 GDPR, the regulation does not apply to personal data of deceased persons, unless Member States have implemented them.
[29] Article 2(2) GDPR foresees also some exceptions to the application of the GDPR, namely if the processing of personal data is conducted "in the course of an activity which falls outside the scope of Union law"(lit. a), "by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU" (lit. b), "by a natural person in the course of a purely personal or household activity" (lit. c), or by competent authorities for the purposes of the prevention of criminal offences and other reasons listed in lit. d.
[30] The GDPR may still apply if the personal data of the deceased person is related to another data subject. This could be in particular the case where genetic data, having the ability to reveal information about the individual and their family members or relatives, is processed (see also: Taner Kuru, Iñigo de Miguel Beriain (2022) Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR", Computer Law & Security Review 47, <https://doi.org/10.1016/j.clsr.2022.105752>).

For the SECURED project, the categories of data concerning health and genetic data will be of particular importance and for which the legal definition is provided in the table hereinunder.

Definitions	
Data concerning health	means 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.[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 the provision of health care services, which reveal information about his or her health status.[32]

3.2.4 Personal data and non-personal data

In order to protect patients and citizens adequately in relation to their fundamental rights and freedoms, it is essential to understand what kind of data constitutes personal data and which type of data are concerned (i.e., personal data and special categories of personal data). Whether data is considered to be personal data and special categories of personal data comes – as indicated above – with different legal consequences and obligations. In addition, personal data has to be distinguished from non-personal data. This is an important distinction, because the processing of anonymous data or non-personal data does not fall under the scope of the GDPR, hence, is not protected under data protection legislation.

What is anonymous data?

The GDPR does not define the term "anonymous data", but excludes it from the GDPR's scope through conversion. Specifically, according to recital 26 GDPR, the GDPR should not apply to "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".

What is the difference between anonymous data and pseudonymous data?

Understanding the difference between anonymous data and pseudonymous data is essential as the latter constitutes personal data, triggering the application of the GDPR. This is because pseudonymized data can still be attributed to an individual through additional information so that the GDPR remains applicable (see Article 4(5), recital 26 GDPR). Anonymous data, on the other hand, is absolutely irreversible, so it is impossible to trace back the identity of the individual whose data has been anonymised. As a result, for the processing of pseudonymous data, a legal basis must be applicable for it to be lawful.

Processing of anonymous data vs. anonymization of personal data

Finally, it is necessary to distinguish between the processing of anonymous data, and the anonymization of personal data. While the former encompasses the processing of anonymous or anonymized data, and is thus excluded from the scope of the GDPR, the latter is not. The latter, i.e. the anonymization of personal data, concerns the process of anonymization and thereby includes the processing of personal data which should result in anonymous data. The latter

[31] Article 4(15) GDPR.
[32] Article 4(13) GDPR.

case thus contains personal data and consequently falls under the scope of the GDPR, requiring an applicable legal basis for the anonymization to be lawful.

3.3 GDPR principles

Article 5 GDPR lays down the general principles relating to data processing. These principles apply to all types of personal data processing, regardless of whether personal data and special categories of personal data are processed. Consequently, they need to be respected by the data controller and data processor at all times. In particular Article 5(1 and 2) GDPR set out the following data protection principles:

The data protection principles	
Lawfulness, fairness, and transparency[33]	• Personal data must be processed fairly and lawfully. It is lawful if a legal basis applies to the envisaged data processing. • The legal basis has to be determined prior to the processing activity. • The personal data must be processed in a transparent manner in relation to the data subject, so that the data subject is clearly informed about the why, how, for which and by whom the data is processed.
Purpose limitation[34]	• The personal data must be collected for a specified, explicit and legitimate purpose. • It is not possible to collect and then later decide to use the data for a different purpose. • Personal data cannot be further processed in a manner that is incompatible with those purposes.
Data minimization[35]	• The personal data must be adequate, relevant and limited to what is necessary with a view to the purpose for which it is being processed.
Accuracy[36]	• The personal data collected and processed must be accurate, and, where necessary, kept up to date. • Where data is inaccurate, data subjects can ask for the correction of their personal data.
Storage limitation[37]	• In principle, the personal data must be kept in a form which permits the identification of the data subject for no longer than it is necessary. • If the data are no longer needed, it should be deleted or anonymized. • Data may be stored for a longer period where the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR, which is

