Project Title	AI-based long-term health risk evaluation for driving behaviour change strategies in children and youth
Project Acronym	SmartCHANGE
Grant Agreement No.	101080965
Project Start Date:	1 May 2023
Project Duration:	48 months
Project Website:	https://www.smart-change.eu/

D2.1 – Benchmark of regulatory and ethical frameworks

Work Package	**2**
Lead Partner	VUB
Contributing Author(s)(Partner)	Renato Sabbadini (VUB), Paul Quinn (VUB), Teatske Altenburg, Fawad Taj (VUMC)
Due Date	2023.10.31
Date	2023.10.25
Version	1.3 DRAFT NOT YET APPROVED BY EUROPEAN COMMISSION

Dissemination Level

X	PU – Public, fully open
	SEN – Sensitive, limited under the conditions of the Grant Agreement
	Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444

Funded by the European Union

	Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444
	Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444

Abstract:	This deliverable summarizes the main findings of T2.1 at the early stage, which primarily focuses on benchmark research of the legal and ethical requirements pertaining to fundamental rights for data protection and privacy. Additionally, it explores the social and ethical acceptance of the technologies involved in the Smart-CHANGE project. It is important to note that the context of this analysis is mainly limited to the project's research activities. This deliverable will serve as a foundational framework for the legal and ethical requirements and will inform the subsequent development phase of the project.
Keyword List:	Legal and ethical issues, SELP, Data protection, Privacy, GDPR, Artificial Intelligence Act, AI Act, Medical Device Regulation, EHDS, European Health Data Space, artificial intelligence
Licensing information:	
Disclaimer:	This project (GA No. 101080965) has received funding from the Horizon Europe R&I programme. The information provided in this document reflects solely the author's views. The European Community, Agency, and Commission are not liable for any use that may be made of the information contained herein. The content is provided without any guarantee or warranty of fitness for a particular purpose. Users utilise the information at their own risk and liability. In the case of proprietary information of the SmartCHANGE Consortium, it shall not be used, duplicated, or communicated to third parties without prior consent.

Versioning history

Version	*Date*	*Author(s)*	*Notes &/or Reason*
1.0	20/09/2023	Renato Sabbadini (VUB)	Table of Contents
1.1	03/10/2023	Renato Sabbadini (VUB)	Sections 0, 1,
1.2	24/10/2023	Renato Sabbadini, Paul Quinn (VUB), Teatske Altenburg, Fawad Taj (VUMC)	Sections 2, 3, and 4
1.3	25/10/2023	Renato Sabbadini, Paul Quinn (VUB), Teatske Altenburg, Fawad Taj (VUMC)	Internal checks and exec summary

Quality Control (peer & quality reviewing)

Version	*Date*	*Name (Organisation)*	*Role & Scope*
1.3	29/10/2023	Mitja Lustrek (JSI)	Reviewer
1.3	28/10/2023	Anton Gradišek (JSI)	Reviewer
1.3	01/11/2023	José Ribeiro (UPORTO)	Reviewer

Funded by the European Union

Contents

Funded by the European Union

List of figures

List of tables

Funded by
the European Union

Executive summary

The overall goal of the SmartCHANGE project is the development of trustworthy, AI-based decision-support tools to help health professionals and citizens reduce long-term risk of non-communicable diseases, through the accurate assessment of the risk of children and youth, including those with difficult-to-detect risks, and the promotion and delivery of optimised risk-lowering strategies. To achieve this goal, risk-prediction models based on existing datasets will be developed in order to create AI-tools that will be tested and perfected in real world healthcare scenarios in four countries on 400 children, whose data will be collected by means of wearable devices. From a regulatory perspective this means that at least three areas of the work at the heart of the project are affected or are likely to be affected, namely: i) personal/health data collection and processing, ii) use of wearable devices and iii) Artificial Intelligence.

This deliverable, therefore, lays out and analyses the main legal and ethical requirements for the SmartCHANGE project, preparing the ground, so to speak, for an actualised and contextualised Societal, Ethical, Legal and Privacy (SELP) compliance framework that will result in deliverable D2.3. The aim is to elucidate which requirements are likely to be applicable to the project. It is not possible to apply them in a contextual manner at this stage given that a number of the contours of the project must still be decided upon in the coming months (this will occur in the other work packages of this project). This document will therefore raise the likely relevance of key legal and ethical frameworks at an early stage in the project, giving them prominence, so that consortium members will know that they are likely to have to take them into account, inter alia in sharing secondary data and in pilot design.

As far as legal requirements are concerned, after a general introduction to the concept and requirements of privacy, this benchmark focuses primarily on two pieces of current legislation at the EU level, i.e. the General Data Protection Regulation (GDPR) and the Medical Devices Regulation (MDR), while trying to assess the impact and relevance of two pieces of EU legislation still in their legislative process, i.e. the Artificial Intelligence Act (AIA) and the European Health Data Space Regulation (EHDS). These legislative initiatives are (or will be) binding in all EU Member States. A review of the relevant pieces of national legislation is also included, in light of the fact that the proof-of-concept study for the SmartCHANGE project will take place in four EU Member States, i.e. Finland, the Netherlands, Portugal and Slovenia. Legal and ethical requirements will be discussed in a more applied manner in the SmartCHANGE impact assessment, due to be carried out in the first half of 2024. As far as

Funded by
the European Union

ethical requirements are concerned, this benchmark lays out the principles related to research involving humans, particularly children, and the development of lawful, ethical and robust AI systems, that respect human autonomy, prevent harm, are fair and explicable. The contextual application of ethical requirements will be further discussed in deliverable D2.3 (Month 9).

List of abbreviations

Abbreviation	*Definition*
AI	Artificial Intelligence
AIA	AI Act
CoE	Council of Europe
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EHDS	European Health Data Space
EHR	Electronic Health Record
EU	European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
IFU	Instructions for use
IP	Internet Protocol (address)
MDR	Medical Devices Regulation
PMS	Post-market surveillance
SELP	Societal, ethical, legal and privacy (related)
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

Funded by
the European Union

WP	Work package

Funded by
the European Union

0 Introduction

0.1 Purpose and scope

This benchmark is the first deliverable (D2.1) of the work package 2 in the SmartCHANGE project. The key aim of this deliverable is to provide initial input for other work packages in terms of legal and ethical requirements. The overall goal of the SmartCHANGE project is the development of trustworthy, AI-based decision-support tools to help health professionals and citizens reduce long-term risk of non-communicable diseases, "by accurately assessing the risk of children and youth, including those with difficult-to-detect risks, and promoting delivery of optimised risk-lowering strategies." (SmartCHANGE DoA: 2). Very succinctly, SmartCHANGE aims at developing risk-prediction models based on existing datasets that can be turned into AI-tools to be tested and perfected in real world healthcare scenarios in four countries on 400 children, whose data will be collected by means of wearable devices. From a regulatory perspective this means that at least three areas of the work at the heart of the project are affected or are likely to be affected:

1. Personal / health data collection and processing
2. Use of wearable devices
3. Artificial Intelligence (AI)

In relation to point 1 above, the main regulatory framework is represented by the General Data Protection Regulation (GDPR) and the relevant national laws. However, the fact that the data collected and processed is health data may subject the work of this project to one more piece of legislation currently discussed but not yet adopted at the time of writing this benchmark, i.e. the European Health Data Space regulation (EHDS). In relation to point 2 above, the main regulatory framework is the Medical Devices Regulation (MDR). As for point 3, artificial intelligence, there is currently no regulatory framework at the EU level, although at the time of writing this benchmark, the European Parliament and the European Council are discussing a compromise for the adoption of the AI Act (AIA), presumably by the end of 2023.

The processing of personal health data, the fact that at the centre of the proof-of-concept study there will be children, and the use of AI, even if or – some would say – especially if the European Parliament and the European Council were not to adopt the AI Act, have also implications for the SmartCHANGE project in terms of ethical requirements and will be treated in a dedicated section of this benchmark.

Funded by the European Union

0.2 Contribution to other deliverables

While this benchmark outlines a general compliance framework for the project, its content, shaped by the specific project requirements, the plan for user engagement, the technical development and the proof-of-concept study, will be the basis for a contextual application of the frameworks analysed here to the tasks outlined in the other work packages, particularly WP4 (Privacy preserving risk-prediction), WP5 (Robust and explainable AI), WP6 (Risk-prediction tool for healthcare professionals and citizens) and WP7 (Proof-of-concept study). The result of the contextual frameworks application will constitute the deliverable D2.3, i.e. the SELP Compliance framework, that will allow each partner to understand their specific legal-ethical requirements vis-à-vis their role in the project. On the basis of deliverable D2.3, the Vrije Universiteit Brussel will prepare the questionnaires for the partners in order to carry out the SELP impact assessment described in the task 2.4 of work package 2.

0.3 Structure of the document

Considering that the analysis of regulatory frameworks relevant to the SmartCHANGE project will touch both current legislation and yet-to-be-adopted legislation, the structure of this document will deal first with the former and then the latter. Preceded by a brief history of the concept of 'privacy', the next section will deal with the General Data Protection Regulation, the Medical Devices Regulation and the national laws related to data protection of the countries where the proof-of-concept study will take place. The following section will present the two legislative proposals related to artificial intelligence, i.e. the AI Act, and to health data, i.e. the EHDS. The final section will deal with the ethical issues raised by this project in relation to the collection and processing of personal health data, especially in the context of research conducted on and with children, and the use of tools based on artificial intelligence.

Funded by
the European Union

1 Current relevant legislation

In this chapter we will examine current EU legislation pertinent to the SmartCHANGE project, starting from a brief historical review of the concept of privacy and the right to privacy, the rise of the concept of protection of personal data, to an illustration of the main tenets of the General Data Protection Regulation (GDPR) and the Medical Devices Regulation (MDR), and conclude with a brief overview of the relevant national legislation for those partners whose tasks involve the collection and processing of data for the proof-of-concept study.

1.1 The right to Privacy and Respect for Private Life

1.1.1 Background information

The distinction between public and private areas of social life has often been claimed to be one of the key tenets of liberal thinking (Cane/Conaghan 2008: 931) and the rise of the notion of privacy as a domain in need of protection by the law is best understood in this context. When Warren and Brandeis (1890) established the right to respect one's private life as a distinct notion, the concept arose in light of those technological advancements of the time, like instant photography and the growth of newspaper businesses, that had an increasingly negative impact on people's private life because of the collection and publication of unauthorised pictures of private individuals or the publication of comments on private and domestic life affairs (Roda/Böröcz 2019: 10). Warren and Brandeis defined therefore the right to privacy as the right to be alone (Warren/Brandeis 1890: 195).

The concept of privacy, however, despite it having been around for over a century, knows to this day no single, widely agreed definition. The very term 'privacy' is highly dependent on various social, cultural, ethical perspectives and/or circumstances. Solove (2008) classified approaches and theories about privacy into the following six categories:

- **The right to be left alone**, i.e. the right "to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law."[1]
- **The limited access to the self**, i.e. the ability to shield oneself from unwanted public observation and discussion by others.

[1] The original quote is by Justice Abe Fortas.

- **Secrecy**, where privacy is infringed upon through public disclosure of information that was previously concealed and where the interest of the individual is to avoid public disclosure of personal matters.[2]
- **Control over personal information**, i.e. the power of individuals, groups or institutions to decide when, how and to what extent information about them is given to others.
- **Personhood**, i.e. the protection of the integrity of personality, specifically "those attributes of an individual which are irreducible in the selfhood" (Solove 2008: 9).
- **Intimacy**, which centres on the development of personal relationships and different degrees of intimacy and self-revelation.[3]

In legal systems the first appearance of the right to privacy as one of the core protected human rights is to be found in the 1948 Universal Declaration of Human Rights (UDHR), as described in the *Handbook on European data protection law* (FRA/CoE 2018: 21-22). Following the adoption of the UDHR at the United Nations, the European countries recognised this right also in the European Convention on Human Rights (ECHR), as seen since it very first version of 1950. According to case law produced by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), the term 'private life' is not to be interpreted restrictively (Kokott/Sobotta 2013: 223), as "whether or not there is or has been an interference with 'private life' is determined by the context and facts of each case" (FRA/CoE 2018: 20).

1.1.2 Universal Declaration of Human Rights

On 10 December 1948, the United Nations General Assembly proclaimed the Universal Declaration of Human Rights (UDHR): a document envisioned as a common standard of achievement for all peoples and all nations. The Universal Declaration sets out the fundamental human rights to be universally protected, including the right to privacy as described in Article 12 (UDHR, Article 12, see below). For the first time in history an international instrument mentions an individual's right to protect his or her private life against interference from others, particularly from the state:

[2] From Whalen v Roe (1977)
[3] See also Roda/Böröcz, 2019:10.

Article 12 of the UDHR:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

1.1.3 European Convention of Human Rights

Founded in 1949 in London with the aim of achieving "a greater unity between its Members for the purpose of safeguarding and realising the ideals and principles which are their common heritage and facilitating their economic and social progress" (Statute CoE, Article 1), the Council of Europe (CoE) is an international organisation of European countries that – as of 2023 – comprises 46 members, 27 of which are also EU Member States. In 1950 the CoE adopted the European Convention on Human Rights (ECHR), which entered into force in 1953. All CoE Member States are signatories to the ECHR and have to respect the rights stipulated in the Convention in the exercise of any activity or power.[4]

Article 8 of the ECHR: Right to respect for private and family life

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

Four interests can be identified in the first paragraph of Article 8 of the Convention: private life, family life, home and correspondence. In some cases, these four interests might overlap. While Article 8 does not refer to explicit procedural requirements, due respect for the interests safeguarded by the article must be ensured. There are, nevertheless, conditions (second paragraph of Article 8) that allow a state to interfere with the enjoyment of the protected right, namely in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Limitations, therefore,

[4] See also: "The Council of Europe in brief": https://www.coe.int/en/web/about-us accessed on 29 September 2023.

are allowed if these: i) have a legal basis ("in accordance with the law" or "prescribed by law"), and ii) are necessary in a democratic society for the protection of the objectives set out above.[5]

In other words, respect for private life is not an absolute right, as the exercise of this right could infringe upon other rights, such as freedom of expression and access to information, while the latter rights might in turn clash with the right to privacy. The European Court of Human Rights (ECtHR) strives therefore to balance the different rights at stake, in an assessment of the test of necessity in a democratic society.[6]

1.1.4 Charter of Fundamental Rights of the European Union

Declared in 2000, the Charter of Fundamental Rights of the European Union came into force in December 2009 with the adoption of the Lisbon Treaty. The Charter brings together the core personal freedoms and rights enjoyed by citizens of the EU into one legally binding document that is consistent with the ECHR, so that where it refers to rights that stem from the Convention, their meaning and scope are the same. At the same time, however, the Charter strengthens the protection of fundamental rights by making those very rights more visible and explicit for citizens, also because the number of rights it covers is larger compared to the ECHR and includes – therefore – rights not included in the Convention, like the right to engage in work, the rights of the elderly, the right of access to a free placement service and the right to health care (Hartley 2014: 156).

Article 7 of the Charter is identical to Article 8 of the ECHR with minor changes:

Article 7 of the Charter: Respect for private and family life

> *Everyone has the right to respect for his or her private and family life, home and communications.*

It is complemented by Article 52 of the Charter, which provides specific limitations of respect to private and family life:

[5] See "Guide on Article 8 of the European Convention on Human Rights": https://www.echr.coe.int/documents/guide_art_8_eng.pdf accessed on 29 September 2023.
[6] Ibid.

Funded by the European Union

Article 52 of the Charter: Scope and interpretation

> *1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*
>
> […]
>
> *3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*

These limitations, similar to those covered by the ECHR, must: 1) be provided by law; 2) respect the essence of the right to privacy; 3) be necessary and proportionate; 4) genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. In other words, the Court of Justice of the European Union must engage in a balancing exercise between the different rights at stake, similar to the one the ECtHR engages in, with the important difference that the provisions of the Charter are addressed to the institutions and bodies of the European Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law, whereas the provisions of the ECHR apply to all national legislations (Tamba 2017: 30-31).

A further important difference between the ECHR and the Charter is that the latter not only guarantees the respect for private and family life, but also establishes a specific right to the protection of personal data:

Article 8 of the Charter: Protection of personal data

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

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

This difference between the ECHR (and the UDHR) and the Charter draws attention, of course, to the five decades that separate the two documents and to how the development of computers and the birth of the internet required a new right, connected to but distinct from the right to privacy, viz. the right to protection of personal data (see section below).

1.2 The Right to the Protection of Personal Data and the GDPR

1.2.1 Background information

The right to the protection of personal data bears a close kinship to the right to privacy, as both derive from the need to maintain, in a functional society, a separation between public and private aspects of life (Cane/Conaghan 2008: 931). The notion of data protection stems from the notion of privacy. As mentioned in the previous section, the development of computers and the internet and the rise of the information society made legislators and judges aware of the need for specific rules to govern the collection and use of personal data, in a process that led to the emergence of a new concept of privacy, "known in some jurisdictions as 'informational privacy' and in others as the 'right to informational self-determination'." (FRA/CoE 2018: 18). While the first local government to adopt a specific law on data protection was the German state of Hesse (1970), the first country in the world to adopt a similar piece of legislation was Sweden in 1973, opening a path followed by France, Germany, the Netherlands and the United Kingdom in the 1980s (FRA/CoE 2018: 19).

