Project Acronym:	HosmartAI
Grant Agreement number:	101016834 (H2020-DT-2020-1 – Innovation Action)
Project Full Title:	Hospital Smart development based on AI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016834

DELIVERABLE

D8.1 – SELP Benchmark Report

Dissemination level:	PU -Public
Type of deliverable:	R -Report
Contractual date of delivery:	31 May 2021
Deliverable leader:	VUB
Status - version, date:	Final – v1.0, 2021-05-31
Keywords:	Social, Ethical and Legal Issues, SELP, Fundamental Rights, Patients' Rights, Right to Privacy, Data Protection, Medical Ethics, Informed Consent, AI, Robotics, Medical Devices Regulation

Executive Summary

The main goal of the HosmartAI Project ("Project") is to build up an effective and efficient health care system transformation by using AI and robotic technologies. To this end, the Project will introduce "an AI platform that will allow for core facilities to be shared and linked composing smart services for healthcare professionals, patients, information system managers, and health organisation administrations"[1].

A number of regulatory and ethical frameworks would be relevant to the Project:

- Most fundamentally, various legal framework on **fundamental rights/human rights** will be relevant because the Project engages human participants.
- Patients' rights under the **EU Patients' Rights Directive** will be relevant because HosmartAI will take place in a medical context and the human participants are patients in this regard.
- Various legal framework on data protection/privacy law, namely the **GDPR**, including regulation on **profiling**, and the data protection laws at national level will be most relevant because: (1) the development, deployment, and use of AI platform in the Project will entail processing of personal data, including **special categories of personal data**; and (2) at least some of the healthcare tasks mentioned in the Proposal (e.g., Screening of high-risk patients and frail adults including pregnant women and seniors and recommend preventive measures; Computer-aided diagnosis systems; Personalized rehabilitation and precise treatment) involves technologies that fall within the definition of profiling.
- As the Project anticipates tech start-ups/SMEs/healthcare entities joining the HosmartAI platform, the concept of data controller and processor, and identifying which entity is data controller/processor, will be central.
- Various ethical and social issues will be implicated because the use of AI will lead to various concerns or risks that are not yet legally regulated as of now.
- From the technological perspective, these ethical/social concerns or risks include: obscurity and "**black box effect**," **discrimination**, **unfairness**. They are relevant because: (1) the Proposal exactly mentions "**Explainable AI frameworks**", and (2) some healthcare tasks (e.g., Screening of high-risk patients and frail adults including pregnant women and seniors and recommend preventive measures; Computer-aided diagnosis systems; Personalized rehabilitation and precise treatment) may be susceptible to these concerns.
- From the medical perspective, they include difficulties in obtaining **informed consent** because the settings of the Project would take place in tertiary hospitals and care or rehabilitation centre as some patients may not be able to provide valid consent due to incapacity.
- Finally, the **EU Medical Devices Regulation** is relevant because **physical services**, including robotics, may fall within the jurisdiction of the EU Medical Devices

[1] HosmartAI Grant Agreement, Annex 1 (Part B), Section 1.1.2.

Regulation. Some of the **digital services** mentioned in the Proposal may also be subject to the Medical Devices Regulation because software can also fall within the definition of "medical device."

Deliverable leader:	Paul Quinn (VUB)
Contributors:	Hideyuki MATSUMI (VUB)
Reviewers:	Arton Lipaj (UKCM), Marianna Fotiadou (AHEPA)
Approved by:	Athanasios Poulakidas, Irene Diamantopoulou (INTRA)

Document History			
Version	**Date**	**Contributor(s)**	**Description**
0.1	2021-04-22	Hideyuki MATSUMI	Initial complete draft
0.2	2021-05-10	Hideyuki MATSUMI	Updated complete draft for internal peer review
0.3	2021-05-23	Hideyuki MATSUMI	Pre-final version addressing review comments
1.0	2021-05-31	A. Poulakidas, I. Diamantopoulou	Final version for submission