[33] Article 5(1)(a) GDPR.
[34] Article 5(1)(b) GDPR.
[35] Article 5(1)(c) GDPR.
[36] Article 5(1)(d) GDPR.
[37] Article 5(1)(e) GDPR.

	subject to the implementation of appropriate technical and organizational safeguards.
Integrity and confidentiality[38]	• The personal data must be processed in a way that ensures the appropriate security of the personal data through technical and organizational measures. • Technical and organizational measures include – but are not limited to – the security against unauthorized or unlawful processing, and accidental loss.
Accountability[39]	• Data controllers and data processors are responsible for compliance with the data protection legislation. • Data controllers must be able to demonstrate compliance with all of the abovementioned data protection principles and rules and maintain relevant documentation thereof.

3.4 Legal grounds

As indicated earlier, the level of protection depends on the type of personal data processed, and is embedded in the processing requirements. This is because special categories of personal data are more sensitive in nature compared to personal data. For the processing of personal data to be lawful, one of the legal bases enshrined in Article 6(1) must be fulfilled. The processing of special categories of personal data is in principle prohibited according to Article 9 (1) GDPR. Derogations from the prohibition should be allowed when provided for in the law and subject to suitable safeguards in order to protect the data subject's fundamental rights.[40] Exceptions to the general prohibition can be found in Article 9(2) GDPR, which sets out the legal grounds for the processing of special categories of personal data. For each and every processing activity, one of the legal grounds embedded in Article 6 and 9 GDPR, respectively, must be applicable.

For the processing of personal data as per Article 6(1), see for instance:	For the processing of special categories of personal data as per Article 9(2), see for instance:
• Consent, Article 7-8 GDPR • Contract • Legal obligation • Vital interest of the data subject • Task carried out in the public interest or in the exercise of official authority • Legitimate interest of the controller	• Explicit consent • Necessary for employment and social security purposes • Vital interest of the data subject where the data subject is physically or legally incapable of giving consent • Legitimate activities by a foundation or other not-for-profit body as per Article 9(2)(lit. d) GDPR • Personal data manifestly made public by the data subject • Necessary for the establishment, exercise or defence of legal claims • Necessary for reasons of substantial public interest • Necessary for purposes of preventive or occupational medicine or for the management of health or social care systems and services

[38] Article 5(1)(f) GDPR.
[39] Article 5(2) GDPR.
[40] Recital 52 GDPR; Also, Article 89 GDPR regulates the safeguards and derogations with regard to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- Necessary for public interest in the area of public health
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

3.5 Rights of the data subject

The data subject, which is the individual whose personal data is being processed, is granted certain rights under the GDPR. These rights are pivotal to maintaining the data subject's autonomy and dignity, coming with certain obligations for data controllers and processors.

The data subject's rights*

1. The right to be informed, Article 13, 14
2. The right to access the personal data about them and to obtain information about the processing, Article 15
3. The right to rectification of their personal data, Article 16
4. The right to erasure of their personal data, also known as the right to be forgotten, Article 17
5. The right to temporarily restrict the processing of their data, Article 18
6. The right to data portability, allowing individuals to have their data transferred from one controller to another, Article 20
7. The right to object to the processing of their data, Article 21
8. The right not to be subject to solely automated decision-making, Article 22

*to be granted if the conditions enshrined in the GDPR are fulfilled.

3.6 Data Protection Impact Assessment

What is a DPIA?