In terms of case law, the Federal Constitutional Court of Germany affirmed in 1983 judgement the right to "informational self-determination" (*Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff) as a right derived from the fundamental right to respect for personality, as protected in the German Constitution (FRA/CoE 2018: 19). Two years before, the Council of Europe adopted a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), while the European Union, apart from laying down the right to protection of personal data both in the Charter of Fundamental Rights (Article 8) and in the Treaty on the Functioning of the European Union (TFEU, Article 16(1)), adopted its first data protection legislation in 1995 with the Directive 95/46/EC, succeeded in 2016 by the General Data Protection Regulation (see below).

As in the case of the right to privacy, the right to protection of personal data is equally a non-absolute right and it can be restricted under certain conditions described in the Charter of Fundamental Rights. As in the case of the right to privacy, the right to protection of personal

data too must be balanced against other rights, e.g. freedom of expression or access to information, or public and private interests, e.g. national security[7] .

As seen in the previous section, the Charter explicitly raises the level of protection for personal data to that of a fundamental right in EU law, with the implication that EU institutions and bodies must guarantee the respect of this right, and Member States must do the same when implementing EU law (Charter, Article 51). Moreover, despite the right to personal data protection being laid down five years after the Directive 95/46/EC, Article 8 of the Charter "must be understood as embodying pre-existing EU data protection law." (FRA/CoE 2018: 28) and as laying the basis for key principles that will be found also in the GDPR, as can be seen in paragraph 2, which will be requoted here for convenience (Charter, Article 8(2)):

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

The protection of natural persons in relation to the processing of personal data is currently regulated by the General Data Protection Regulation (Regulation 2016/679, a.k.a. GDPR) and by Regulation 2018/1725, which concerns the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices, and agencies.

1.2.2 Concepts, principles, rights and obligations under the GDPR

In consideration of the complexity of the GDPR, the following sections will deal with the concepts, principles, rights and obligations most relevant to the SmartCHANGE project. For the sake of clarity, in most cases, the wording will be identical to the one of the GDPR Articles referred to in various sections.

1.2.2.1 Core definitions

Article 4 of the GDPR contains 25 definitions. The following is the selection of the definitions that are most important for the project partners to be familiar with.

[7] European Data Protection Supervisor. Data Protection: https://edps.europa.eu/data-protection/data-protection_en last accessed 29 September 2023.

Table 1: Core definitions in the GDPR[8]

Concept	Definition
Personal data	Any information relating to an identified or identifiable natural person (Data subject).
Identifiable natural person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g., IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing	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 subject	Any natural person whose personal data is being processed.
Data controller	A natural or legal person who, alone or jointly, determines the purposes and means of processing.
Data processor	A natural or legal person who processes personal data on behalf of the controller.
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Sensitive data	Personal data which are, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms. It may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Data concerning health	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.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural

[8] Based on Yao/Quinn 2023.

	person, such as facial images or dactyloscopic data (fingerprint identification).
Automated individual decision-making	Decision based solely on automated processing, including profiling, which produces legal effects concerning data subject or similarly significantly affects him or her.
Pseudonymisation	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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Consent of the data subject	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.
Personal data breach	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Cross-border processing	a) 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; or b) 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.

As the GDPR applies to only to personal data, it is crucial for partners involved in the SmartCHANGE project to establish from the very beginning, whether or not they will be processing personal data. The important factor to consider is not, however, whether the data originates from natural persons, as presumably all data in health and social sciences does, but rather whether or not the data enables the identification or re-identification of the individual natural persons at the origin of the data. Within the context of scientific research, therefore, particular attention needs to be paid to understanding whether or not the data to be processed is anonymous or pseudonymous, as the former is not personal data, while the latter most definitely is, as shown in the case *Breyer v. Bundesrepublik Deutschland* (CJEU, C-582/14), where the CJEU discusses the indirect identifiability of data subjects in the concrete case of dynamic IP addresses, where only a service provider has the necessary additional data

to identify the person, and concludes that a dynamic IP address is personal data.[9] The definition of pseudonymous data can be derived from the definition of 'pseudonymisation' given in table 1, whereas the definition of anonymous data can be found in recital 26 of the GDPR:

> […] *The principles of data protection should therefore not apply to anonymous information, namely 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.* […]

While the existence of truly anonymous data is open for debate, as the more data entry-points there are for any given subject, the higher the likelihood to identify the data subject given enough resources,[10] a researcher needs also to ponder the inevitable proportionally inverse relationship between data utility and privacy (Li/Li 2009; WP29 2014: 3). The same Recital 26 of the GDPR seen above clarifies when data can be reasonably considered anonymous:

> […] *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****.* […] [our emphasis]

In a research project such as SmartCHANGE, where there is processing of existing datasets and the creation, by means of data collection during the proof-of-concept study, of new data sets, and where there is a balance between utility and privacy of the data to be maintained, the safest approach is to consider all data pseudonymous or to be pseudonymised once collected and before processing, unless one is dealing with an existing dataset, i.e. controlled

[9] Ruling: "1. Article 2(a) of Directive 95/46/EC of the European Parliament and of 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 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person." (p. 11)

[10] See for instance Gadotti *et alii* 2023.

by a third-party, i.e. a non-project partner, but made publicly available, where it can be reasonably argued the re-identification of the data subject is impossible for project partners and other parties.

1.2.2.2 General principles

The two main objectives of the GDPR are regulating the protection of natural persons concerning the processing of personal data and the free movement of personal data within the EU (GDPR, Article 1). These objectives are pursued through seven principles of personal data processing listed in Table 2 below. Compliance with these principles is crucial, particularly where the legal base is consent. As section 1.2.2.3 below will discuss, in a project such as SmartCHANGE, consent is likely to be the only legal base for the processing of personal data collected in the proof-of-concept study, whereas research could be the legal base to be used for pre-existing datasets, depending on national legislation.

Table 2: Principles of data processing in the GDPR[11]

Principle	Explanation
Lawfulness, fairness and transparency	The principle means that personal data shall be processed lawfully, fairly, and in a transparent manner. What is more important, these requirements should be fulfilled in relation to the data subject.
Purpose limitation	The purpose limitation principle means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	The data minimisation principle means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	The accuracy principle means that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Storage limitation	The storage limitation principle means that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and confidentiality	The integrity and confidentiality principle means that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

[11] Based on Yao/Quinn 2023

	processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The accountability principle means that the data controller shall be responsible for and be able to demonstrate compliance with all the previously mentioned principles.

Lawfulness, fairness and transparency (GDPR, Article 5(1)(a))

The requirements of this principle, i.e. lawful, fair and transparent processing, need to be met in relation to the data subject. Lawful processing means that for personal data to be processed one of the legal grounds listed in Article 6 of the GDPR is necessary. The legal grounds potentially applicable to the SmartCHANGE project are: i) prior and informed consent of the data subject or ii) scientific research purposes as set in Article 9(2)(j) of the GDPR. These two legal grounds will be explored further in section 1.2.2.4.

Fair processing relates primarily to the relationship between the controller and the data subject (FRA/CoE 2018: 118). Controllers must notify data subjects and the general public that they will process data in a lawful and transparent manner and must be able to demonstrate compliance with the GDPR. Processing personal data cannot happen in secret and data subjects should be made aware of potential risks (FRA/CoE 2018: 118). Compliance with the wishes of the data subject also falls under the fair principle, especially where consent is the legal basis of the data processing (FRA/CoE 2018: 118).

Transparency relates to the obligation of the controller to keep the data subject(s) informed about how their data are being used “in a concise, transparent, intelligible and easily accessible form, using clear and plain language” (GDPR, Article 12(1)). Transparency also relates to the information given to the data subject before the actual processing begins (GDPR, Articles 13 and 14; FRA/CoE 2018: 120) and to the fact that information should be readily accessible to data subjects during the processing (FRA/CoE 2018: 120; WP29 2017: 23), but also to the information given to data subjects following a request for access to their own data (GDPR, Article 15).

Purpose limitation (GDPR, Article 5(1)(b))

The purpose limitation principle creates: i) an obligation whereby personal data can be collected only for specified, explicit and legitimate purposes and ii) a prohibition for any further processing incompatible with those purposes, knowing that the purpose must be defined before the beginning of any processing (FRA/CoE 2018: 122). In practice this means

that any processing of personal data must be done for specific, well-defined purposes, while any additional specified purpose has to be compatible with the original one(s). This principle "is strongly connected with transparency, predictability, and user control of data processing: if the purpose of the processing is sufficiently specific and clear, individuals know what to expect." (Yao/Quinn 2023), to the benefit of legal certainty and transparency.

When considering the scope and limits of a particular purpose, the following points should be taken into account (GDPR, Recital 50 and Article 6(4)):

a) any link between those purposes and the purpose of the intended further processing;
b) the context in which the personal data have been collected, in particular concerning the reasonable expectations of data subjects based on their relationship with the controller on its further use;
c) the nature of the personal data;
d) the consequence of the intended further processing for data subjects; and
e) the existence of appropriate safeguards in both the original and intended further processing operations.

Both the GDPR (Article 5(1)(b)) and the Modernised Convention 108 (Article 5(4)(b)) state that the "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" is considered compatible with the initial purposes, although safeguards such as anonymization, encryption or pseudonymization of the data and restriction of access to the data must be adopted prior to the further processing (GDPR, Article 6(4); Modernised Convention 108, Article 5(4)(b)).

Data minimisation (GDPR, Article 5(1)(c))

Data minimisation means that personal data has to be adequate, relevant and limited to what is necessary in relation to the purposes of the processing. In other words (FRA/CoE 2018: 125):

- the data processing has to be limited to what is necessary to fulfil a legitimate purpose;
- the processing of personal data should take place only when the purpose of the processing itself cannot be reasonably achieved through other means;
- the processing of the data must not interfere in a disproportionate manner with the rights, interests and freedoms at stake.

Accuracy (GDPR, Article 5(1)(d))

Data accuracy refers to the obligation of ensuring the correctness of the personal data, including, if necessary, its being kept up to date, while ensuring prompt erasure or

rectification in relation to the purposes of the processing. In a project such as SmartCHANGE the accuracy of data collection and processing will need to rely also on the correct functioning and precision of wearable devices used in the proof-of-concept study. The updating of stored data, however, may in certain cases be legally prohibited, due to the fact that the purpose of retaining the data is to document events as instants of history, so to speak. Typically this is the case of medical records of surgeries, which cannot be changed or "updated" even if the original findings in the record turn out to be wrong at a later stage. In these circumstances, additions to the record may be made only when clearly marked as contributions made at a later stage (FRA/CoE 2018: 128).

Storage limitation (GDPR, Article 5(1)(e))

Storage limitation refers to the obligation of keeping personal data in a form that allows the identification of the individual data subjects for no longer than necessary vis-à-vis the processing purposes. In other words, once those purposes have been achieved, the data must be either erased or anonymised. Controllers must therefore set time limits for the storage of personal data that apply until the identification of the subjects is still possible, i.e., once the data has undergone anonymisation, the time limits no longer apply.

Exceptions to the storage limitation principle are allowed for the processing of personal data in relation to archiving purposes, in the public interest, scientific or historical research purposes or statistical purposes (GDPR, Article 89(1)). Nevertheless, appropriate technical and organisational measures must be adopted to safeguard the rights and freedoms of the data subjects. In the Modernised Convention 108 (Article 11(1)) exceptions to the principle of storage limitation are allowed where these are: i) provided by law, ii) respect the essence of fundamental rights and freedoms and iii) are necessary and proportionate for the pursuit of a limited number of legitimate aims (Article 11(1)).

Integrity and confidentiality (GDPR, Article 5(1)(f))

The integrity and confidentiality principle implies that personal data has to be processed in a manner that ensures the appropriate security of personal data, i.e. protecting it against accidental, unauthorised, or unlawful access, use, modification, disclosure, loss, destruction, or damage. Therefore appropriate technical and organisational measures, such as pseudonymisation and encryption need to be implemented, while the effectiveness of these measures needs to be verified on a regular basis. Data controllers and processors need to consider "state of the art, the cost of implementation and the nature, scope, context and purpose of data processing, as well as the risk of varying likelihood and severity for the right

and freedoms of natural persons" (GDPR, Article 32(1)) when implementing such measures. Data controllers are also encouraged to implement data protection by design (GDPR, Article 25).

Accountability (GDPR, Article 5(2))

The accountability principle relates to the responsibility and ability of the controller to prove compliance with all the other principles of the GDPR, by means of:

- records of the processing activities, to be made available to the supervisory authority upon request (GDPR, Article 30);
- designation of Data Protection Officer (DPO), to be involved in all issues related to personal data protection (GDPR, Articles 37-39);
- Data Protection Impact Assessments to be carried out when processing is likely to result in a high risk to the rights and freedoms of natural persons (GDPR, Article 35);
- data protection by design and by default (GDPR, Article 25);
- policies and procedures that allow data subjects to exercise their rights (Roda/Böröcz 2019: 19);
- codes of conduct or certification mechanism (GDPR, Articles 40 and 42).

Accountability also has implications for the processors, such as keeping a record of processing activities, appointing a DPO when one is needed (GDPR, Articles 5(2), 30 and 37), implementing any measure ensuring data security (GDPR, Articles 23(3)(c)), providing assistance to the controller concerning compliance requirements in set in the contracts between them and the controller, e.g. performing a data protection impact assessment or notifying the controller of any personal data breach as soon as they become aware of it (GDPR, Article 28(3)(d)).

1.2.2.3 Sensitive data

So far the term 'personal data' has been used as a designating a uniform category, distinct from other categories that are not personal data, e.g. non personal data (i.e. data not related to persons) or anonymous data (i.e. data that makes it impossible or reasonably unfeasible to re-identify the human subjects that originated the data). Within the domain of personal data, however, the GDPR identifies a special sub-category, a kind of personal data whose processing is prohibited unless certain conditions are present. These data are defined as "particularly sensitive in relation to fundamental rights and freedoms" (GDPR, Recital 51) and worthy of specific protection. Article 9(1) of the GDPR lists the protected characteristics associated with this kind of data:

> *1. Processing of personal data revealing* ***racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data*** *for the purpose of uniquely identifying a natural person, data concerning* ***health*** *or data concerning a natural person's* ***sex life or sexual orientation*** *shall be prohibited.* [our emphasis]

While the characteristics listed above may lead someone to believe that sensitive data is a relatively restricted and easy to identify category, there is a growing literature highlighting how it is not always easy to ascertain the sensitivity of a given set of data, particularly in light of the increase of computational power and of the possibility of combining on the surface non sensitive data points from different datasets to derive conclusions that are sensitive in nature.[12] In a project such as SmartCHANGE, however, the collection and analysis of health data places firmly the data processing under the purview of Article 9 of the GDPR.

1.2.2.4 Legal grounds for the processing of personal data

The most direct consequence of the lawfulness principle (GDPR, Article 6) is the need for a valid legal basis whenever personal data is processed. The GDPR lays down the legal bases for data processing in Article 6, for all personal data, and in Article 9(2), for sensitive data. Table 3 lists succinctly the bases of both articles without going into details and highlighting the bases that are most relevant for the SmartCHANGE project.

Table 3: Legal bases for the processing of data (GDPR, Articles 6 and (9)(2))

Art. 6(1)	Legal base	Legal base	Art. 9(2)
(a)	Consent	Consent	(a)
(b)	Necessary for performance of contract	Employment/social security	(b)
(c)	Compliance with legal obligation	Vital interests of data subject	(c)
(d)	Vital interests of data subjects	Members of non-profit bodies	(d)
(e)	Public interest	Data made public by data subject	(e)
(f)	Legitimate interest	Exercise/defence of legal claims	(f)

[12] See Quinn & Malgieri 2021 for an in-depth review of this topic.

		Substantial public interest	(g)
		Preventative, occupational medicine, etc.	(h)
		Public health	(i)
		Scientific, historical research	(j)

As mentioned in the previous section and as highlighted in yellow in Table 3 above, the two legal bases most relevant for the SmartCHANGE project are:

1. Consent: where the data subject has given explicit consent to the processing of personal data for one or more specified purposes (GDPR, Article 9(2)(a)).

2. Scientific research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with art. 89(1) of the GDPR based on Union or Member State law (GDPR, Article 9(1) and 9(2)(j)).

Legal basis no. 2 above will be important for SmartCHANGE in that it will allow personal data to be processed without consent where obtaining such consent would not be possible or it would pose serious questions for the research in question.

The conditions for lawful consent will be dealt with in the section below, while the research exception to Article 9(1) of the GDPR will be discussed in conjunction with national legislation in section 1.4 below.

1.2.2.5 Consent

In the context of a proof-of-concept study for a project such as SmartCHANGE, it is crucial to prioritize obtaining valid consent from individuals as the primary legal basis for processing their personal data. The GDPR provides that the consent should be (FRA/CoE 2018: 143-149):

- **Freely given.** Consent can be considered freely given "if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent." (WP29 2011: 12). The GDPR clarifies that in order to assess whether consent is freely given or not "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." (GDPR, Article 7(4)).

- **Informed.** Informed consent must rely on "a precise and easily understandable description of the subject matter requiring consent." (Yao/Quinn 2023). Moreover, the person whose consent is need for the purpose of data processing must receive "in a clear and understandable manner, accurate and full information on all relevant issues, such as the nature of the data processed, purposes of the processing, the recipients of possible and the rights of the data subject." (WP29 2007: 9).