Table of Contents

Table of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym/ Abbreviation	Title
AI HLEG	High-Level Expert Group on Artificial Intelligence
CFR	Charter of Fundamental Rights of the European Union
CIOMS and CIOMS Guidelines	The International Ethical Guidelines for Health-Related Research Involving Humans by the Council for International Organizations of Medical Sciences
ECHR	European Convention on Human Rights
EC	European Commission
EU	European Union
ICCPR	International Covenant on Civil and Political Rights
ICH and ICH GCP	The Guideline for Good Clinical Practice by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use
IDPA	Italian Data Protection Act
MDR	EU Medical Devices Regulation
PRD	EU Patients' Rights Directive
UDHR	Universal Declaration of Human Rights
WHO GCP	WHO's Handbook for Good Clinical Research Practice

1 Introduction

1.1 Project Information

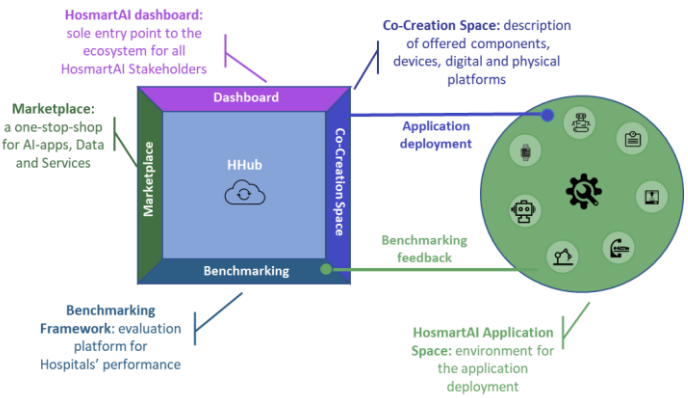
VISION

The HosmartAI vision is a strong, efficient, sustainable and resilient European **Healthcare system** benefiting from the capacities to generate impact of the technology European Stakeholders (SMEs, Research centres, Digital Hubs and Universities).

MISSION

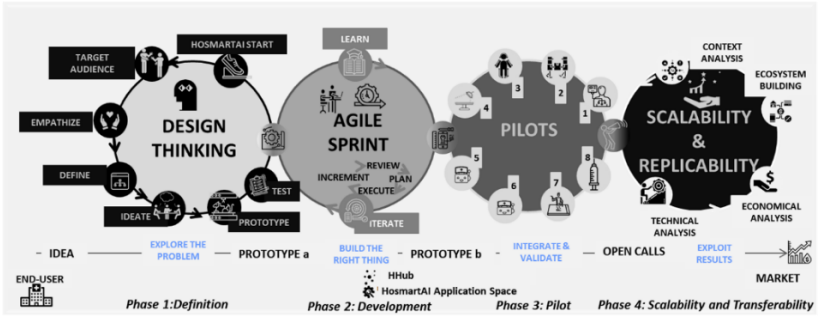
The HosmartAI mission is to guarantee the **integration** of Digital and Robot technologies in new Healthcare environments and the possibility to analyse their benefits by providing an **environment** where digital health care tool providers will be able to design and develop AI solutions as well as a space for the instantiation and deployment of a AI solutions.

HosmartAI will create a common open Integration **Platform** with the necessary tools to facilitate and measure the benefits of integrating digital technologies (robotics and AI) in the healthcare system.



A central **hub** will offer multifaceted lasting functionalities (Marketplace, Co-creation space, Benchmarking) to healthcare stakeholders, combined with a collection of methods, tools and solutions to integrate and deploy AI-enabled solutions. The **Benchmarking** tool will promote the adoption in new settings, while enabling a meeting place for technology providers and end-users.

Eight Large-Scale Pilots will implement and evaluate improvements in medical diagnosis, surgical interventions, prevention and treatment of diseases, and support for rehabilitation and long-term care in several Hospital and care settings. The project will target different **medical** aspects or manifestations such as Cancer (Pilot #1, #2 and #8); Gastrointestinal (GI) disorders (Pilot #1); Cardiovascular diseases (Pilot #1, #4, #5 and #7); Thoracic Disorders (Pilot #5); Neurological diseases (Pilot #3); Elderly Care and Neuropsychological Rehabilitation (Pilot #6); Fetal Growth Restriction (FGR) and Prematurity (Pilot #1).