As per Article 35(1) GDPR, the data controller is required to carry out the so-called Data Protection Impact Assessment (DPIA) where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, namely the data subjects.[41] A DPIA is consequently not required for every processing activity resulting in risks for the rights and freedoms of natural persons, but for such that result in a *high risk*. The DPIA encompasses an assessment of the impact of the envisaged processing operation on the protection of personal data, taking into account the nature, scope, context, and purposes of the data processing. Such assessment must be conducted by the data controller *prior* to the processing and the controller shall seek the advice of the data protection officer, if appointed, when carrying out the DPIA.[42] If a set of similar processing operations present similar high risks, the data controller may address those in a single assessment.[43]

When is a DPIA required?

The law requires the carrying out of a DPIA particularly with a view to the use cases enlisted in Article 35(3) GDPR. Additionally, national supervisory authorities may have established lists which comprise possibly additional kind of processing operations which are subject to the requirements of a DPIA.[44] That being said, and with a view to the

[41] Article 35(1) GDPR.
[42] Article 35(1) and (2) GDPR. It is the obligation of the data controller and data processor to ensure that the data protection officer is involved – properly and in a timely manner – in all issues in relation to the protection of personal data (see Article 38 (1) GDPR).
[43] Article 35(1) GDPR.
[44] Article 35(4) GDPR.

SECURED project, the following cases requiring the conduct of a DPIA according to Article 35(3) GDPR are of particular importance:

Where data controllers conduct "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"; (*lit. a*)	**or**	Where the research activities encompass the "processing on a large scale of special categories of personal data referred to in Article 9" GDPR (*lit. b*).

Especially the second example (*lit. b*) includes special categories of personal data, such as data concerning health and genetic data as defined in Article 9 GDPR. A typical example of large-scale processing in the medical context would be the holding of patient records by hospitals.[45] The GDPR provides some guidance in recital 91 to fill out the notion of "large scale" processing, which considers processing as a large-scale operation that aims "to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects". Beyond this, the WP29 suggests furthermore to consider especially the following four factors to determine whether the processing takes place on a large scale:

a. "the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b. the volume of data and/or the range of different data items being processed;
c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity."[46]

The list provided in Article 35 GDPR provision, determining when a DPIA is mandatory, is however, non-exhaustive. Thus, processing operations encompassing high risks may not be covered by the rule directly. The Article 29 Working Party in its guidelines on the Data Protection Impact Assessment[47] considers different criteria which can lead to processing operations being *likely to result in a high risk,* such as including the processing of special categories of personal data as defined in Article 9 GDPR, the processing of data on a large scale, the matching or combining of datasets, or the involvement of data concerning vulnerable data subjects. In particular with regard to the last point, the vulnerability of an individual results from the power imbalance between the data subject and the data controller, which does not allow the individual to consent or object freely to the data processing such as children. Another example provided by the Article 29 Working Party is where the vulnerability results from the special protection afforded to individuals such as mentally ill persons, elderly, patients, and others.[48] To this end, it is important to note that these cases do not need to be met cumulatively in order to result in a high risk processing operation. A data controller might conclude that already one of these criteria is likely to result in a high risk, which would require the conduct of a DPIA.[49] Where it might be unclear whether a DPIA is needed, the Article 29 Working Party suggests to carry out a DPIA nonetheless as it is an adequate tool for data controllers to comply with data protection rules.[50]

[45] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679'. Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017, p. 9 <https://ec.europa.eu/newsroom/article29/items/611236>.
[46] Ibid., p. 10.
[47] Ibid..
[48] Ibid., p. 10.
[49] Ibid., p. 11-12.
[50] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, p. 8 <https://ec.europa.eu/newsroom/article29/items/611236>.

Minimum requirements

The minimum requirements which have to be covered by such Data Protection Impact Assessment are:

- "a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller"[51];
- "an assessment of the necessity and proportionality of the processing operations in relation to the purposes"[52];
- "an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1"[53]; and
- "the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned"[54].