- **Specific.** Consent must be specific concerning the processing purpose, which, again, must be described clearly and in unambiguous terms, having in mind the reasonable expectations of an average data subject.

- **Unambiguous.** Consent requires "a statement from the data subject or a clear affirmative act, meaning it must always be given through an active motion or declaration." (Yao/Quinn 2023). In other words, it has to be obvious that the data subject has consented to the processing, with a "clear affirmative action" (GDPR, Article 4(11)), i.e. he or she has taken a deliberate action to consent to the processing. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

1.2.2.6 Rights of data subjects

Table 4: Rights of data subjects under the GDPR[13]

Right	Explanation
Right to be informed	The controller shall take appropriate measures to provide the data subject information about data controller (identity, contact detail, contacts of DPO), the purposes of the processing, the recipients of data and other information. It should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
Right of access	The data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and related information.
Right to rectification	The data subject shall have the right to obtain from the controller without undue or excessive delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have

[13] This table and the following privacy related sessions draw from Yao/Quinn 2023

	incomplete personal data completed, including by means of providing a supplementary statement.
Right to erasure ('right to be forgotten')	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay in certain conditions.
Right to restriction of processing	The data subject shall have the right to obtain from the controller restriction of processing in certain conditions.
Right to data portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on a consent of data subject or performance of the contract and the data processed by automated means.
Right to object	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on public interest or legitimate interest of data controller, including profiling based on those provisions and marketing purposes. The controller shall no longer process the personal data unless some exceptions are applied.
Right to lodge a complaint with a supervisory authority	Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.
Right to an effective judicial remedy against a supervisory authority and to receive compensation	Whenever the data subject considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR, he or she has the right to an effective judicial remedy and the right to receive compensation.

In the digital era the processing of data and its increasing pervasiveness have become more and more difficult for most individuals to understand, which is why the GDPR has conferred data subjects a number of rights for them to have greater control in relation to the processing of their personal information (FRA/CoE 2018: 205). All controllers need to be aware of these rights and facilitate them. The data subject rights are:

Right to be informed (GDPR, Article 12, 13 and 14)

Data controllers shall take appropriate measures to provide the data subject information about the data controller (identity, contact detail, contacts of DPO), the purposes of the processing, the recipients of data and other information. It should be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language (GDPR, Article 12). It must be provided in written form, including electronically where appropriate, and it may even be provided orally at the data subjects' request and if his or her identity is proven beyond doubt. The information shall be provided without excessive delay or expense.

Under the GDPR, data controllers have an obligation to inform data subjects at the time of collecting their personal data about the intended processing. This obligation is proactive and should be fulfilled regardless of whether data subjects explicitly request the information or show interest in it. The information that should be provided to data subjects includes:

a) the controller's identity and contact details, including the DPO's details, if any;
b) the purpose and legal basis for the processing, i.e., a contract or legal obligation;
c) the data controller's legitimate interest, if this provides the basis for processing;
d) the personal data's eventual recipients or categories of recipients;
e) whether the data will be transferred to a third country or international organisation, and whether this is based on an adequacy decision or relies upon appropriate safeguards;
f) the period for which the personal data will be stored, and if establishing that period is not possible, the criteria used to determine the data storage period;
g) the data subjects' rights regarding processing, such as the rights of access, rectification, erasure, and to restrict or object to processing;
h) whether the provision of personal data is required by law or a contract, whether the data subject is obliged to provide his or her personal data, as well as the consequences in case of failure to provide the personal data;
i) the existence of automated decision-making, including profiling;
j) the right to lodge a complaint with a supervisory authority;
k) the existence of the right to withdraw consent.

Under EU law, the transparency principle requires that personal data processing be generally transparent to individuals. Data subjects have the right to know which personal data are collected and how they are processed and be made aware of the risks, safeguards, and their rights regarding processing (GDPR, Recital 39). Data controllers must notify data subjects of the origin of the personal data when the data is not obtained from the data subject directly.

In the case of automated decision-making, including profiling, data subjects must be provided with meaningful information about the logic of the profiling, its significance, and the potential consequences of processing activities (GDPR, Articles 13(2) and 14(2)(f)). Finally, if data controllers intend to process personal data for a purpose other than those originally stated to the data subject, controllers must provide data subjects with information about this new purpose before the new processing: i.e. when data subjects consent for personal data processing, the controller must obtain the subject's renewed consent if they want to process their data for further purposes.

Moreover, in accordance with the fairness principle, the information provided by data controllers must be easily understandable for the data subjects. The language used should be appropriate for the intended audience. The type and level of language used should vary depending on the target groups, e.g. adults or children, the general public or academic experts. One of the most effective methods of providing information is by including suitable information clauses on the controllers' homepage, such as a website privacy policy. However, it is important to consider that a significant portion of the population does not use the Internet, and alternative means of communication should be taken into account (FRA/CoE 2018: 213).

Right of access (GDPR, Article 15)

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, obtain access to the personal data and the following information (GDPR, Article 15(1)):

a) the purpose of the processing;
b) the categories of personal data concerned;
c) the recipients of personal data;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling.

The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form (GDPR, Article 15(3)).

Data controllers must provide data subjects with a copy of the personal data being processed in an intelligible form, making sure that the information is understandable to data subjects. As discussed above, when there is implementation of automated decision-making, the underlying logic of the decisions should be explained, and if the data is not directly collected from the data subject, information about the data source should be provided in response to an access request, where available. It is important to interpret this provision taking into account the principles of fairness, transparency, and accountability.

Right to rectification (GDPR, Article 16)

The data subject shall have the right to obtain from the controller without undue or excessive delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement (GDPR, Article 16).

According to the GDPR, the accuracy of personal data is essential to ensure a high level of data protection of data subjects, therefore inaccurate personal data must be rectified without undue or excessive delay (GDPR, Article 16 and Recital 65). In certain cases, a data subject's request for rectification of their personal data, such as their name and address, may be sufficient. However, when such requests are related to matters of legal relevance, including the data subject's legal identity, the data controller may have the right to request proof of the alleged inaccuracy in addition to the rectification request. It is important to note that this demand for proof should not impose an unreasonable burden on data subjects, preventing them from rectifying their data.

Right to erasure ('right to be forgotten') (GDPR, Article 17)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following applies (GDPR, Article 17(1)):

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based and where there are no legal grounds for processing;
c) the data subject objects to the processing and there is no other legitimate ground for processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services.

Providing data subjects with a right to have their personal data erased is particularly important for effectively applying data protection principles, including the principle of data minimisation (FRA/CoE 2018: 221). In line with the lawfulness of data processing and the principle of accountability, data controllers are responsible for proving that the data processing is legitimate. They must demonstrate that there is a sound legal basis for their data processing at any time. Otherwise, the processing must be stopped (GDPR, Article 5 and 6). The GDPR, however, lists exceptions to the right to be forgotten where data processing activity is necessary for (GDPR, Article 17(3)):

a) exercising the right of freedom of expression and information;
b) compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) reasons of public interest in the area of public health;
d) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
e) the establishment, exercise or defence of legal claims.

When a data controller has made personal data public and is under obligation to the same data, he or she has a responsibility to take 'reasonable' steps to inform other controllers, processing the same data, about the data subject's request for erasure. The actions of the controller should consider the available technologies and the cost of implementation.

Right to restriction of processing (GDPR, Article 18)

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies (GDPR, Article 18(1)):

a) the accuracy of the personal data is contested by the data subject;
b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing when the processing is based on public interest or legitimate interest of the data controller by pending the verification of whether the legitimate grounds of the controller override those of the data subject.

The method that a controller can use to restrict personal data processing includes temporary movement of the selected data to another processing system, making the data unavailable to users or the removal of personal data on a temporary basis (GDPR, Recital 67). Furthermore, the controller must notify the data subject before the restriction on processing is lifted (GDPR, Article 18(3)). The controller must communicate any rectification, erasure of personal data, or any processing restriction to each recipient to whom the controller disclosed the personal data. If the data subject requests information about those recipients, the controller must provide him or her with this information (GDPR, Article 19).

Right to data portability (GDPR, Article 20)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on a consent of data subject or performance of the contract and the data processed by automated means (GDPR, Article 20).

The right to data portability supports user choice, user control and user empowerment, aiming to give data subjects control over their personal data (WP29 2016: 13). The main elements of data portability include:

a) the data subject's right to receive their own personal data processed by the controller in a structured, commonly used, machine-readable and interoperable format;
b) the right to transmit personal data from one data controller to another data controller without hindrance if this is technically feasible;

c) the regime of controllership – when a controller responds to a data portability request, they act on the data subject's instructions, meaning that they are not responsible for the recipient's compliance with data protection law, given that the data subject decides whom the data is ported to;
d) the exercise of the right to data portability is without prejudice to any other right, as with any other rights in the GDPR.

Under the GDPR, data subjects enjoy the right to data portability in situations where the personal data that they have provided to a controller are processed by automated means on the basis of consent or where the personal data processing is necessary for the performance of a contract and is carried out by automated means. This means that personal data processing is based on a legal ground other than consent or a contract (GDPR, Article 20(1) and Recital 68). Data subjects could have their personal data transmitted directly from one controller to another if it is technically feasible (GDPR, Article 20(2)). To realise this, data controllers should develop interoperable formats to enable data portability (GDPR, Article 20(1) and Recital 68). Interoperability could be defined in a road sense as the information system's ability to exchange data and enable information sharing.[14] The GDPR does not impose recommendations on the specific format, and they may differ across sectors (WP29 2016: 13).

Right to object (GDPR, Article 21)

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on public interest or legitimate interest of the data controller, including profiling based on those provisions and marketing purposes. The controller shall no longer process the personal data unless some exceptions are applied (GDPR, Article 21(1)).

The GDPR empowers the data subject to raise objections relating to their particular situation where the legal basis for the processing is the controllers' performance of a task carried out in the public interest or where the processing is based on the controllers' legitimate interests (GDPR, recital 69, Art. 6(1)(e) and (f)). This right aims to strike the correct balance between the data subject's data protection rights and the legitimate rights of others in processing their data (FRA/CoE 2018: 230). The effect of a successful objection is that the controller may no

[14] European Commission, Communication on stronger and smarter information systems for borders and security, COM (2016) 205 final, 2 April 2016.

longer process the data in question. Processing operations performed on the data subject's data prior to the objection will remain legitimate.

Besides, the data subject has the right to object to the use of his or her personal data for direct marketing purposes at any time and free of charge. Data subjects must be informed of this right in a clear manner, separate from any other information (GDPR, Article 21(4)). When personal data is used for information society services,[15] data subjects could exercise their right to object to the processing of their personal data by automated means.

The GDPR balances the requirements of scientific, statistical, or historical research and the rights of data subjects with specific safeguards and derogations in Article 89. Thus, Union or Member State law may provide derogations of the right to object insofar as such right is likely to render impossible or seriously impair the achievement of the research purposes and if such derogations are necessary for the fulfilment of those purposes (GDPR, Article 89).

Right to lodge a complaint with a supervisory authority (GDPR, Article 77)

Every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement, if the data subject considers that the processing of personal data relating to him or her infringes the Regulation (GDPR, Article 77).

Data subjects can benefit from the assistance of a supervisory authority in exercising their rights irrespective of their nationality or residence (Modernised Convention 108, Article 18). A request for assistance may only be rejected in exceptional circumstances, and data subjects should not cover the costs and fees for the assistance (Modernised Convention 108, Articles 16 and 17).

The GDPR requires supervisory authorities to adopt measures to facilitate the submission of complaints, such as creating an electronic complaint submission form (GDPR, Article 57(2)). The data subject can lodge the complaint with the supervisory authority in the Member State of his or her habitual residence, place of work, or place of the alleged infringement, while the supervisory authority has the obligation to inform the person concerned of the outcome of the proceedings dealing with the claim (GDPR, Article 77(1) and (2)).

[15] Information society services are defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, e.g. social media platforms.

Right to an effective judicial remedy against a supervisory authority and to receive compensation (GDPR, Article 78 and 82)

Whenever the data subject considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR, he or she has the right to an effective judicial remedy and the right to receive compensation (Roda/Böröcz 2019: 23).

In addition to the right to complain to the supervisory authority, data subjects have the right to an effective judicial remedy and to bring their case before a court. The right to a legal remedy is well-established in the European legal tradition and is recognised as a fundamental right (Charter, Article 47 and ECHR, Article 13).

1.2.2.7 Obligations of data controllers

In addition to the obligations of controllers corresponding to the rights of data subjects, the GDPR specifies other requirements for data controllers and processors. The demonstration of compliance reflects the accountability principle of data processing and it is important to be aware of the relevant obligations. The obligations of data controllers provided by the GDPR are as follows:

Demonstration of compliance (GDPR, Article 24)

The GDPR establishes the general obligation of data controllers to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. These measures should be implemented while considering the nature, scope, context, and purposes of the processing, as well as the risks to the rights and freedoms of individuals, which can vary in likelihood and severity. It is important to regularly update and review these measures as necessary (GDPR, Article 24(1). Examples of the measures that should be taken include implementing data protection policies, codes of conduct, and certification (GDPR, Article 24(2) and (3)). Moreover, these measures will need to be updated and reviewed where necessary.

Data protection by design and by default (GDPR, Article 25)

The data protection by design obligation requires data controllers both at the time of the determination of the means for processing and at the time of the processing itself to implement appropriate technical and organisational measures, which are designed to comply with data protection principles, such as data minimisation, in an effective manner and to

integrate the necessary safeguards (GDPR, Article 25(1)). The implementation shall consider the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing. An example of the measure is *pseudonymisation*.

The data protection by default obligation reflects data minimization and purpose limitation principles. It requires data controllers to implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed and "That obligation applies to the amount of personal data collected, the extent of their processing, the storage period and accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." (GDPR, Article 25(2).

To demonstrate compliance with the obligations of data protection by design and by default, controllers might apply an approved certification mechanism (GDPR, Article 25(3).

Records of processing activities (GDPR, Article 30)

The obligations require data controllers (and processors, if any) to record in writing (including the electronic form) the information about the data controller and details about data processing, including, *inter alia*, the categories of data subjects and categories of data, the purpose of processing (GDPR, Article 30). While the obligations have a few exceptions, these do not apply when processing sensitive data.

Cooperation with the supervisory authority (GDPR, Article 31)

"The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks." (GDPR, Article 31).

Security of processing (GDPR, Article 32)

The data controller and data processor (if applicable) shall implement the appropriate technical and organisational measures to ensure data processing security (GDPR, Article 32). The examples of the measures to be taken are (GDPR, Article 32(1)):

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring processing security.

The Handbook on European data protection law suggests the following organisational measures to ensure privacy (FRA/CoE 2018: 167):

- Regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations.
- Clear distribution of responsibilities and a clear outline of competencies in matters of data processing, especially regarding decisions to process personal data and to transmit data to third parties or to data subjects.
- Use of personal data only according to the instructions of the competent person or according to generally laid down rules.
- Protection of access to locations and to hardware and software of the controller or processor, including checks on authorisation for access.
- Ensuring that authorisations to access personal data have been assigned by the competent person and require proper documentation.
- Automated protocols on electronic access to personal data and regular checks of such protocols by the internal supervisory desk (therefore requiring all data processing activities to be recorded).
- Careful documentation for other forms of disclosure than automated access to data so as to demonstrate that no illegal data transmissions have taken place.

The measures are defined based on 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 (FRA/CoE 2018: 167).

Notification of a personal data breach (GDPR, Article 33)

The controller shall notify about a personal data breach to the supervisory authority without undue delay and where feasible, not later than 72 hours after having become aware of it. Moreover, the data controller shall document the breach and the remedial measures taken. The exception from the notification obligation is the ability of controllers to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons (GDPR, Article 33). Moreover, when the personal data breach is likely to result in a high risk to the

rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (GDPR, Article 34).

Prior consultation (GDPR, Article 36)

The controller is required to consult the supervisory authority before processing personal data if a data protection impact assessment (DPIA) indicates that the processing would result in a high risk to individuals' rights and freedoms in the absence of measures taken by the controller to mitigate the risk (GDPR, Article 36).

Stakeholders' consultation (GDPR, Article 35(9))

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations GDPR, Article 35(9)).

The GDPR establishes data controllers' liability for non-compliance with data processing requirements. In general, fines should be effective, proportionate and dissuasive (GDPR, Article 83(9)), where the proportionality depends on the interpretation of the imposing authority and the effectiveness should be directly proportional with its dissuasiveness. In certain cases, fines can reach 20 million EUR or up to 4% of the total worldwide annual turnover of the preceding year (GDPR, Article 83(5) and (6)).

1.2.3 Data controllers and data processors

When project partners process personal data in the SmartCHANGE project, they must demonstrate compliance with all GDPR data protection requirements. The scope of their obligations and responsibilities will be determined by their GDPR status-whether they are data controllers or data processors. If the project partner defines the purpose and means of data processing, the partner should be defined as the data controller and the primary entity responsible for compliance with data protection rules. In other words, the first and foremost role of the data controller is to allocate responsibility (WP29 2010). Data processors process personal data on behalf of data controllers and in accordance with the data controllers' instructions. Their processing activity may be restricted to a single task or context or be more general and extensive (WP29 2010). While data processors process personal data on behalf of data controllers, the lawfulness of processors' data processing activity is determined by the mandate given by data controllers. A processor that goes beyond its mandate and acquires a relevant role in determining the purpose or the essential means of processing is a controller or joint controller rather than just a processor (GDPR, Article 28(10)).