To ensure a user-centred approach, harmonization in the process (e.g. regarding ethical aspects, standardization, and robustness both from a technical and social and healthcare perspective), the **living lab** methodology will be employed. HosmartAI will identify the appropriate instruments (**KPI**) that measure efficiency without undermining access or quality of care. Liaison and co-operation activities with relevant stakeholders and **open calls** will enable ecosystem building and industrial clustering.

HosmartAI brings together a **consortium** of leading organizations (3 large enterprises, 8 SMEs, 5 hospitals, 4 universities, 2 research centres and 2 associations – see Table 1) along with several more committed organizations (Letters of Support provided).

Table 1: The HosmartAI consortium.

Number[2]	Name	Short name
1 (CO)	INTRASOFT INTERNATIONAL SA	**INTRA**
1.1 (TP)	INTRASOFT INTERNATIONAL SA	**INTRA-LU**
2	PHILIPS MEDICAL SYSTEMS NEDERLAND BV	**PHILIPS**
3	VIMAR SPA	**VIMAR**
4	GREEN COMMUNICATIONS SAS	**GC**
5	TELEMATIC MEDICAL APPLICATIONS EMPORIA KAI ANAPTIXI PROIONTON TILIATRIKIS MONOPROSOPIKI ETAIRIA PERIORISMENIS EYTHINIS	**TMA**
6	ECLEXYS SAGL	**EXYS**
7	F6S NETWORK IRELAND LIMITED	**F6S**
7.1 (TP)	F6S NETWORK LIMITED	**F6S-UK**
8	PHARMECONS EASY ACCESS LTD	**PhE**
9	TERAGLOBUS LATVIA SIA	**TGLV**
10	NINETY ONE GMBH	**91**
11	EIT HEALTH GERMANY GMBH	**EIT**
12	UNIVERZITETNI KLINICNI CENTER MARIBOR	**UKCM**
13	SAN CAMILLO IRCCS SRL	**IRCCS**
14	SERVICIO MADRILENO DE SALUD	**SERMAS**
14.1 (TP)	FUNDACION PARA LA INVESTIGACION BIOMEDICA DEL HOSPITAL UNIVERSITARIO LA PAZ	**FIBHULP**
15	CENTRE HOSPITALIER UNIVERSITAIRE DE LIEGE	**CHUL**
16	PANEPISTIMIAKO GENIKO NOSOKOMEIO THESSALONIKIS AXEPA	**AHEPA**
17	VRIJE UNIVERSITEIT BRUSSEL	**VUB**
18	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	**AUTH**
19	EIDGENOESSISCHE TECHNISCHE HOCHSCHULE ZUERICH	**ETHZ**
20	UNIVERZA V MARIBORU	**UM**

[2] CO: Coordinator. TP: linked third party.

Number[2]	Name	Short name
21	INSTITUTO TECNOLÓGICO DE CASTILLA Y LEON	**ITCL**
22	FUNDACION INTRAS	**INTRAS**
23	ASSOCIATION EUROPEAN FEDERATION FORMEDICAL INFORMATICS	**EFMI**
24	FEDERATION EUROPEENNE DES HOPITAUX ET DES SOINS DE SANTE	**HOPE**

1.2 Document Scope

WP8 "Social, Ethical and Legal Issues (SELP)" is responsible for assessing the impact in terms of social ethical and legal compliance, including issues related to fundamental rights, data protection, and privacy of the methods proposed in the context of the HosmartAI ("Project"). This document, entitled D8.1 SELP Benchmark Report, summarises the main findings of T8.1, which focuses on identifying the key ethical and legal requirements that are likely to be applicable to the Project.

This D8.1 "SELP Benchmark Report" will be followed by the following reports: Building upon this document, D8.2 SELP "Compliance Report" will describe (a) the development of the appropriate SELP framework for measurements of the applicable ethical and social principles, and (b) how HosmartAI complies to those measurements. D8.3 "SELP Impact Assessment" which is planned to be issued approximately one year after the launch of the Project, will document the SELP requirements and how they will be implemented in practice. Specifically, it aims to report the results of the liaison with the technical task leaders to ensure that the outcomes create the most positive impacts for the Project. Finally, D8.4 "SELP Continuous Monitoring Report 1" and D8.5 "SELP Continuous Monitoring Report 2" will document SELP issues raised during the Project.