If the results of the conducted DPIA as per Article 35 GDPR show that the envisaged data processing would result in a high risk in the absence of measures taken by the controller to mitigate the identified risks, then the data controller must consult with the national supervisory authority before the data processing takes place.[55]

3.7 Data protection by design and by default

According to Article 25 GDPR, the data controller is required to implement the above listed data protection principles (e.g., transparency, data minimization, et cetera) in the processing of personal data using data protection by design and by default. This allows consequently also for an effective implementation of the data subject's rights and freedoms by design and by default.[56] It demonstrates an important consideration, namely that data protection is an integral part of the technological and design architecture and not merely a tool to be considered after the completion thereof. For an adequate "*by design"* implementation, different elements, which are laid down in Article 25(1) GDPR, need to be taken into account early on when planning and designing processing operations:

Data protection by design, Article 25(1) GDPR	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks and varying likelihood and severity for rights and freedoms of natural persons posed by the processing
	the **controller** shall,
	both at the time of the determination of the means for processing **and** at the time of the processing itself
	implement **appropriate technical and organization measures**, such as pseudonymization, which are designed to **implement data-protection principles**, such as data minimization, in an effective manner and **to integrate the necessary safeguards** into the processing
	in order to meet the requirements of this regulation and protect the rights of data subjects.

[51] Article 35(7)(a) GDPR.
[52] Article 35(7)(b) GDPR.
[53] Article 35(7)(c) GDPR.
[54] Article 35(7)(d) GDPR.
[55] Article 36(1) GDPR.
[56] EPDB, '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>.

Again, the data controller must be able to demonstrate compliance and show that the GDPR principles have been sustained. It is also their responsibility to determine the appropriateness of the measures with regard to the processing activity at stake.[57] The data processor is bound through the accountability principle to help the data controller to maintain such compliance. The term data protection *by default* refers to the controller's choices regarding configuration values or processing options that are implemented in the processing systems (e.g., in devices, software applications, etc.).[58] Furthermore, the "technical and organizational measures" foreseen under the data protection by default principles refer explicitly to the implementation of the data minimization principle.[59]

3.8 Notification of personal data breach

A remark should be made regarding the GDPR provisions concerning the breach of personal data. In the case of a personal data breach, data controllers and processors are confronted with certain obligations towards the supervisory authority and the data subject whose personal data has been affected. A personal data breach is defined by the GDPR as "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."[60]

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.

[57] Ibid..
[58] Ibid., p. 11-12.
[59] Ibid.; see also Article 25(2) GDPR.
[60] Article 4(12) GDPR.

4 Ethical principles

4.1 The relationship between law and ethics

The development of new technological approaches such as artificial intelligence (AI), or multi-computation, or synthetic data generation raises legal but also ethical questions in relation to the protection of an individual's human rights. Ideally, the law will account for possible ethical consequences and will have ethical considerations implemented into its provisions. For instance, we can see that the legislator embedded some ethical factors into the data protection regulation in the form of the principle of fairness, transparency, accountability, or the protection of digital rights and fundamental rights more generally.[61] Also the concept of consent is an important tool to preserve an individual's autonomy and dignity. Besides building a basis for the law, ethical values and principles can provide additional guidance that goes beyond the law. This is essential as, in the advent of rapid technological developments, not all ethical considerations can be predicted at the time when privacy and data protection come into force. Ethical principles can provide guidance through standards but also impose possible constraints on technology developments and the use of data.[62] On this note, it is worth mentioning that simply following ethical principles alone like "ticking boxes" does not automatically lead to the design of ethical-conform tools, as "being ethical" is an ongoing process which requires continuous re-evaluation of the techniques applied. Nevertheless, securing ethical values and principles are a crucial step towards the ethical use of personal data and design of new technologies.