Data controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the protection of the rights and freedoms of data subjects (GDPR, Article 28(1)). Furthermore, the controller and processor must enter into an agreement that specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and data subject categories, and the controller's obligations and rights (GDPR, Article 28(3)).

Therefore, when different partners of the project are involved in processing personal data in a single processing activity (such as using the same technology), it is essential to define their respective roles prior to the processing activity. For example, in the scenario of an AI-based app for health advice, various partners may be involved, including the manufacturers of wearable devices, providers of technologies and algorithms for data analysis, providers of technologies for user identification or similar. While some partners may primarily serve as technical tools for data collection and processing, others may have decision-making authority regarding the purposes and methods of data processing activities. Depending on their functions, the role and responsibilities of each partner will vary under the GDPR. Further clarification on these roles and responsibilities will be addressed in later tasks and deliverables within other work packages.

1.2.4 Transfer of personal data within and outside the EU

The GDPR establishes distinct procedures and requirements for personal data transfers within and outside the EU. The majority of SmartCHANGE project partners are from European Union Member States. In this regard, the GDPR establishes free data movement within the European Union, which shall not be restricted or prohibited for the protection of natural persons in the processing of personal data (GDPR, Article 1(3)). When multiple entities are involved in processing personal data, their rights and obligations must be defined according to their roles: data controllers and processors.

There is, however, also one partner in this project that is based outside of the EU, namely in Switzerland, i.e. the Università della Svizzera Italiana (USI). With respect to the transfer of personal data to third countries, the GDPR establishes different requirements depending on the procedure and basis of the transfer. The basis applicable to the transfer of personal data from any EU-based SmartCHANGE partner to the Swiss partner is the adequacy decision – a decision of the European Commission that acknowledges an adequate level of data protection

in a country outside the European Union.[16] In the case of Switzerland, the Commission has already adopted an adequacy decision.[17] When personal data is transferred to an entity located in the country providing an adequate level of protection, such a transfer does not require any specific or extra authorization (GDPR, Article 45(1)).

When a country to which personal data is transferred does not provide an adequate level of protection, the transfer can take place with appropriate safeguards. These safeguards include binding corporate rules, standard data protection clauses, an approved code of conduct, and an approved certification mechanism (GDPR, Article 45(2)). In the absence of appropriate safeguards, other grounds for transfer can be applied, such as the data subject's explicit consent to the transfer subject to his/her being informed of the potential risks of such transfers for the data subject due to the lack of an adequacy decision and appropriate safeguards (GDPR, Article 49(1)).

1.2.5 Data protection impact assessment (DPIA)

In accordance with the GDPR's risk-based approach, performing a DPIA is not mandatory for every processing operation (WP29 2017a: 5). The GDPR requires a DPIA "[w]here a type of processing, in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR, Article 35(1)). The GDPR provides some examples when a DPIA is required (GDPR, Article 35(2)):

a) 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;*
b) processing on a large scale of special categories of data (such as data concerning health and biometric data), or personal data relating to criminal convictions and offences;
c) a systematic monitoring of a publicly accessible area on a large scale.

[16] European Commission. Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, last accessed 17th October 2023.
[17] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance) (2000/518/EC), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000D0518-20161217.

A DPIA is not only a requirement of the GDPR but a significant accountability tool. It helps data controllers comply with the GDPR requirements and demonstrate that appropriate technical and organisational measures have been taken to ensure compliance with the Regulation. In a word, a DPIA is a process for building and demonstrating compliance (WP29 2017a: 5).

There is no easy method, however, vis-à-vis impact assessments:

> "What matters is the choice of an appropriate assessment method allowing for the best understanding and treatment of possible consequences of the envisaged initiative. These methods can include qualitative or quantitative risk management, scenario planning, and scientific foresight, all while ensuring compliance with relevant legal and regulatory requirements (e.g., technical standards)." (Kloza et al. 2017)

The GDPR specifies the following minimum requirements for a DPIA (GDPR, Article 36(7) and Recitals 84 and 90):

- *a description of the envisaged processing operations and the purposes of the processing*;
- *an assessment of the necessity and proportionality of the processing*;
- *an assessment of the risks to the rights and freedoms of data subjects*;
- *the measures envisaged to:*
  - *address the risks;*
  - *demonstrate compliance with the Regulation*.

DPIAs can be used to evaluate a single data processing operation or multiple processing operations similar in nature, scope, context, purpose, and risks (WP29 2017a: 7). Depending on the specific implementation of the SmartCHANGE project, it is important to identify which processing operations meet the requirements for Data Protection Impact Assessments (DPIAs) and can be considered similar in nature. Conducting a DPIA can be beneficial for evaluating the potential impact on data protection when implementing a technology product, such as hardware or software, that is likely to be used by multiple data controllers for various processing operations. This may be relevant in the context of the project during the development of new technologies that will be utilized by different project partners. By conducting DPIAs, the project can assess and address any potential data protection risks associated with these technologies and ensure compliance with applicable regulations.

1.3 Medical Devices Regulation

1.3.1 Introduction

As explained in the introductory section of this benchmark, the use of wearable devices in the proof-of-concept study of the SmartCHANGE project and the development of software, e.g. an app, requires an analysis of Regulation 2017/745, i.e. the Regulation on Medical Devices (MDR), a very complex and technical piece of legislation (101 Recitals, 123 Articles and 17 annexes), that in this benchmark can be presented only very succinctly. The contextual application of this regulatory framework to the project will be dealt with in the deliverable D2.3 (SELP compliance framework, M9). Key questions for the project partners directly dealing with the development of software and the use of wearable devices will be asked in the process leading to the production of deliverable D2.3 in order to assess if and the extent to which wearable devices and software fall under the scope of the MDR.

1.3.2 Scope of 'Medical device'

In the MDR 'medical device' refers to (MDR, Article 2(1)):

> "[…] *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 the following **specific medical purposes***:
>
> - *diagnosis, **prevention**, monitoring, **prediction**, prognosis, treatment or alleviation **of disease**,*
> - *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
> - *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
> - *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.*
>
> *and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.* […]" [MDR, Article 2(1), our emphasis]

Funded by the European Union

For the sake of this benchmark, two are the key aspects of this definition: the intentional element and the presence of an exhaustive list of medical purposes, one or more of which, the device must fulfil to be classified as a medical device. The intentional element means that the manufacturer's intent in relation to the product, as can be understood from the information appearing on labels, user manuals, promotional or sales materials, is essential, i.e. the intention of users alone or a third party, such as a physician, is not relevant to qualify a given product as medical device. The second key aspect, i.e. the exhaustive list of medical purposes, qualifies the intentions of the manufacturer, restricting these to a limited and well-defined inventory.

The Regulation, in the same Article 2, reiterates that:

> *"4. 'active device' means any device, the operation of which depends on a source of energy other than that generated by the human body for that purpose, or by gravity, and which acts by hanging the density of or converting that energy. Devices intended to transmit energy, substances or other elements between an active device and the patient, without any significant change, shall not be deemed to be active devices.*
>
> ***Software shall also be deemed to be an active device**;"* [MDR, Article 2(4), our emphasis]

1.3.3 Essential requirements

A device that falls into the scope of the MDR and whose manufacturers/producers plan to put on the market needs to go through procedures such as a clinical evaluation, a conformity assessment, assessing the risks of the device, 'CE' marking of the device, control during the marketing of the device and registration in the following electronic systems (Yao/Quinn 2023):

- of medical devices,
- of Unique Device Identification System ('UDI system'),
- of devices' economic operators,
- of clinical investigations,
- of vigilance and post-market surveillance,
- of market surveillance.

While the manufacturer is the primary subject responsible for the compliance with the requirements, importers and distributors or other subjects may have to comply with obligations as well (MDR, Article 16(1)):

"1. *A distributor, importer or other natural or legal person shall assume the obligations incumbent on manufacturers if it does any of the following:*

a) makes available on the market a device under its name, registered trade name or registered trademark, except in cases where a distributor or importer enters into an agreement with a manufacturer whereby the manufacturer is identified as such on the label and is responsible for meeting the requirements placed on manufacturers in this Regulation;

b) changes the intended purpose of a device already placed on the market or put into service;

c) modifies a device already placed on the market or put into service in such a way that compliance with the applicable requirements may be affected." […][our emphasis]

The specific procedures and requirements to launch a device on the market depend on the classification of the device itself, as described in the following section.

1.3.4 Classification

The classification rules for medical devices stem from the vulnerability of the human body in light of the potential risks that come with a device on the basis of its design and material features, hence the obligation for manufacturers to "establish, implement, document, and maintain a risk management system. Risk management shall be understood as a continuous iterative process requiring regular, systematic updating throughout the entire lifecycle of a device." (MDR, Annex I, Chapter 1, Article 3)

The MDR assigns medical devices to four classes named with the Roman numerals I, IIa, IIb, and III, depending on their intended purpose and inherent risks (MDR, Article 51(1)), where class I refers to devices with the lowest risk and class III to those with the highest risk. While the criteria of classification, laid out in Annex VIII, are quite complex, it is fair to say that the more a device interferes with the human body system, the more this will be assigned to a high-risk category, on a continuum where intuitive lines can be drawn between devices applied to the surface of the body, those that enter body orifices and those that are implanted in the body itself. It is easy, therefore, to understand why a pair of spectacles will fall in the lowest-risk category, i.e. class I, and a pacemaker in the highest-risk category, i.e. class III, the requirements and procedures for the latter being stricter than for the former. In other words, the "classification rules are determined by the device's duration of body contact,

invasive character, use of energy source, effect on the central circulation or nervous system, diagnostic impact, or incorporation of a medicinal product." (Yao/Quinn 2023).

Wearable devices, particularly smart wearable ones, are defined in a document by the European Commission, as:

> "*body-borne computational and sensory devices which can sense the person who wears them and/or their environment. Wearables can communicate either directly through embedded wireless connectivity or through another device (e.g. a smartphone). The data collected by the wearable device about the user or its environment is processed in a processing unit located locally or in an external server, and the results are ultimately provided to the wearer. Smart wearables may have control, communication, storage and actuation capabilities.*"[18]

As written in section 1.3.2 above, the intentions of the manufacturer matter. It is therefore not always easy to determine whether a wearable fulfils a medical purpose or a non-medical one. For instance, a heart rate monitoring bracelet produced to improve the performance of a runner may not be considered a medical device, but it could be considered one if the purpose of the monitoring is medical in nature, such as "prediction" or "prognosis" (MDR, Article 2(1)). According to Annex VIII (Chapter 3, Rule 10),

> *"Active devices intended for diagnosis and monitoring are classified as class IIa:*
> *— if they are intended to supply energy which will be absorbed by the human body, except for devices intended to illuminate the patient's body, in the visible spectrum, in which case they are classified as class I;*
> *— if they are intended to image in vivo distribution of radiopharmaceuticals; or*
> *— **if they are intended to allow direct diagnosis or monitoring of vital physiological processes**, unless they are specifically intended for monitoring of vital physiological parameters and the nature of variations of those parameters is such that it could result in immediate danger to the patient, for instance variations in cardiac performance, respiration, activity of the central nervous system, or they are intended for diagnosis in clinical situations where the patient is in immediate danger, in which cases they are classified as class IIb."* [our emphasis]

In general, "software, which drives a device or influences the use of a device, shall fall within the same class as the device." although "if the software is independent of any other device,

[18] EUROPEAN COMMISSION - Directorate-General for Communications Networks, Content and Technology. *Smart Wearables Reflection and Orientation Paper*. December 2017. Available at: ec.europa.eu/newsroom/dae/document.cfm?doc_id=50020

it will be classified in its own right." (MDR, Annex VIII, Chapter 2, Article 3(3)). As far as software is concerned, the Medical Device Regulation defines the classes as follows (MDR, Annex VIII, Chapter 3, Article 6.3: Rule 11):

> *"Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:*
> *— death or an irreversible deterioration of a person's state of health, in which case it is in class III; or*
> *— a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as class IIb.*
> *Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.*
> *All other software is classified as class I."*

When a dispute related to the application of Annex VIII arises between the manufacture and the notified body, i.e. the conformity assessment body designated in compliance with the MDR, it will be "referred for a decision to the competent authority of the Member State in which the manufacturer has its registered place of business." (MDR, Article 51(2))

The attribution of a class defines the additional procedures vis-à-vis the marketing of the device and the conformity assessment.

1.3.5 Conformity assessment

Annexes IX and X of the MDR list the rules for the conformity assessment rules, i.e. the process demonstrating the compliance with the Regulation by way of establishing, documenting, and implementing a quality management system by the manufacturer, as described in Chapter 1 of Annex IX.

1.3.6 The "CE" marking

The 'CE' marking "indicates that the relevant products sold in the EEA have been evaluated to meet high safety, health, and environmental protection requirements", (Yao/Quinn 2023) thus certifying the compliance with the applicable (MDR, Article 10(6)). The marking must: i) be affixed visibly, legibly, and indelibly to the device or its sterile packaging (MDR, Article 20(3) and (4)), ii) appear in any operating instructions and on any sales packaging, followed by the identification number of the relevant notified body responsible for the conformity assessment (if involved).

1.3.7 National notified bodies

National notified bodies are the authorities responsible with regard to conformity assessments and related procedures at the Member State level. “Any Member State that intends to designate a conformity assessment body as a notified body, or has designated a notified body, to carry out conformity assessment activities shall appoint an authority (‘authority responsible for notified bodies’), which may consist of separate constituent entities under national law and shall be responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for the monitoring of notified bodies, including subcontractors and subsidiaries of those bodies.” (MDR, Article 35(1)).

1.3.8 Clinical evaluation and investigation

The term *clinical evaluation* refers to a “systematic and planned process to continuously generate, collect, analyse and assess the clinical data pertaining to a device in order to verify the safety and performance, including clinical benefits, of the device when used as intended by the manufacturer” (MDR, Article 2(44)). A *clinical investigation*, on the other hand, is a “any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device” (MDR, Article 2 (45)), mandatory for class III devices. In light of the wearable device to be used and app to be developed in the SmartCHANGE project, this section will concentrate on the clinical evaluation.

The European Commission in its Guideline on medical devices (MEDDEV 2.7/1: 10) states:

> *“Clinical evaluation is conducted throughout the life cycle of a medical device as an ongoing process. Usually, it is first performed during the development of a medical device in order to identify data that need to be generated for market access. Clinical evaluation is mandatory for initial CE-marking, and it must be actively updated thereafter.”*

It is based on a “comprehensive analysis of available pre- and post-market clinical data relevant to the intended purpose of the device in question, including clinical performance data and clinical safety data.” (MEDDEV 2.7/1: 10) The clinical data is information about safety and performance that is generated with the use of the device and is “sourced from:

- clinical investigation(s) of the device concerned,
- clinical investigation(s) or other studies reported in scientific literature, of a device for which equivalence to the device in question can be demonstrated,

- reports published in peer-reviewed scientific literature on other clinical experiences of either the device in question or a device for which equivalence to the device in question can be demonstrated,
- clinically relevant information coming from post-market surveillance, in particular the post-market clinical follow-up." (MDR, Article 2(48))

In MEDDEV 2.7/1 the European Commission describes the stages of a clinical evaluation (MEDEV 2.7/1: 13):

- *"Stage 0: define the scope, and plan the clinical evaluation;*
- *Stage 1: identify pertinent data;*
- *Stage 2: appraise each individual data set in terms of its scientific validity, relevance and weighting;*
- *Stage 3: analyse the data, whereby conclusions are reached about:*
  - *compliance with essential requirements on performance and safety of the device, including its benefit/risk profile,*
  - *the contents of information materials (including the label, IFU of the device, available promotional materials, including accompanying documents possibly foreseen by the manufacturer),*
  - *residual risks and uncertainties or unanswered questions (including rare complications, long-term performance, and safety under widespread use), whether these are acceptable for CE-marking, and whether they are required to be addressed during PMS.*
- *Stage 4: finalise the clinical evaluation report. The clinical evaluation report summarises and draws together the evaluation of all the relevant clinical data documented or referenced in other parts of the technical documentation. The clinical evaluation report and the relevant clinical data constitute the clinical evidence for conformity assessment."*

1.3.9 SmartCHANGE as a research project

From the point of view of the SmartCHANGE project, if the wearable and the developed app will be found to fall under the scope of the MDR, particularly vis-à-vis possible exploitation paths at the end of the project, the consortium will need to consider the necessity of conducting a clinical evaluation. While an in-depth analysis of this issue, as written at the beginning of this section, will be discussed in depth in deliverable D2.3, there is nevertheless the question of SmartCHANGE as a research project, i.e. independent from SmartCHANGE as

an exploitable product.[19] Such a distinction is useful if SmartCHANGE partners would like to avoid, at this stage, the full application of the strict requirements under the EU Medical Devices Regulation, though it will be for the partner's consideration whether they wish to pursue this path, or rather opt for the full conformity assessment process at this point, following a determination of the SmartCHANGE system, or parts thereof, as a medical device. Requirements and considerations related to both paths are set out below.

Article 5(5) of the MDR provides that in situations where "devices, manufactured and used only within health institutions established in the Union" (i.e. where there is no intention to place it on the market, but limit its use to the health institution), the Regulation shall not apply, with the exception of Annex I.