1.3 Document Structure

This document is comprised of the following chapters:

Chapter 1 presents an introduction to the project and the document.

Chapter 2 presents a brief description of HosmartAI Project that is relevant in the context of Social, Ethical and Legal Issues (SELP).

Chapter 3 and **4** address the legal issues and relevant framework. **Chapter 3** touches upon the fundamental rights and patients' rights of human participants in the Project. First it provides a survey of legal instruments relevant to fundamental/human rights. Then it clarifies the various rights of patients in the EU. **Chapter 4** lays out the regulatory framework on the Right to Privacy and Data Protection. This Chapter is separated from **Chapter 3** because legal issues concerning data protection relevant to the Project are extensive and the number of pages is large.

Section 5 discusses ethical and social issues. While all issues covered in this Report are ethical, legal, and social in nature, they can be categorized into issues that are addressed by legally

binding instruments and issues that are not (e.g., addressed by non-legally binding framework issued authorities).

Finally, **Chapter 6** provides a survey on Medical Device Regulation. This Chapter is placed at the end of the Report because the subject matter is primarily on devices while **Chapter 3** to **5** are about humans[3].

[3] Chapters 3 to 6 will rely on experiences and knowledge gained by the VUB through the involvement in the PROTEIN, FASTER, and TENDER projects, all funded under Horizon 2020.

2 Brief description of the Project relevant in the context of SELP

2.1 Overview

The objective of HosmartAI project ("Project") is "to promote an effective and efficient health care system transformation, by the use of AI technological developments and robotics" [4]. To achieve this, the Project will "introduce an AI platform that will allow for core facilities to be shared and linked composing smart services for healthcare professionals, patients, information system managers, and health organisation administrations" [5]. HosmartAI will be tested in eight (8) pilots integrated within existing health and care facilities such as six hospitals and one care facility in five countries, and the Pilots will focus on applying AI and robotics to a range of functions[6].

Table 2: Applying AI and Robotics to range of functions.

Range of functions	#1	#2	#3	#4	#5	#6	#7	#8
Screening and prevention						+		
Diagnosis, treatment and surgical support	+		+	+	+		+	+
Organisational aspects and logistics in hospitals		+						

The Project will target the following medical aspects or manifestations.

Table 3: Targeting medical aspects or manifestations.

Medical aspects or manifestations	#1	#2	#3	#4	#5	#6	#7	#8
Cancer	+	+						+
Gastrointestinal (GI) disorders	+							
Cardiovascular diseases	+			+	+		+	
Thoracic Disorders					+			
Neurological diseases			+					
Elderly Care and neuropsychological rehabilitation						+		
Fetal growth restriction (FGR) and prematurity	+							

In Phase 2, the pilots will collect data of the procedure delivered by humans[7]. In Phase 3 (Validation phase), the prototype systems of the 8 Pilots will be used in the real environments, and the tests are planned to be performed in the following countries: Greece (Pilot 1-AHEPA),

[4] HosmartAI Grant Agreement, Annex 1 (Part B), Section 1.1.2 [hereinafter *HosmartAI*].
[5] *Id.*
[6] HosmartAI, Section 1.3.1.
[7] *Id.*

Belgium (Pilot 2-CHUL), Italy (Pilot 3-IRCCS), Spain (Pilot 4-SERMAS), Slovenia (Pilot 5-UKCM), Spain (Pilot 6-INTRAS), Belgium (Pilot 7-Philips) and Belgium (Pilot 8-VUB)[8].

Relevance to Social, Ethical, and Legal Issues.

While there is no unique and definite definition of "AI", it is one of the most discussed topics in the context of SELP. As of today, there is no overarching law regulating AI technology. However, a number of institutions have issued various documents addressing social, ethical, or legal issues of the technology. Importantly, the EC has issued its Proposal for a Regulation laying down harmonised rules on artificial intelligence ("Proposal for the AI Act") very recently. Once put into force, it is likely to have significant impact on the Project.