4.2 Principles in biomedical ethics

The principles established by Beauchamp and Childress[63] are classic principles widely recognized in medical ethics. They often build the foundation for the creation of technology-related ethics guidelines, in particular in relation to AI ethics for which they build a good foundation due to their adaptability in terms of the challenges created through artificial intelligence[64]. This report will therefore explore the biomedical principles in this report that builds the ground work for the upcoming research and deliverable due at M9. The order of the illustrated principles does not imply that one deserves moral priority over the other, as they shall receive equal consideration. The four bioethical principles established by Beauchamp and Childress are beneficence, non-maleficence, respect for autonomy and justice:

(1) *Autonomy*: The principle of respect for a person's autonomy highlights the need to respect an individual's choices and to not interfere with the decision-making process regarding their actions. Thereby, it protects the fundamental right to self-determination, fostering individuals to make intentional and voluntary decisions that are not controlled by other, external determinants. Examples for duties which respect a person's autonomy are, for instance, to tell the truth or to respect a person's privacy by securing the confidentiality of their information. Also informed consent constitutes an essential tool for maintaining and respecting a person's autonomy.[65]

(2) *Non-maleficence*: The principle of non-maleficence requires us to not inflict harm on others, also including the duty to abstain from creating *risks* of harm to other people. The notion of harm has to be understood in a broad manner. It covers any behavior that has a negative impact on another individual regardless of

[61] Hielke Hijmans and Charles Raab (2021) Ethical Dimensions of the GDPR, AI Regulation and Beyond. *Direito Público*, *18*(100), <https://doi.org/10.11117/rdp.v18i100.6197>.
[62] Griet Verhenneman, Anton 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>.
[63] Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition.
[64] Luciano 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>.
[65] Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, p. 103-107.

whether that person acted with or without malicious intent. Consequently, adverse effects on one's liberty, dignity, or privacy must be avoided.[66]

(3) *Beneficence*: Complementary to the principle of non-maleficence, which requires to refrain from harming others, we are obligated to actively and positively contribute to other people's well-being and welfare. This positive duty falls under the principle of beneficence and imposes charitable actions. Whilst specific forms of beneficence typically rest on particular professional roles and commitments (e.g., physicians towards their patients), the general principle of beneficence goes beyond particular relationships and is aimed at all people. For instance, it requires to protect the rights and freedoms of others by removing adverse conditions that create impairment to these.[67]

(4) *Justice*: The principle of justice is associated with the notion of fairness, which coincides with the ideal to provide equal and just opportunities for everyone. It is coined by a formula traditionally ascribed to Aristotle: equals should be treated equally and unequals unequally. As a result, the principle of justice is a wide-ranging theory which allows one to take numerous factors into account that could harm and discriminate individuals based, for instance, on their limited capabilities, social or financial status et cetera. These considerations alleviate harm in the form of inequalities in access to the healthcare system and others.[68]

[66] Ibid., p. 150-155.
[67] Ibid., p. 202-205.
[68] Ibid., p. 249-277.

5 Conclusions

This report has laid out the basic, yet important, legal definitions and ethical norms to be considered in the SECURED project. It is an essential document for all consortium members and especially for those who generate or use personal data, in particular health data. The processing of (sensitive) personal data, regardless of the amount that is being processed, bears risks to the fundamental rights and freedoms of individuals due to the uncertainty embedded in rapidly evolving technologies. This deliverable therefore aimed at providing an overview of fundamental concepts of the primary data protection framework and ethical norms protecting data subjects regarding the processing of their personal data.

6 Main references

Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, <https://ec.europa.eu/newsroom/article29/items/611236>.

Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data', Adopted on 20th June, WP 136, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

EPDB, '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>.

Griet Verhenneman, Anton 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>.

Hielke Hijmans and Charles Raab (2021) Ethical Dimensions of the GDPR, AI Regulation and Beyond. Direito Público, 18(100), <https://doi.org/10.11117/rdp.v18i100.6197>.

Luciano 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>.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

Taner Kuru, Iñigo de Miguel Beriain (2022) Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR", Computer Law & Security Review 47, <https://doi.org/10.1016/j.clsr.2022.105752>.

Tom L. Beauchamp, James F. Childress (2013) Principles of Biomedical Ethics, 7th Edition, Oxford University Press, 2013.

Treaty on European Union (Consolidated Version), Treaty of Maastricht , 7 February 1992, Official Journal of the European Communities C 325/5, 24 December 2002.