Within the SmartCHANGE the research project, there is not an immediate intention in bringing the SmartCHANGE system onto the market (exploitation is only considered at the end of the project). Rather, the project aims to develop and test the system in the controlled environment of the pilots without the intention to request a 'CE' marking (see Section 5.6) at this stage. Accordingly, it seems that the project would fit under Article 5(5) of the MDR which allows development and use of a medical device without the intention of requesting a 'CE' marking within health institutions.

The application of Article 5(5) requires that a number of conditions are met, namely:

(a) The devices are not transferred to another legal entity;

(b) manufacture and use of devices occurs under appropriate quality management systems;

(c) the health institution justifies in its documentation that the target patient group's specific needs cannot be met, or cannot be met at the appropriate level of performance by an equivalent device available on the market;

(d) the health institution provides information upon request on the use of such devices to its competent authority which shall include a justification of their manufacturing, modification and use;

(e) the health institution draws up a declaration which it shall make publicly available, including:

i) the name and address of the manufacturing institution;

[19] The following part of this section draws from Feirabend/Quinn 2020.

ii) the details necessary to identify the device;

iii) a declaration that the device meets the general safety and performance requirements set out in Annex I to this Regulation and, where applicable, information on which requirements are not fully met with a reasoned justification therefore.

(f) the health institution draws up documentation that makes it possible to have an understanding of the manufacturing facility, the manufacturing process, the design and performance data of the devices, including the intended purpose, and that is sufficiently detailed to enable the competent authority to ascertain that the general safety and performance requirements set out in Annex I to this Regulation are met;

(g) the health institution takes all necessary measures to ensure that all devices are manufactured in accordance with the documentation referred to in point (f), and

(h) the health institution reviews experience gained from clinical use of the devices and takes all necessary corrective actions.

Application of Article 5(5) of the MDR would result in an exemption of the stringent requirements of the Regulation, with the exception of Annex I and those set out in Article 5(5).

1.3.9.1 Safety and performance requirements under Annex I

Annex I sets out the general safety and performance requirements that a medical device should adhere to. The requirements in the Annex aim to reduce the risks of the use of a medical device as far as possible without adversely affecting the benefit-risk ratio (MDR, Annex I, para. 2). It sets out some general safety and performance requirements, requirements regarding design and manufacture, as well as regarding necessary information supplied with the device (MDR, Annex I, Chapters I to III).

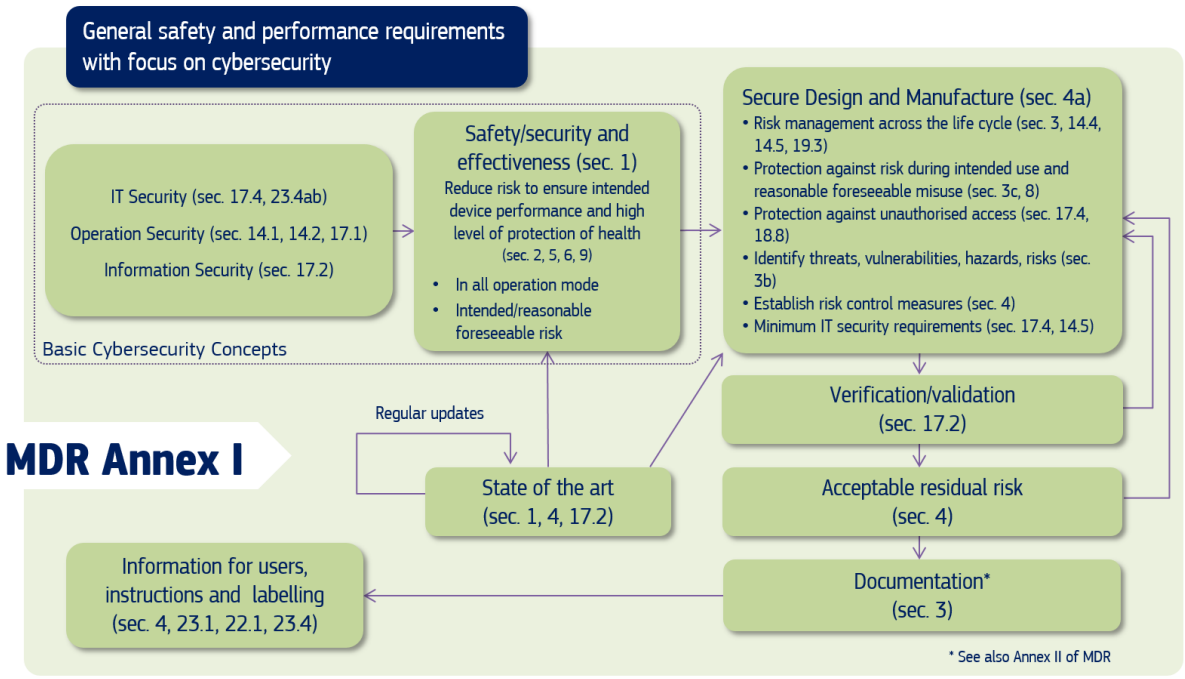
For instance, it requires manufacturers to establish and implement a risk management system, to adopt risk control measures and to minimise all known and foreseeable risks and undesirable side-effects (MDR, Annex I, para. 3, 4, 8 and 14). Any diagnostic devices and devices with a measuring function must provide sufficient accuracy, precision and stability for their intended purpose, based on appropriate technical methods (MDR, Annex I, para. 15).

Highly relevant for SmartCHANGE are the requirements set out for electronic programmable systems (both devices that incorporate electronic programmable systems and software that are devices themselves) (MDR, Annex I, para. 17). Paragraph 17(2) requires that “software shall be developed and manufactured in accordance with the state of the art taking into

account the principles of development life cycle, risk management, including information security, verification and validation." Furthermore, paragraph 17(3) sets out that such software intended to be used in combination with mobile computing platforms "shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise)." Manufacturers shall also set out the minimum requirements in terms of "hardware, IT network characteristics and IT security measures, including protection against unauthorised access" that is necessary to run the software as intended (MDR, Annex I, para. 17(4)).

In their guidance, the MDCG helpfully sets out the cybersecurity requirements contained in Annex I in relation to both pre-market and post-market aspects, which are illustrated in the following figure: [20]

Figure 1 - Cybersecurity requirements contained in MDR Annex I



[20] MDCG, *MDCG 2019-16 Guidance on Cybersecurity for medical devices*, December 2019, see https://ec.europa.eu/docsroom/documents/38941 (last accessed on 18 October 2023), p. 5.

Further requirements related to 'active devices' (the operation of which depends on a source of energy other than that generated by the human body for that purpose) (MDR, Article 2(4)) and devices connected to them are also set out, including the need to adopt appropriate measures to eliminate or reduce consequent risks of a single fault condition and that devices are developed in such a way to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended (MDR Annex I, para. 18).

Devices must also be developed in such a way that they protect, as much as possible, users against mechanical and thermal risks (MDR, Annex I, para. 20). As the SmartCHANGE system is also intended to be used by lay persons, Annex I requires that it be developed and manufactured in such a way that "they perform appropriately for their intended purpose taking into account the skills and means available to laypersons and the influence resulting from variation that can be reasonably anticipated in the layperson's environment." (MDR, Annex I, para. 22(1)).

Finally, it sets out what information should be provided to users of the device, including on the label as well as the instructions for use. Such information will identify the device and its manufacturer and any safety and performance information relevant to the user, and "may appear on the device itself, on the packaging or in the instructions for use" (MDR, Annex I, para. 23(1)). If the manufacturer has a website, such information should also be included there and kept up to date (MDR, Annex I, para. 23(1)).

For class I and class IIa devices, no instructions for use are necessary in case such devices can be used safely without such instructions (MDR, Annex I, para. 23(1)(d)). In the event instructions of use are nevertheless prepared, and if devices are intended for use with other devices or general purpose equipment, it should include information to identify such devices/equipment to ensure a safe combination as well as information related to known restrictions to combinations of devices/equipment (MDR, Annex I, para. 23(4)(q)).

Paragraph 23(2) of Annex I lists the information that should be included on the label of the device, including that, if it is intended for clinical investigation only, the words 'exclusively for clinical investigation' (MDR, Annex I, para. 23(2)(q)).

1.3.9.2 Device used in connection with the SmartCHANGE system

In terms of the technologies that will be used to collect data to input in the SmartCHANGE system, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, while some might already bear the 'CE'-marking of a medical device, some of these will not be considered a medical device at all as their manufacturer did not intend them

for medical purposes, even if they are used as such. In case of the latter technologies, it is important to note that the relevant national ethical boards may take particular note of any tests with the use of non-'CE'-marked medical devices.

1.3.9.3 SmartCHANGE research proof-of-concept study

Falling under Article 5(5) of the EU Medical Devices Regulations means that the SmartCHANGE research project would not have to follow all the stringent requirements set by the Regulation, including conformity assessment, clinical evaluation and investigation, as it would not seek 'CE' certification and placement on the internal EU market during the course of the SmartCHANGE project.

The SmartCHANGE research project does intend to conduct large scale testing of the SmartCHANGE system on human participants. According to the EU Medical Devices Regulation, "any systematic investigation involving one or more human subjects undertaken to assess the safety or performance of a device" constitutes a clinical investigation. While by definition the SmartCHANGE pilots may constitute a clinical investigation, they do not fall under Article 62(1) of the MDR as they are not "carried out as part of a clinical evaluation for conformity assessment purposes" as SmartCHANGE would not, at this stage, intending to obtain a 'CE' marking. Article 82(1) provides that such 'other' clinical investigations only have to observe a number of minimal requirements set out in Article 62(2), (3), (4)(b), (c), (d), (f), (h), (l) and (6):

- *Where the sponsor of a clinical investigation is not established in the Union, that sponsor shall ensure that a natural or legal person is established in the Union as its legal representative.*
- *Clinical investigations shall be designed and conducted in such a way that the rights, safety, dignity and well-being of the subjects participating in a clinical investigation are protected and prevail over all other interests and the clinical data generated are scientifically valid, reliable and robust.*
- *Clinical investigations shall be subject to scientific and ethical review. The ethical review shall be performed by an ethics committee in accordance with national law.*
- *A clinical investigation may only be performed when:*
  - *an ethics committee, set up in accordance with national law, has not issued a negative opinion in relation to the investigation, which is valid for that entire Member State under its national law;*
  - *the sponsor, or its legal representative or a contact person is established in the Union;*
  - *vulnerable populations and subjects are appropriately protected;*
  - *the subject or, where the subject is not able to give informed consent, their legally designated representative has given informed consent;*

- *the rights of the subject to physical and mental integrity, to privacy and to the protection of the data concerning them in accordance with the GDPR are safeguarded;*
- *the investigational device(s) in question conform(s) to the applicable general safety and performance requirements set out in Annex I apart from the aspects covered by the clinical investigation and that, with regard to those aspects, every precaution has been taken to protect the health and safety of the subjects. This includes, where appropriate, technical and biological safety testing and pre-clinical evaluation, as well as provisions in the field of occupational safety and accident prevention, taking into consideration the state of the art.*

- *The investigator shall be a person exercising a profession which is recognised in the Member State concerned as qualifying for the role of investigator on account of having the necessary scientific knowledge and experience in patient care. Other personnel involved in conducting a clinical investigation shall be suitably qualified, by education, training or experience in the relevant medical field and in clinical research methodology, to perform their tasks.*

Moreover, Article 82(2) further provides that Member States will define further requirements for such investigations to ensure the protection of the rights, safety and well-being of research participants as well as the scientific and ethical integrity on the investigation.

While application of Article 82 (and relevant parts of Article 62) of the MDR is not strictly required in connection to the development and use of devices under Article 5(5) (as this provides that with the exception of Annex I, the MDR does not apply), it is advisable to nevertheless take guidance from the requirements under Article 82, as they mainly sets out basic principles of good clinical practice for conducting research with medical devices involving human participants. Moreover, taking into consideration the requirements of Article 82 during the SmartCHANGE pilots would facilitate the use of any clinical data gathered during these pilots in any future conformity assessment process under the MDR should the SmartCHANGE partners wish to place the system on the market during its exploitation stage.

Moreover, in terms of retaining the clinical data gathered during the SmartCHANGE project pilots, it is recommended to keep these on file for a period of 25 years. This is based on a reading of the MDR with the EU Clinical Trials Regulation (CTR). As mentioned above, while the EU Clinical Trials Regulation will only be directly applicable in cases of clinical trials that test medicinal products, there are a number of provisions in the EU Medical Devices Regulation that require harmonisation of certain parts of the medical device trial procedures with the Clinical Trials Regulation.[21] This may be interpreted to mean that it shows the

[21] For instance, see MDR, Recital 67 and Articles 73(2) and 78(7).

underlying intention that the MDR strives for compatibility and synergy with the EU Clinical Trials Regulation, where possible. Accordingly, as a measure of good clinical practice, and especially since the SmartCHANGE pilots will use of human participants, it is advised to strive for this 25-year retention period to ensure the validity of the research.

1.3.9.4 SmartCHANGE as exploitable product

For SmartCHANGE as an exploitable product at the end of the SmartCHANGE research project, there is the intention to bring the SmartCHANGE system onto the market. With that intention comes the renewed consideration of whether the SmartCHANGE system, or any of its modules, is intended as a medical device. As identified above, it is considered likely that, at least some of its modules, are intended and therefore will be considered a medical device. At that time, it would fall under the full scope of the MDR.

Under MDR, the SmartCHANGE system would have to "go through the procedures of clinical evaluation, conformity assessment, assessing the risks of the device, 'CE' marking of the device, control during marketing of the device" as well as registration in a number of electronic systems (of medical devices; Unique Device Identification System ("UDI system"); devices' economic operators; clinical investigations; vigilance and most-market surveillance; and market surveillance). The obligations under the MDR are mostly directed to manufacturers of devices. For instance, Article 10 sets out the general obligations of manufacturers. In the event a manufacturer is not established in the EU, the device may only be placed on the EU internal market if the manufacturer designates a sole authorised representative (MDR, Article 11). Obligations are also foreseen for importers, distributers and, in some instances, other persons (MDR, Articles 13, 14 and 16).

1.4 Relevant regulatory frameworks in Member States

Article 9(4) of the GDPR permits Member States to maintain divergent laws pertaining to health, biometric or genetic data. It is therefore important to consider Member State laws on the processing of health data given that the SmartCHANGE project will likely make extensive use of personal health data. In addition, as mentioned in section 1.2.2.4 above, the research exception to article 9(1) of the GDPR needs to be analysed together with the relevant national legislation, as the GDPR itself refers to national legislation both in article 9(2)(j), i.e.:

> *"processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with art. 89(1) of the GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable*

> *and specific measures to safeguard the fundamental rights and the interests of the data subject."*

and in Article 89(1):

> *"Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of* ***data minimisation****. Those measures* ***may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."*** [our emphasis]

Furthermore, the same Article 89, in paragraph (2), clarifies that:

> "*Where personal data are processed for scientific or historical research purposes or statistical purposes,* ***Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21*** *subject to the conditions and safeguards referred to in paragraph 1 of this Article in* ***so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes****."* [our emphasis]

The Articles 15, 16, 18 and 21 referred to in Article 89(2) above are those pertaining data subject rights, specifically and respectively: the right of access, the right to rectification, the right to restriction of processing and the right to object. The GDPR "thus accords research special treatment in respect of the general data protection rules to avoid limitations to research development and to comply with the objective of achieving a European research area, as set out in Article 179 TFEU." (FRA/CoE 2018: 340). This special treatment includes "the processing of personal data for scientific research purposes, including technological development and demonstration, basic research, applied research and privately funded research." (FRA/CoE 2018: 340), acknowledging also the difficulty in "fully identifying the subsequent purpose of personal data processing for scientific research purposes at the time of data collection." (FRA/CoE 2018: 340)

As both Article 9(2)(j) and Article 89(2) of the GDPR mention specifically Member State law, the following sections will look at the relevant laws of the fours EU Member States where the

Funded by the European Union

proof-of-concept study of the SmartCHANGE project will take place, i.e. Finland, the Netherlands, Portugal and Slovenia, bearing in mind that the scientific research exception to Article 9 is especially suited, in the context of a project such as SmartCHANGE, for large datasets already in existence at the start of the project. The most advisable legal base for the proof-of-concept study, considering the size of the samples, is consent.

1.4.1 Finland

Finland adopted the national Data Protection Act 1050/2018 that "specifies and supplements Regulation (EU) 2016/679" (FINDPA 2018, Section 1). The two most relevant sections of the Act, form the point of view of the research conducted in the SmartCHANGE project, are Section 6 and Section 31. Section 6 confirms scientific research as a legal base in line with Article 9(2)(2) of the GDPR:

> *"Article 9(1) of the Data Protection Regulation does not apply:*
> *[…]*
> *7) to the processing of data for scientific or historical research purposes or for statistical purposes;*
> *[…]"* (FINDPA 2018: Section 6)

Although Section 6 of the Act only lists special measures for the safeguard of the data subject's rights with reference to cases "when an insurance institution processes data it has received in the course of insurance activities on an insured person's or claimant's state of health, illness or disability, or such data on the treatment or other comparable measures directed at the insured or the claimant that are necessary for determining the liability of the insurance institution;" (FINDPA 2018: Section 6(1)), Article 89 of the GDPR, with regards to measures in line with the principle of data minimisation (e.g. pseudonymisation) still applies.