Applying AI and robotics to a range of medical functions, such as screening and preventing or diagnosis, treatment and surgical support, may trigger various provisions of the General Data Protection Regulation ("GDPR"), including provisions concerning profiling. The Project targets various medical aspects or manifestations, such as cancer, neurological diseases, fetal growth restriction (FGR) and prematurity. These will entail processing of genetic, biometric or health data, and will trigger rules concerning processing of special categories of personal data under the GDPR.

2.2 Human Participants

The Project will engage "numerous stakeholders, including patients and vulnerable groups of citizens like pregnant women and older adults, healthcare professionals like clinicians, nursing staff and occupational therapists and administrative staff including healthcare managers" [9]. In addition to the fact that HosmartAI aims to deliver pilots across the EU in five (5) countries in six (6) healthcare organizations (namely, UKCM, IRCCS, SERMAS, CHUL, AHEPA and INTRAS), they will take place in multiple healthcare settings[10].

Table 4: Multiple healthcare settings

Healthcare settings	#1	#2	#3	#4	#5	#6	#7	#8
Tertiary hospitals	+	+		+	+		+	+
Primary care settings	+							
Care or rehabilitation centre			+			+		

It is estimated that "[m]ore than 3000 patients and vulnerable citizens, 300 healthcare professionals and 600 stakeholders including administrative stuff will be included in different piloting activities." Furthermore, [a]n additional number of 200 patients, 50 healthcare professionals and 3 additional healthcare organizations are expected to be approached in the realm of the Open Calls."

[8] HosmartAI, page 25 of 70.
[9] *Id.*, page 7 of 70.
[10] *Id.*, page 7 of 70.

To ensure an increase of the Project outreach, it will define "a programme of two Open Calls (OCs) that will directly finance start-ups & SMEs as well as healthcare entities to join HosmartAI" [11]. Consequently, tech start-ups/SMEs/healthcare entities applying for the OCs and joining the Project are not consortium partners initially foreseen.

Sex and gender analysis will be carried out as part of the analysis of epidemiological and socio-economic data of each HosmartAI pilot because of "the interrelations between sex-related biological differences and socio-economic and cultural factors that affect the behaviour of women and men and their access to health services" [12].

Relevance to Social, Ethical, and Legal Issues

Because many human individuals from different countries and/or socioeconomic status will participate in the Project, various legal and ethical frameworks on fundamental/human rights will be relevant. Moreover, the EU Patients' Rights Directive will be relevant because the Project will take place in a medical context and the human participants are patients in this regard.

The Project will take place in multiple healthcare settings, including care or rehabilitation centre. In such a medical setting, some patients may not be competent to provide valid consent necessary to participate in the Project.

As the Project anticipates tech startups/SMEs/healthcare entities joining the HosmartAI platform, the concept of data controller and processor, and identifying which entity is data controller/processor, will be central.

2.3 Technologies Involved

The Project engages various cutting-edge technologies. The project aims to integrate and offer two categories of services: (1) **physical** and (2) **digital** services[13]. The **physical services** include: Embodied conversational agents for better care delivery and patient experience, remote health and rehabilitation monitoring systems based on IoT and wearables, care assistant robots, autonomous surgical navigation systems. The **digital services** include: explainable computer-aided diagnosis systems, digital twins capable of delivering real-time simulations and decision-making during surgeries or scheduling of operations within the hospital, patient digital phenotyping towards the delivery of personalized and more precise treatments in oncological and high-risk cardiovascular patients, fusion of different omics data[14] for faster and more accurate decision making of the HCP[15].

[11] HosmartAI, page 26 of 70.
[12] HosmartAI, page 27 of 70.
[13] HosmartAI, page 6 of 70.
[14] They include genomics profile DNA, transcriptomics measure transcripts; proteomics and metabolomics quantify proteins and metabolites. Ana Conesa & Stephan Beck, Making multi-omics data accessible to researchers, 6 Scientific Data 251 (2019), 10/gjqwxt (last visited Apr 19, 2021). See also Omics data – RD-Connect, https://rd-connect.eu/what-we-do/omics/ (last visited Apr 19, 2021).
[15] Health care professionals.