Moreover, in Section 31 of the Finnish Act, the scientific research exception is qualified as follows:

> "*Where personal data are processed for scientific or historical research purposes, the rights of the data subject laid down in Articles 15, 16, 18 and 21 of the Data Protection Regulation may be derogated from, where necessary, provided that:*
>
> *1) the processing is based on an* ***appropriate research plan****;*
>
> *2) a* ***person or group responsible*** *for the research has been* ***designated****; and*

*3) the personal data are used and disclosed only for scientific or historical research purposes or for other compatible purposes, and the procedure followed is also otherwise such that **data concerning a given individual are not revealed to outsiders**.* […]" (FINDPA 2018: Section 31) [our emphasis]

In addition to the requirements listed above, Section 31 requires also:

"[…] *that a **data protection impact assessment** referred to in Article 35 of the Data Protection Regulation be carried out **or** that **codes of conduct** in accordance with Article 40 of the Data Protection Regulation, in which the derogation from the rights of the data subject referred to above is appropriately taken into account, be complied with. The **written data protection impact assessment shall be submitted to the Data Protection Ombudsman for information before the processing is started**.*" (FINDPA 2018: Section 31) [our emphasis]

1.4.2 Portugal

Portugal adopted in 2019 the law 58/2019, known as General Data Protection Regulation Implementation Act. There is currently no official translation into English of the Act and the following information relies on machine translations of the Portuguese text, which will be checked against the understanding of the law by the DPO of the Portuguese partner in view of deliverable D2.3 of the SmartCHANGE project.

The key requirements in terms of processing of personal data for scientific research purposes in law 58/2019 are listed in Article 31, which on the one hand bases itself on the content of Article 89 of the GDPR, while on the other hand adds further requirements (bold and underlined in the text below):

*(1) Processing for archiving purposes of public interest, scientific or historical research purposes or statistical purposes must respect the principle of **data minimization and include anonymization or pseudonymization** whenever the intended purposes can be achieved by one of these means.*

*(2) When personal data is processed for archiving purposes of public interest, scientific or historical research purposes or statistical purposes, the rights of access, rectification, limitation of processing and opposition provided for in articles 15, 16, 18 and 21 GDPR, **are derogated to the extent necessary**, if those rights are likely to make it impossible or seriously harm the achievement of those purposes.*

[…]

(4) Consent regarding the processing of data for scientific research purposes may cover different areas of research or be given only for certain areas or specific research projects, and ***in any case the ethical standards recognized by the scientific community must be respected****.*

(5) Without prejudice to the provisions of the National Statistical System Law, personal data processed for statistical purposes must be anonymized or pseudonymized, in order to safeguard the protection of data subjects, particularly with regard to the impossibility of re-identification once the statistical operation has been completed. [Law 58/2019, Portugal, Article 31, our emphasis]

1.4.3 Slovenia

Slovenia adopted in December 2022 the ZVOP-2 Act (Zakon o varstvu osebnih podatkov, i.e. Personal Data Protection Act). There is currently no official translation into English of the Act and the following information relies on machine translations of the text in Slovenian, which will be checked against the understanding of the law by the DPOs of the Slovenian partners in view of deliverable D2.3 of the SmartCHANGE project.

In ZVOP-2 the prohibition to process personal data in manner that would lead to discrimination is laid out very early in the text of the law:

"*The processing of personal data is prohibited if it is carried out in a way or results in impermissible discrimination based on nationality, race, skin color, religion, ethnicity, gender, language, political or other belief, sexual orientation, gender identity, property status, location birth, education, social status, disability, citizenship, place or type of residence, state of health, genetic predisposition or any other personal circumstance of an individual (hereinafter: individual).*" (ZVOP-2, Article 2)

For the processing of personal data with scientific research purposes, the ZVOP-2 lays out very specific requirements in Article 68 and 69 of the Act:

"*(1) The processing of personal data for scientific research, historical research and statistical purposes (hereinafter referred to as: research) is permitted for organizations and individuals that use* ***ethical principles and methodology in the field of research*** *and the rules regarding the protection of personal data from this chapter in their operations.*

(2) It is considered that ***the purpose of processing personal data for research does not conflict with the purpose of their collection****.*

(3) For access to personal data for research purposes, ***the provisions of Chapter 2 of Part I of this Act regarding the procedure before the controller and the processor shall apply mutatis mutandis****.*" (ZVOP-2, Article 68, our emphasis)

Article 69 goes very much into detail:

"*1)* ***Regardless of the original purpose*** *of the processing, the controller may further process personal data,* ***including special types of personal data****, for the purpose of research, if such processing is permitted by another law or* ***if****:*

1. the individual to whom this data relates ***has not prohibited*** *the processing of his personal data for the purpose of research or prohibited the processing of his personal data in a specific research field, which also includes the purposes of research, or*

2. the individual to whom the personal data, which constitutes a professional secret, relates, has given written consent to the processing.

(2) Research organizations and researchers ***who are bound by the ethical principles*** *and methodology referred to in the first paragraph of the previous article may obtain personal data from the controller for research purposes, including special types of personal data,* ***if they submit a description*** *of the research, which includes:*

1. the ***title*** *of the research and the* ***name of the person responsible*** *for the research (for natural persons, personal name, title and place of residence, and for legal persons, company, registration number and registered office);*

2. ***data on the researchers*** *(personal name, title, place of residence, possible relationship to the research owner and possible researcher code);*

3. ***purposes*** *or objectives of the research;*

4. ***intended means and actions*** *of personal data processing,* ***including a statement of ethical principles*** *and methodology from the first paragraph of the previous article and measures for the security of personal data;*

> *5. the **types of personal data** that we would like to obtain from the controller and the categories of individuals to whom this data relates;*
>
> *6. **the form in which they wish to receive personal data** (original personal data, pseudonymized personal data, personal data in a form that does not allow identification, anonymized data), and a statement of the reason for the specific data format;*
>
> *7. **method of publication** or other accessibility of the research.*" (ZVOP-2, Article 68, our emphasis)

Moreover, Article 69 of the ZVOP-2 Act, requires that the description of the research has to be accompanied by a DPIA if the conditions of Article 35 and 36 of the GDPR apply, i.e. when the processing is likely to result in a high risk to the rights and freedoms of natural persons (ZVOP-2, Article 69(3). Article 69(4) of the same Act lays out the conditions for a refusal to provide personal data for the research by the controller:

> "*1. if the conditions from the second and third paragraphs of this article are not met;*
> *2. if he considers that the requested personal data **are not suitable** for carrying out the research;*
> *3. if he considers that the purposes or goals of the research **do not justify interference** with the rights of individuals to whom personal data refer;*
> *4. if the operator from the private sector and the research organization or the researcher **do not reach an agreement on the price** of providing the data;*
> *5. if he considers that **the measures for the security** of personal data are not adequate, or*
> *6. if it is **confidential information** in accordance with the Act on Confidential Information.*" (ZVOP-2, Article 69(4), our emphasis)

Article 69(5) lays out that there is no obligation to inform the individual data subject in relation to the processing connected to the research, but rather have the obligation to announce to the general public via a website that the processing is taking place. At the end of the research:

> "*(6) Personal data that was the subject of the research shall be **destroyed or irretrievably anonymized** at the end of the research, **unless another law provides otherwise**, if the individual has consented to the further storage of personal data or the further storage is important for the execution of the purpose of the research. At the end of the research, the researcher informs the manager to whom the personal data was provided in writing whether, when and how he/she destroyed it or handled it in a different way.*" (SVOP-2, Article 69(6), our emphasis)

The results of the research "are published in an anonymized form. The results of the research may also be published in a pseudonymized form, if the publication of the data in an anonymized form is not possible for technical reasons or due to the pursuit of the research objectives" (ZVOP-2, Article 69(7)), although personal data can be published if the data subject has given written consent to this end (ZVOP-2, Article 69(7)). The rights of the data subject to access (GDPR, Article 15) and to object (GDPR, Article 21) are guaranteed, unless these rights jeopardize the purpose of the research (ZVOP-2, Article 69(8)). Controllers in the public sector must provide data for research purposes free of charge (ZVOP-2, Article 69(9)).

1.4.4 The Netherlands

The Parliament of the Netherlands adopted the law implementing the GDPR in May 2018. The General Data Protection Regulation Implementation Act is available in a version translated into English (NLGDPRIA 2018).

The scientific research exception to article 9 of the GDPR is dealt with in Article 24 and 44 of the NLGDPRIA 2018. Article 24 states that:

> *"In view of Article 9(2)(j) of the Regulation, the prohibition on processing special categories of personal data does not apply if:*
>
> > *a. the processing is necessary for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) of the Regulation;*
> >
> > *b. the research referred to in point (a) serves a public interest;*
> >
> > *c. requesting* ***explicit consent proves to be impossible*** *or requires disproportionate effort; and*
> >
> > *d. adequate* ***safeguards are provided to prevent disproportionate infringement*** *of the data subject's privacy."* (NLGDPRIA 2018, Article 24, our emphasis)

Article 44 of the Dutch Act repeats almost the same exception to data subjects rights of Article 89(2) of the GDPR, i.e. for Article 15, 16 and 18 of the GDPR, but nor for Article 21 of the GDPR (i.e. the right to object):

> *"The controller may refrain from observing Articles 15, 16 and 18 of the Regulation when processing is carried out by agencies or services for scientific research or statistical purposes and the necessary measures have been taken to ensure that*

personal data can only be used for statistical or scientific purposes." (NLGDPRIA 2018, Article 44)

As far as consent from minors is concerned, Article 5 of the Dutch Act states:

"*1. If Article 8 of the Regulation does not apply*[22] *and the data subject is* ***under sixteen years*** *of age, the consent of the data subject's* ***legal representative is required*** *instead of the consent of the data subject.*

2. If the data subject has been placed ***under guardianship or is the subject of an administration or protection order****, the consent of the legal representative is required instead of the consent of the data subject insofar as the data subject has no legal capacity or authorization to act in the matter in question.*

3. The legal representative of the data subject ***may revoke consent at any time****.*

4. The data subject's rights as referred to in Chapter III of the Regulation are to be exercised by the data subject's legal representatives if the data subject is under sixteen years of age, has been placed under guardianship or is the subject of an administration or protection order and insofar as the data subject has no legal capacity or authorization to act in the matter in question." (NLGDPRIA 2018, Article 5, our emphasis)

[22] i.e. if consent is not sought for in relation to the offer of information society services (e.g. social media platforms).

2 Ethical and Societal Concerns

This section lays out the general principle of ethics and societal concerns in relation to the relevant subject matter of the SmartCHANGE project, particularly in relation to research involving children and the potential impact of an AI-tool on children and the general public. A contextual application of the principles described in this section will be part of deliverable D2.3, i.e. “SELP compliance framework” upon feedback from partners vis-à-vis the proof-of-concept study, and also inform the ethics review of month 12.

2.1 Introduction

As stated in the introduction to this benchmark, the overall aim of the SmartCHANGE project is to is to develop trustworthy, AI-based decision-support tools that will help health professionals and citizens reduce long-term risk of Non-Communicable Diseases, by accurately assessing the risk of children and youth, including those with difficult-to-detect risks, and promoting delivery of optimised risk-lowering strategies. End-users – health professionals, families, children and youth – will be engaged from the start of the project in four EU countries, namely: Finland, the Netherlands, Portugal and Slovenia. End-users will be engaged in exploration of the use, benefits and risks of AI, co-creation of risk-prediction models, their explanations and visualisations, as well as co-design of the SmartCHANGE tools. Health professionals, families, children and youth will additionally participate in the proof-of-concept study in four different real-world healthcare scenarios in four countries, where they will be assigned to an intervention or control group. To evaluate the SmartCHANGE tools, the following outcomes will be assessed using surveys and (focus group) interviews: feasibility outcomes (acceptability, demand, implementation, practicality, adaptation, integration, expansion, limited efficacy testing), usability and explainability, health outcomes (improvement to standard of care; aggregated risk score, individual risk factor levels).

End-users participating in the co-design and proof-of-concept study will be diverse in terms of age, gender and cultural background. End-users will be recruited through existing networks in the four countries. Facilitators in the co-design process will be trained to ensure a collaborative, equitable partnership throughout all phases.

2.2 Sources for Principles of Ethics in Research with Humans

The SmartCHANGE project involves research with human subjects and will adhere to ethical principles to protect the dignity, rights and welfare of the research participants, including the principles listed in the Declaration of Helsinki, first adopted by the World Medical Association in 1964 and subsequently amended. The Declaration Helsinki, although not legally binding, has served for more than half a century as a foundational ethical framework for medical research involving human participants, addressing principles related to risks, informed consent, including research on identifiable human material and data (WMA, para. 1). While the Declaration of Helsinki is mainly aimed at physicians, it encourages others involved in medical research with human participation to adopt these principles (WMA, para. 2). It includes guiding principles related to risks, burdens, and benefits for human participants in research, vulnerable groups and individuals, informed consent, confidentiality, and research ethics committees.

Other instruments similar to the Declaration of Helsinki are the International Ethical Guidelines for Health-related Research Involving Humans by the Council for International Organizations of Medical Sciences (CIOMS and CIMOS Guidelines, respectively), which set out to provide internationally vetted ethical principles and detailed commentary on how universal ethical principles should be applied.[23] There is also the World Health Organisation's Handbook on good clinical research practice (GCP), that draws from international guidelines and serves as a broad framework for ethical and methodologically sound research on human participants. It is intended to apply to various research studies, not limited to pharmaceutical or medical product research.

Moreover, one needs also to take into account international instruments that assert the necessity to involve children in medical treatment and research decisions affecting them, in a line of ethical principles descending from the UN Convention on the Rights of the Child, where it highlights the right of children to be heard in proceedings directly affecting them (CRC, Article 12). The EU Clinical Trial Directive (2001/20/EC) requires that minors receive information based on their understanding (CTD, Article 4(b)). Different countries set age-specific rules for children's involvement in decisions; for instance, in the Netherlands, children

[23] Council for International Organizations of Medical Sciences ("CIOMS") in collaboration with the World Health Organisation ("WHO"), *International ethical guidelines for health-related research involving humans*, (1982, and most recently amended in 2016) ("CIOMS Guidelines").

as young as 12 can give informed consent for research or treatment alongside their parents.[24] In the US, children as young as 7 may be asked for assent,[25] and in the UK, children under 16 typically require parental consent unless deemed mature under the Gillick ruling (Thornton 2021).

2.3 Principles of ethics in research with humans

Before the start of both the co-design of the SmartCHANGE tools with end-users and the proof-of-principle study, ethical approval will be obtained – in the four countries, including the following principles of ethics in research with humans:

***Principle of voluntariness, informed consent and community agreement*:** According to the Declaration of Helsinki, it is emphasized that, once ensuring that the potential subject comprehends the information, a physician or another suitably qualified individual should then actively seek the potential subject's voluntary and informed consent, preferably in written form (WMA, para. 25). All participants will be fully informed about the research, its associated risks and benefits, and will be informed of the right to abstain from the research or withdraw consent at any time (WMA, para. 26). In case of participants younger than 16 years, informed consent of (one of) their parent(s)/caregiver(s) will be obtained.

***Respect for Vulnerable Individuals*:** Vulnerable individuals are those who, due to various factors such as impaired decisional capacity or challenging circumstances, are relatively or absolutely unable to safeguard their own interests (GCP: 65). When engaging with users, particularly in the context of research or technological developments, special considerations must be given to vulnerable individuals. Vulnerability may arise due to various factors, such as age, cognitive capacity, or socio-economic status (GCP: 27). The Declaration of Helsinki also states that investigations involving individuals who are unable to provide consent due to physical or mental incapacitation should only be conducted when such incapacitation is an essential attribute of the research group (WMA, para. 30).

Right to Withdraw Consent: Users should be made aware of their right to withdraw consent at any time during their engagement without facing adverse consequences. This principle is

[24] https://english.ccmo.nl/investigators/additional-requirements-for-certain-types-of-research/research-with-subjects-under-the-age-of-16-years-children/consent
[25] https://www.cancer.gov/research/participate/clinical-trials/safety

Funded by the European Union

particularly vital in research studies with human participants (WMA, para. 25 and 26; GCP: 67).

Principle of privacy and confidentiality: The identify and records of the participants will as far as possible be kept confidential, to avoid any form of hardship, discrimination or stigmatization as consequence of having participated in the research (WMA, para. 9).

***Principles of accountability and transparency*:** The research will be conducted in a fair, honest, impartial and transparent manner. Data storage and management will adhere to FAIR principles: Findable, Accessible, Interoperable, and Reusable (Wilkinson et al. 2016). If necessary, members of the SmartCHANGE Ethics Board will be consulted in order to fully comply with the data privacy rules.

***Principle of public domain*:** The research findings will be brought in the public domain, through scientific and other publications, following Open Science principles.

2.4 Ethical Artificial Intelligence

While at present it is not yet known when the proposed AI Act will be adopted and what clear implications it will have for the SmartCHANGE project,[26] compliance with existing non-legally binding frameworks, such as the *Ethics guidelines for trustworthy AI* (ETHG) and the *EU guidelines on ethics in artificial intelligence: Context and implementation* (Madiega 2019), can enhance the project's level of adherence to ethical principles. The Artificial Intelligence (AI) to be used to develop the decision-support tools in this project does not pose any risk to constrain the exercise of participants, beneficiaries and stakeholders' human rights, deceive or manipulate, violate bodily or mental integrity, reduce safety, or create addiction. It will not cause social or political disadvantage or result in discrimination nor physical or psychological suffering, financial harm, or significantly damage social processes and institutions. It will comply with the principles of data minimisation and privacy and only use pseudonymised data, while respecting the principles of lawfulness, transparency and fairness of data processing at all times. There will be also rigorous checks as to the quality, integrity and security of data throughout the AI system's life cycle by maintaining a data management and analysis plan. A key objective will be also the avoidance of bias in both input data and algorithm design, in order to prevent potential discrimination, stigmatisation or any other adverse effects on the individual.

[26] See discussion in 3.1

The primary concern regarding any AI application is the requirement of explainability and its notorious "black box" nature, which results in a lack of transparency and accessibility, consequently eroding trust (Kiseleva 2019). AI algorithms stem from deep learning processes, that require very large quantities of data and inherently make the results difficult to explain at least at the human level.[27] As a consequence, a reduction in effective human oversight and comprehension may lead to consequences in relation to decision-making. The GDPR, however, mandates transparency in processing personal data contingent on automated decision-making. The GDPR necessitates the provision of meaningful information to individuals concerning the rationale behind automated decision-making, as well as the significance and repercussions of these determinations. These rights seek to address the transparency concerns associated with AI applications, mitigating issues arising from AI's autonomy and black-box features (ETHG: 16). To attain this objective, the Expert Group asserts that AI must adopt a human-centric approach and be committed to serving the common good and humanity, with the goal of enhancing human well-being and freedom (ETHG: 5). Within the Guidelines, three pivotal components of trustworthy AI are delineated (ETHG: 5):

Lawful: Complying with all pertinent laws and regulations.

Ethical: Ensuring adherence to ethical principles and values.

Robust: Addressing both technical and social aspects, recognizing that, even with good intentions, AI systems can inadvertently cause harm.

Moreover, the Guidelines stipulate that trustworthy AI should uphold the following four principles (ETHG: 12):

Respect for Human Autonomy: AI systems should empower individuals to maintain full self-determination and active participation in the democratic process, refraining from unjustifiably subordinating, coercing, deceiving, manipulating, conditioning, or herding humans. Their design should focus on augmenting and enhancing human cognitive, social, and cultural abilities.

Prevention of Harm: AI systems must neither inflict nor exacerbate harm or negatively impact human beings. AI systems and environments must prioritize safety and security, ensuring

[27] Vincent Ginis & Andres Algaba (Data Analytics Laboratory, VUB), presentation for the Health and Aging Law Laboratory (VUB), 18 October 2023.

technical robustness while safeguarding against malicious usage. Special attention should be given to vulnerable individuals when applying AI systems.

Fairness: The development, deployment, and utilization of AI systems must adhere to principles of fairness.

Explicability: The processes should be transparent, the capabilities and purpose of AI systems openly communicated, and decisions, to the greatest extent possible, made understandable to those directly and indirectly affected.

Furthermore, it is important to note that AI, or artificial intelligence, is broadly defined as a technology encompassing various elements, including machine learning techniques for data analysis, robotics for programmable machines, and automated decision-making systems predicting human and machine behaviour (Madiega 2019).

2.4.1 Ethics in research with children

In the context of research involving children, ethics plays a pivotal role, and this is especially true when considering the use of AI-driven decision support tools.

Informed Consent: The principle of informed consent is a cornerstone of ethical research. For children, this involves not only obtaining their consent but also considering their evolving capacity to understand the research and its potential consequences. Researchers must provide information in a child-friendly and age-appropriate manner, involving parents or guardians as necessary. Striking the right balance between respecting the child's autonomy and ensuring their protection is crucial.

Privacy and Confidentiality: Given the sensitive nature of health-related research, ensuring the privacy and confidentiality of children's data is paramount. There is a risk that participating children could face stigmatization related to health conditions such as obesity or low physical fitness. To mitigate this risk, data should be anonymized and protected to prevent any unintended disclosure of personal information. Robust data security measures should be in place.

Vulnerable Populations: Children, by their nature, may be considered a vulnerable population. Their limited decision-making capacity, combined with potential disparities in access to resources, emphasizes the need for enhanced safeguards and ethical considerations. Vulnerability can be further exacerbated in cases where children belong to underserved or marginalized groups.

2.5 The Necessity to Balance between Fundamental Rights and Vital Interests of Different Groups of People

In the SmartCHANGE project, the ethical imperative is to strike a delicate balance between the fundamental rights and vital interests of different groups of people. The fundamental rights of individuals, including privacy, autonomy, and non-discrimination, are of paramount importance and will be upheld throughout the project. These rights encompass the ability to make informed choices, safeguard personal data, and be free from any form of harm or discrimination.

However, it is also crucial to recognize the vital interests at stake, especially in the context of public health and the prevention of non-communicable diseases. The project aims to address long-term risks associated with non-communicable diseases, particularly in children and youth. Balancing these interests necessitates careful ethical consideration, ensuring that while upholding individual rights, the collective interest in improving public health is not compromised. This requires ongoing ethical deliberation and a commitment to finding solutions that benefit both the individual and society.

Balancing Fundamental Rights and Vital Interests: Balancing fundamental rights and vital interests of different groups, particularly children, in healthcare research is a complex task.

Children's Rights: Research on children's health behaviours must adhere to the principles of the UN Convention on the Rights of the Child, emphasizing children's rights to be heard and have a say in matters affecting them. This participation can empower children and encourage them to actively engage in their own health management.

Potential Stigmatization: The risk of stigmatization cannot be ignored, especially in the context of behaviours related to obesity or low physical fitness. To mitigate this risk, the focus should be on empowering children and promoting self-esteem and self-efficacy rather than stigmatizing or labelling. Weight stigma is pervasive, harmful, and counterproductive in addressing obesity, causing negative behaviours and quality of life. To combat this issue, healthcare professionals should adopt nonbiased practices, empower patients through empathetic counselling, advocate for training in weight stigma awareness, and engage families in addressing weight stigma at home and in school (Pont et. al. 2017).

Funded by
the European Union

Equity and Inclusivity: It is essential to ensure that research involving children is equitable and inclusive, addressing disparities that may exist in healthcare access. The research should aim to benefit all children, irrespective of their background, and focus on reducing health inequalities.

In summary, conducting research on/with children involves a delicate balance between their fundamental rights, protection against stigmatization, and the potential benefits of AI-driven behaviour change interventions. Ethical considerations, safeguards, and careful design of AI systems can help ensure that research aligns with the best interests of the children involved and contributes positively to their well-being.

2.6 New Technologies: Acceptance by Society and Trust

Ensuring the acceptance of new technologies by society and fostering trust in these innovations is integral to the SmartCHANGE project's success. In a rapidly evolving technological landscape, it is essential to address societal concerns and instil trust in the tools and solutions developed.

In the process of co-designing the SmartCHANGE tools, particular attention will be given to understanding the trustworthy, explainable AI predictions and models. This understanding is cultivated through active engagement and discussions with end-users, including healthcare practitioners, families, children, and youth. By involving these stakeholders in the design and development phases, the project aims to build user-centric solutions that resonate with the needs and expectations of the community.

Funded by
the European Union

3 Upcoming legislation

3.1 Artificial Intelligence Act

3.1.1 Introduction

In April 2021 the European Commission introduced the AI Act (AIA), a proposal aimed at regulating Artificial Intelligence and that is approaching, at the time of writing this benchmark, the end of its legislative process, as representatives of the European Parliament, the Council and the Commission are engaged in a trilogue to finalise a compromise leading to the adoption of the regulation by the end of 2023. This section focuses on the proposal as presented by the Commission in 2021, while a brief summary of the different positions between the European Parliament and the Council on the AIA, as emerged during the first reading by the former, will appear at the end of this section. A more in-depth analysis of the final AI Act – if adopted by the end of 2023 – and of its relevance for the SmartCHANGE project will feature in deliverable D2.3 at month 9 of the project life cycle (February 2024). A proposal for an AI Liability Directive, aiming at protection from damages caused by AI systems has been presented in 2022, and has, at the time of writing this benchmark, not yet reached the European Parliament.[28]

The AI Act at a glance

- **Title I General provisions**: Outlines the scope of the regulation and defines the key terms.
- **Title II Prohibited AI practices**: Defines AI practices that violate fundamental rights and are therefore considered as having an unacceptable level of risk.
- **Title III High-risk AI systems**: Lists the specific requirements for AI systems categorised as high-risk based on their intended purpose.
- **Title IV Transparency obligations for providers and users of certain AI systems**: Outlines transparency obligations for systems that 1) interact with humans, 2) detect emotions or determine social categories based on biometric data, or 3) generate or manipulate multimedia content.
- **Title V Measures in support of innovation**: Introduces measures to favour innovation (e.g. “Regulatory Sandboxes”).
- **Title VI Governance**: Establishment of the European AI Board.

[28] COM (2022) 496: 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), available at https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52022PC0496 .

- **Title VII EU Database for high-risk AI**: establishes a database for high-risk AI systems.
- **Title VIII Post-market monitoring, information sharing and market surveillance**: Sets out reporting and monitoring obligations for AI system providers.
- **Title IX Codes of Conduct**: Provides a framework encouraging the voluntary applications of the high-risk system requirements to non-high-risk AI systems.
- **Title X-XII Final Provisions**: Establishes rules for delegation, implementation, and maintenance powers.

3.1.2 Scope

The AIA aims at establishing harmonised rules for the market placement and deployment of AI systems within the European Union, prohibiting certain AI practices considered as having unacceptable levels of risk, while placing specific requirements and prohibitions for AI systems considered as having a high level of risk, while also aiming at standardizing transparency rules for certain types of AI systems (AIA, Article 1). In general, the proposed regulation covers various aspects of AI, including AI systems that interact with individuals, e.g. emotion recognition and biometric categorization, AI systems used to generate or manipulate multimedia content, such as images, videos, and audio. The regulation applies to various stakeholders involved in the development, deployment and use of AI systems within the European Union, including AI system providers regardless of whether they are based in the Union or not, provided that the systems are placed on the market or used within the EU, and including AI system users within the EU and providers and users located in a third country when the output of the system is utilized in the EU (AIA, Article 2(1)).

The AIA does not apply to AI systems developed or used exclusively for military purposes (AIA, Article 2(3)) nor to "AI systems, including their output, specifically developed and put into service for the sole purpose of scientific research and development" (AIA, Article 2(6)) nor to "any research and development activity regarding AI systems" (AIA, Article 2(7)).

3.1.3 Definitions

Article 3 of the AIA provides a list of relevant terms used in the text of the regulation. Table 5 below shows a selection from the 47 definitions of the Article:

Table 5: Selection of definitions from AIA, Article 3

Article 3	Term	Definition
(1)	Artificial intelligence	a system that is designed to operate with elements of autonomy and that, based on machine and/or human-

	system (AI system)	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
(1b)	General purpose AI system	an AI system that - irrespective of how it is placed on the market or put into service, including as open source software - is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems
(2)	Provider	a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed and places that system on the market or puts it into service under its own name or trademark, whether for payment or free of charge
(4)	User	any natural or legal person, including a public authority, agency or other body, under whose authority the system is used
(12)	Intended purpose	the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation
(13)	Reasonably foreseeable misuse	the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems
(29)	Training data	data used for training an AI system through fitting its learnable parameters
(30)	Validation data	data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent

		overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split
(31)	Testing data	data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service
(32)	Input data	data provided to or directly acquired by an AI system on the basis of which the system produces an output
(44)	Serious incident	any incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) the death of a person or serious damage to a person's health; (b) a serious and irreversible disruption of the management and operation of critical infrastructure; (c) breach of obligations under Union law intended to protect fundamental rights; (d) serious damage to property or the environment

3.1.4 Prohibited Artificial Intelligence Practices

The AIA lists four kind of AI practices creating an unacceptable risk vis-à-vis fundamental rights and freedoms, namely (AIA, Article 5):

1) systems using subliminal techniques, i.e. the use of AI systems to manipulate individuals through hidden or subliminal messages, which can have a significant impact on their behaviour or decision-making without their awareness.

2) systems taking advantage of vulnerabilities, i.e. the use of AI systems to exploit vulnerabilities in individuals or systems, e.g. security vulnerabilities or psychological ones, for malicious purposes.

Funded by the European Union

3) systems used for social scoring, i.e. assigning individuals scores or ratings based on their behaviour, preferences, or social interactions, as this would lead to discrimination or infringement on individuals' rights.

4) real-time, remote biometric identification systems, used to identify individuals on the basis of biometric characteristics (e.g. facial recognition) in real-time, as such practice infringes on privacy rights.

The safeguard of fundamental freedoms and rights, such as privacy, is at the basis of the prohibition of the above listed practices. For item no. 4, however, the original proposal of the regulation allows exceptions for law enforcement agencies in case of emergencies (i.e. to identify missing children, terrorists about to carry out an attack, etc.). This exception has been at the centre, as shall be seen in the final part of this section, of disputes between the European Parliament and the Council.

3.1.5 High-Risk AI Systems

The high-risk AI systems identified by the AIA (AIA, Article 6) can be divided into two categories:

1. Systems that are product of a harmonisation legislation listed in the Annex II of AIA, if required to undergo a third-party conformity assessment based on the legislation mentioned in the annex: said systems, broadly speaking, relates to the following areas: civil aviation, two or three-wheeled vehicles or quads, agricultural and forestry vehicles, marine equipment, rail systems, motor vehicles and trailers and unmanned aircraft.
2. Systems listed in the Annex III of the AIA, i.e. systems intended to be used in the following areas:
    a) Biometric ID
    b) Management and operation of critical infrastructure
    c) Educational and vocational training assessment
    d) Employment/worker assessment and access to self-employment
    e) Access/enjoyment of essential public or private services
    f) Law enforcement risk-assessment (i.e. pre-crime, deep fakes, profiling, etc.)
    g) Migration, asylum and border control
    h) Administration of justice (e.g. “robotic judge”)

The list of criteria or system provided in the original proposal of the AIA is not to be considered final, as Article 7 of the regulation gives the power to the European Commission to amend the Annex 3:

> *"The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:*
> *(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;*
>
> *(b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III."* (AIA, Article 7(1))

In other words, AI system not yet developed, produced or even conceived at the present might end on the Annex III if the criteria described in article 7 apply.

Systems that fall under the scope of Title III of the AIA, i.e. high-risk AI systems, are subjected to numerous requirements, described from Articles 8 to 51, related to: risk management system (Article 9), data and data governance (Article 10), technical documentation (Article 11), record keeping (Article 12), human oversight (Article 14), obligations for providers (Article 16), quality management systems (Article 17), obligations for users (29), harmonised standards (Article 40), conformity assessment (Article 43), etc. At this stage of the analysis, and of the legislative process, an AI-tool such as the one described in the SmartCHANGE project does not seem to fall under the scope of high-risk AI system, though a final assessment can only be made after the adoption of the final version of AIA.

Article 52 lists transparency obligations for providers and users of certain systems, namely systems that are (our emphasis):

- "intended to **interact with natural persons**", where the obligation for providers is to inform natural persons "that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use" (AIA, Article 52(1));
- used for **biometric recognition**, where the obligation for users is to inform natural persons exposed to the operation of the system (AIA, Article 52(2));
- used for **emotion recognition**, where the obligation for users is also to inform natural persons exposed to the operation of the system (AIA, Article 52(3);

Funded by the European Union

- used to **generate or manipulate "image, audio or video content** that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake')", where users must disclose that the content has been artificially generated or manipulated (AIA, Article 52(4)).

Exceptions to the obligations of Article 52 are granted for systems "which are permitted by law to detect, prevent and investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties." (AIA, Article 52). While the systems described in Article 52 do not necessarily fall under the scope of Title III, i.e. high-risk systems, for those that do compliance with Article 52 does not imply an exemption from the requirements listed from Article 8 to 51. The nature of the interaction between the AI-tool developed in the SmartCHANGE and natural persons will need to be analysed and understood better to ascertain whether or not the SmartCHANGE AI falls under Article 52 of the AIA.

3.1.6 Non-high-risk systems

Providers of systems that do not fall under the scope of Title III, i.e. high-risk AI systems, can nevertheless submit to requirements of Title III on a voluntary basis by adhering to codes of conduct:

> "*The Commission, and the Member States shall facilitate the drawing up of codes of conduct intended to encourage the voluntary application to AI systems other than high-risk AI systems of one or more of the requirements set out in Title III, Chapter 2 of this Regulation to the best extent possible, taking into account the available, technical solutions allowing for the application of such requirements.*" (AIA, Article 69(1))

3.1.7 Legislative process update

In June 2023, the European Parliament adopted an amended version of the AIA, following the adoption of the Benifei-Tudorache report by the Civil liberties, justice and home affairs (LIBE) and Internal market (IMCO) committees of the Parliament. The amended version adopted in June represents the Parliament's negotiating position, upon which the Council, the Parliament and the Commission, engaged in a trilogue, need to reach a compromise for the Act to be adopted before the end of 2023.

From the beginning of the debates in the Parliament's committees, one of the most contentious issue was the exception for law enforcement with regard to the use of real-time, remote biometric identification systems, i.e. one of the AI systems otherwise prohibited in

Funded by the European Union

the regulation proposal. The Parliament considers this exception as infringing fundamental rights and freedoms and is inclined to accept only ex-post (i.e. non real-time) use of the system only for serious crime and only with the pre-approval of a magistrate.[29]

Another issue at the centre of the debate is the role of large language models and foundation models in general, i.e. a sub-set of General Purpose AI that did not have any special mention in the original Act, but attracted the attention and alarm of the media and the public after the launch of ChatGPT3 at the end of 2022 and of ChatGPT4 in February 2023. As of October 2023, the Spanish Presidency of the EU is proposing two new categories of foundation models: i) 'very capable foundation models' and ii) 'general-purpose AI systems used at scale'.[30]

Other differences of position between the Parliament and the Council relate to fundamental rights, specifically the need for fundamental rights impact assessments for high-risk AI, to workplace decision-making, and sustainability, particularly for AI systems controlling critical infrastructures.[31]

3.2 European Health Data Space

3.2.1 Introduction

The Commission's first in-depth proposal for a data space relates to the European Health Data Space, within the larger context of the EU's Data Strategy, that includes already the Data Governance Act and the proposed Data Act (currently awaiting the Parliament's first reading position). The European Health Data Space regulation proposal is designed to improve and complement existing EU regulations, such as the General Data Protection Regulation (GDPR), the Medical Device Regulation (MDR) and the In Vitro Diagnostics Regulation (IVDR). In contrast to these regulations, however, the EHDS is focused solely on the healthcare industry.

At the time of writing this benchmark, the EHDS proposal has not completed yet its legislative process and is awaiting the decision by the Civil liberties, justice and home affairs (LIBE) and Environment, public health and food safety (ENVI) committees before the plenary of the Parliament can proceed to adopt its negotiating position vis-à-vis the Council. Political

[29] Luca Bertuzzi, Euractiv.com, "MEPs seal the deal on Artificial Intelligence Act", 27 April 2023, available at https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/
[30] "The EU AI Act Newsletter #38", 6 October 2023, at https://artificialintelligenceact.substack.com/p/the-eu-ai-act-newsletter-38
[31] Ibid.

commentators raise either in relation to the approval of the regulation proposal in the 2019-2024 or to its entry into force, with the Commission hoping for a 2025 launch, the Council a 2035 one and the Parliament looking at a launch on the three-year horizon.[32]

It is difficult, therefore, to judge if the SmartCHANGE project will be really impacted by the proposed legislation in the course of its lifetime, unless, of course, the regulation will be approved by the end of the current legislature despite the most pessimistic forecasts.

The EHDS at a glance

- **Chapter 1: General provisions:** scope and definitions
- **Chapter 2: Primary use of electronic health data:** lays out rights of natural persons, access by health professionals, rules for European Electronic Health Record (EHR), Digital Health Authority, the cross-border infrastructure for primary use.
- **Chapter 3: Electronic health record (EHR) systems and wellness apps:** Interplay of EHR systems with medical devices and AI systems, rule for placement on the market, obligations for economic operators, conformity of EHR systems, market surveillance, interoperability, voluntary labels and registration of wellness applications.
- **Chapter 4: Secondary use of electronic health data:** lays out purposes for which EHR data can be processed, prohibited uses, governance and related mechanisms, rules for data permits, cross-border access and infrastructure, data quality and utility label, EU dataset catalogue.
- **Chapter 5: Additional actions:** measures for capacity building and rules for transfer to third countries.
- **Chapter 6: European governance and coordination:** establishment and task of the EHDS Board.
- **Chapter 7: Delegation and Committee:** delegation and committee rules
- **Chapter 8: Miscellaneous:** lays out penalties, rules for evaluation and review
- **Chapter 9: Deferred application and final provisions,** including entry into force.

3.2.2 Scope

The EHDS regulation proposal is conceived as an extension and improvement of the GDPR in the health sector. The proposal is organised around two main pillars: i) primary use of health

[32] Giedre Peseckyte, Euractiv.com. "EU Parliament solving riddle of secondary use of data in health data space", 3 July 2023 at: https://www.euractiv.com/section/health-consumers/news/eu-parliament-solving-riddle-of-secondary-use-of-data-in-health-data-space/

data and ii) secondary use of health data. In the first pillar, the rules about the primary use is about health data involve data subjects rights, rules for access by health professionals, data portability (in the sense defined by Article 20 of the GDPR), while seeking to facilitate the re-use of health data by consumers, portability between health service providers in support of second opinions, and increased competition between service providers.[33] The proposal introduces a series of rules for the primary use of health data, such as the design and development of electronic health registers, the interoperability of electronic health record systems across the EU, and wellness application rules.

The second pillar establishes the legal framework for the secondary use of health data in the EU. The secondary use of electronic health data is linked to a variety of themes and purposes, including notions of scientific research in the traditional sense (EHDS, Article 34(1)(e)) as well as its application to the innovation of new products or services related to "public health or social security or ensuring high levels of quality and safety of health care, or medical products or devices." (EHDS, Article 34 (1)(f)). Other permitted areas include public health threats (EHDS, Article 34 (1)(a)), improving healthcare delivery and related services, and education and training-related activities (EHDS, Article 34 (1)(d)).

In sum, the EHDS proposal has multiple ambitions, as it aims to i) strengthen patient control over their data, ii) establish rules for electronic health records (EHR) systems to promote reliability, security and interoperability, iii) establish rules for secondary use of health data, and iv) establish mandatory cross-border infrastructures. For a project such as SmartCHANGE it seems safe to assume that the real interest for the EHDS leans toward the second pillar, i.e. secondary use of health data, although the first pillar would also present an interesting possibility, if the EHDS were to be adopted by the end of 2023 and enter in force soon after, as the concept of 'wellness application' is introduced:

> "*'wellness application' means any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than healthcare, such as well-being and pursuing healthy life-styles;*" (EHDS, Article 2(2)(o))

Recalling the discussion in section 1.3.9 above, about the requirements for a SmartCHANGE tool considered as a medical device even within the context of a research project, it would be interesting to explore a possible path for SmartCHANGE as a wellness application instead of

[33] See also Marcus et. al. 2022.

Funded by the European Union

a medical device, at least in relation to the difference in terms of regulatory burdens between the two approaches.

3.2.2.1 Secondary use of health data

The EHDS promotes the secondary use of electronic health data for research, innovation, public health, policy-making, and regulatory purposes, maintaining a high level of legal protection because of its sensitivity under Article 9 of the GDPR. Secondary uses include using individual-level health data or aggregated datasets to support research, innovation, policy-making, regulatory activities, etc. For example, the secondary use of electronic health data can promote scientific research, inform evidence-based policymaking, or improve the efficiency of healthcare systems across populations through better allocation of resources (Terzis 2022: 3). Besides, sharing health data among institutions and databases can validate whether research finding is institution-specific or can lead to generalisable outcomes (McLennan et. el. 2022).

The proposed regulation supports aggregating health data and making them available for secondary use purposes in health care. As stated in Recital 38 of the proposal, "much of the existing health-related data is not made available for purposes other than that for which they were collected [...] In order to fully unleash the benefits of the secondary use of electronic health data, all data holders should contribute to this effort in making different categories of electronic health data they are holding available for secondary use" (EHDS, Recital 38). As a result, the proposal encourages fifteen data categories available for secondary use (EHDS, Article 33(1)). It will allow for more extensive national and union-wide health data aggregation. It will provide new insights into the performance of health products, services, and service providers that would not be possible with analysis based on fragmented datasets. As a result, the secondary use of health data will facilitate innovation in health services and create more transparent service markets in the EU, thereby stimulating competition (EHDS, Article 34(1)(f)).

A further goal of the EHDS proposal is to facilitate the innovation of products and services relating to health care or social security (EHDS, Article 34(1)(f)). Such activities are increasingly data-hungry and as a result secondary health data is often highly sought after. This is for example particularly true in the design and manufacture of medical devices. It is also the case for the design and surveillance of medicinal products, meaning that secondary health date, e.g. from EHRs is in particular demand.

Access to electronic health data (as defined in the EHDS) (e.g., from patient EHRs) will accordingly likely be granted for designing, testing and for follow-up studies on the performance of medical devices.

Furthermore, the EHDS proposal foresees a more specific possibility for providing electronic health data for purposes related to the training, testing and evaluating of algorithms (EHDS, Article 34(1)). This is clearly linked to the provision of electronic health data for the production of products used in health care, including most notably medical devices, to which, as seen section 1.3, software applications belong as well (MDR, Article 2(4)). As the training, testing and evaluation of algorithms used in such devices require large amounts of data, the ability to obtain large data sets for secondary use can be crucial for developers. It may also be essential for obtaining and maintaining (given that such devices must be monitored when placed on the market) regulatory approval.

In sum, it is far from clear whether or not this legislative proposal will affect the SmartCHANGE proposal, in light of its uncertain legislative process at the time of writing, though deliverable D2.3 will provide a last update and attempt a final assessment of the relevance of the EHDS for the project.

Funded by
the European Union

4 References

4.1 Legislation, Treaties, Case law and opinions

AIA: 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:52021PC0206

CHARTER: Charter of the Fundamental Rights of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

CJEU, C-582/14, *Breyer v. Bundesrepublik Deutschland*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582

CONVENTION 108 (1981): Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/1680078b37

CRC: United Nations, 1989. Convention on the Rights of the Child. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

CTD: Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use. ("Clinical Trials Directive"). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:121:0034:0044:en:PDF

CTR: 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0536

ECHR: European Convention on Human Rights. https://www.echr.coe.int/documents/d/echr/Convention_ENG

EHDS: 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

ETHG: European Commission, 2019. *Ethics guidelines for trustworthy AI*. Prepared by the High-Level Group on AI set up by the European Commission, as of 8th of April 2019.

https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai accessed on 22 October 2023

FINDPA 2018: Data Protection Act (1050/2018; amendments up to 239/2023 included). Translation from Finnish. Legally binding only in Finnish and Swedish. Ministry of Justice, Finland. https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf

GDPR: 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

MDR: Regulation on medical devices 2017/745 of the European Parliament and of the Council of April 2017, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745&qid=1697462381286

MEDDEV 2.7/1 (2016): European Commission. DG Internal Market, Industry, Entrepreneurship and SMEs Consumer, Environmental and Health Technologies Health technology and Cosmetics. *Guidelines on medical devices. Clinical evaluation: A GUIDE FOR MANUFACTURERS AND NOTIFIED BODIES UNDER DIRECTIVES 93/42/EEC and 90/385/EEC 6.2. MEDDEV 2.7/1.* Revision 4. June 2016. Art.6.2. [*Guidelines on clinical evaluation*] https://www.medical-device-regulation.eu/wp-content/uploads/2019/05/2_7_1_rev4_en.pdf accessed October 18 2023

MODERNISED CONVENTION 108 (2018): Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data – Consolidated text. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

NLGDPRIA 2018: General Data Protection Regulation Implementation Act, 16 May 2018, The Netherlands. Unofficial translation available at: https://www.dataguidance.com/sites/default/files/dutch_general_general_data_protection_regulation_implemention_act.pdf accessed October 19 2023

STATUTE COE: Statute of the Council of Europe. https://treaties.un.org/doc/Publication/UNTS/Volume%2087/volume-87-I-1168-English.pdf accessed on 10 October 2023

TFEU: Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European

Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT

UDHR: Universal Declaration of Human Rights. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

WMA: World Medical Association, 1964. 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/

WP29 2007: Article 29 Working Party, 2007. *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf accessed October 12 2023

WP29 2010: Article 29 Data Protection Working Party, 2010. *Opinion 1/2010 on the concepts of "controller" and "processor"*. 00264/10/EN WP 169.

WP29 2011: Article 29 Data Protection Working Party *Opinion 15/2011 on the notion of consent.* Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf accessed on October 14 2023

WP29 2014: Article 29 Data Protection Working Party. *Opinion 05/2014 on anonymisation techniques*. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf accessed on October 14 2023

WP29 2016: Article 29 Data Protection Working Party, 2016. *Guidelines on the right to data portability*, WP 242, 13 December 2016 and revised on 5 April 2017, Available at https://ec.europa.eu/newsroom/article29/items/611233 accessed on October 16 2023

WP29 2017: Article 29 Data Protection Working Party. *Opinion 2/2017 on data processing at work*. Available at https://ec.europa.eu/newsroom/article29/items/610169/en accessed on October 14 2023

WP29 2017a: Article 29 Data Protection Working Party, 2017. *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*. 17/EN WP 248 rev.01. ["DPIA

Guidelines"] Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. Available at: https://ec.europa.eu/newsroom/article29/items/611236/en accessed 19 October 2023

4.2 Bibliography

CANE, PETER & CONAGHAN, JOANNE (eds.), 2008. *The New Oxford Companion to Law*. Oxford, Oxford University Press.

FEIRABEND, LISA & QUINN, PAUL, 2020. TeNDER (EU funded project). D1.1 *Fundamental Rights, Ethical and Legal Implications and Assessment*.

FRA/COE: European Union Agency for Fundamental Rights and Council of Europe, 2018. *Handbook on European data protection law*. Luxembourg, Publications Office of the European Union.

HARTLEY, T. C., 2014. *The Foundations of European Union Law.* Oxford, Oxford University Press.

GADOTTI, ANDREA, HOUSSIAOU, FLORIMOND, ANNAMALAI, MEENATCHI, DE MONTJOYE, YVES-ALEKANDRE, 2023. "Pool Inference Attacks on Local Differential Privacy: Quantifying the Privacy Guarantees of Apple's Count Mean Sketch in Practice" Preprint available at: https://www.researchgate.net/publication/370058817_Pool_Inference_Attacks_on_Local_Differential_Privacy_Quantifying_the_Privacy_Guarantees_of_Apple's_Count_Mean_Sketch_in_Practice accessed 16 October 2023

GCP: World Health Organisation, 2005. *Handbook for good clinical research practice: guidance for implementation.* https://iris.who.int/handle/10665/43392

KISELEVA, A., 2019. "Decisions made by AI versus transparency: Who wins in Healthcare?" In T. C. Bächle & A. Wernick (Eds.), *The futures of eHealth. Social, Ethical and legal challenges*. Berlin, Germany: Humboldt Institute for Internet and Society.

KLOZA D., VAN DIJK, NIELS, GELLERT, R., BÖRÖCZ I., TANAS A., MANTOVANI E., QUINN P., 2017. "Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals." in *d.pia.lab Policy Brief* No. 1/2017

KOKOTT, J., SOBOTTA, C., 2013. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" in *International Data Privacy Law*, Vol. 3, No. 4, p. 222-228

LI, TIANCHENG, LI NINGHUI, 2009. “On the Tradeoff between Privacy and Utility in Data Publishing”. Conference paper available at: https://www.cs.purdue.edu/homes/ninghui/papers/privacy_utility_kdd09.pdf accessed 15 October 2023

MADIEGA, TAMBIANA ANDRÉ, 2019. *EU guidelines on ethics in artificial intelligence: Context and implementation*. European Parliament Think Tank. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2019)640163 accessed on 22 October 2023

MARCUS, J. SCOTT, MARTENS, BERTIN, CARUGATI, CHRISTOPHE, BUCHER, ANNE, GODLOVITCH, ILSA, 2022. *The European Health Data Space*. Publication for the committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

MCLENNAN, S., RACHUT, S., LANGE, J., FISKE, A., HECKMANN, D., BUYX, A., 2022. "Practices and attitudes of bavarian stakeholders regarding the secondary use of health data for research purposes during the COVID-19 pandemic: qualitative interview study." *Journal of Medical Internet Research* 24.6 (2022): e38754. available at https://www.jmir.org/2022/6/e38754/

PONT, STEPHEN J., PUHL, REBECCA, COOK, STEPHEN R., SLUSSER, WENDELIN, 2017. “Stigma Experienced by Children and Adolescents With Obesity” in *Pediatrics* (2017) 140 (6): e20173034. https://doi.org/10.1542/peds.2017-3034

QUINN, PAUL, 2021. “Research under the GDPR – a level playing field for public and private sector research?” in *Life Sciences Society and Policy* 17(1), March 2021.

QUINN, PAUL & MALGIERI, GIANCLAUDIO, 2021. “The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework” in *German Law Journal* 22(8):1583-1612, December 2021.

RODA, S., BÖRÖCZ, I., 2019. HR-Recycler (EU funded project). D2.1 *Report on security, data protection, privacy, ethics and social acceptance*.

SOLOVE, DANIEL J., 2008. *Understanding privacy*. Cambridge Massachusetts, Harvard University Press.

TAMBA, EMMA, 2017. *The Relationship Between the EU Charter and the ECHR in the EU and the EEA*. Master thesis. The Arctic University of Norway.

TERZIS, PETROS, 2022. "Compromises and Asymmetries in the European Health Data Space." In: *European Journal of Health Law* 1.

THORNTON, JACQUI, 2021. "Court upholds Gillick competence in puberty blockers case." in *The Lancet*, World report, volume 398, issue 10307, p. 1205-1206, October 02 2021. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)02136-X/fulltext accessed 24 October 2023

WARREN, SAMUEL D. & BRANDEIS, LOUIS D., 1890. "The Right to Privacy" in *Harvard Law Review*, Vol. 4, No. 5, p. 193-220

WILKINSON, M. D. ET AL., 2016. "The FAIR Guiding Principles for scientific data management and stewardship." In nature.com/scientific data. https://www.nature.com/articles/sdata201618

YAO, CONG & QUINN, PAUL, 2023. SUN (EU funded project). D7.3 *Ethics and the GDPR*.

Funded by the European Union