More specifically, the HosmartAI platform will integrate a multitude of AI and robotics technologies through the eight (8) Pilot use cases[16].

Table 5: AI and robotics technologies.

AI and robotics technologies	#1	#2	#3	#4	#5	#6	#7	#8
Explainable AI frameworks	+							
Deep learning, reinforcement learning techniques and convolutional neural network architectures	+	+		+	+			
Patient clustering	+			+				
Natural language processing		+		+	+	+		
(Embodied) conversational robots/agents		+			+	+		
Robotics and sensor-based rehabilitation devices			+			+		
Remote surgical navigation systems				+			+	

Both the physical and digital services will be applied in a wide spectrum of healthcare tasks[17].

Table 6: Healthcare tasks.

Healthcare tasks	#1	#2	#3	#4	#5	#6	#7	#8
Screening of high-risk patients and frail adults including pregnant women and seniors and recommend preventive measures	+					+		
Computer-aided diagnosis systems	+							+
Personalized rehabilitation and precise treatment			+					+
Surgical support based on computer modelling and digital twins				+			+	
Provision of assistive care					+	+		
Optimization of hospital resource utilization		+						

The Project will adopt "advanced technologies, such as AI, Robotics, autonomous systems, Big Data, Decision Support, Benchmarking, etc" to take the initiative "to lead the Digital Transformation of the European Healthcare sector" [18].

[16] HosmartAI, at 6 of 70.
[17] *Id.*
[18] HosmartAI, page 10 of 70.

Relevance to Social, Ethical, and Legal Issues

Because the Project aims to offer both physical and digital services, the EU Medical Devices Regulation is likely applicable as they may fall within the definition of "medical device" (including software).

The physical and digital services applied in various healthcare tasks, such as screening high-risk patients and frail adults, computer-aided diagnosis systems, and personalized rehabilitation and precise treatment, may implicate the profiling regulations under the GDPR.

The Project explicitly mentions "Explainable AI frameworks." In SELP context, many institutions and experts raise concern that AI often cannot provide rationale or explanation as to how and why it reached a particular output. To address these concerns, there are a number of documents or guidelines applicable or helpful to the Project, such as "Ethics guidelines for trustworthy AI" drafted by High Level Expert Group on Artificial Intelligence, which will be touched on in detail in Section 5.4.2 "Note on Explanainability".

3 Fundamental Rights and Patient's Right

3.1 Introduction

The Project engages "numerous stakeholders, including patients and vulnerable groups of citizens like pregnant women and older adults, healthcare professionals like clinicians, nursing staff and occupational therapists and administrative staff including healthcare managers" [19]. It aims to deliver pilots across the EU in five (5) countries in six (6) healthcare organizations, and the pilots will take place in three (3) healthcare settings[20]. The Project estimates "[m]ore than 3000 patients and vulnerable citizens, 300 healthcare professionals and 600 stakeholders including administrative stuff will be included in different piloting activities."

Under given facts, various instruments of fundamental rights will be pertinent to the Project. Moreover, the patients participating in the Project are entitled to rights and protections conferred by the Directive 2011/24/EU on patients' rights in cross-border healthcare ("Patients' Rights Directive" or "PRD"). The Report will touch upon the perspective of fundamental rights/human rights in the next Section and touches on the aspect of patients' rights in the Section following it.

3.2 Fundamental Rights

3.2.1 Universal Declaration of Human Rights ("UDHR")

The United Nations General Assembly ("UN GA") proclaimed the Universal Declaration of Human Rights ("UDHR") as "a common standard of achievement for all peoples and nations" [21]. For the first time, it set out the fundamental human rights "to be universally protected" [22]. With the inclusion of Article 12, the UDHR became the first international instrument that set out an "individual's right to the protection of their private sphere against intrusion from others, especially from the state" [23].

Notwithstanding its non-binding character, the UDHR is a widely recognised human rights instrument and serves as a foundation and influence for subsequent national, European and international instruments[24].

While a number of articles are potentially relevant to the Project, the right to privacy enshrined in Article 12 of the UDHR, is most relevant:

[19] HosmartAI, page 7 of 70.
[20] *Id.*, page 7 of 70.
[21] Preamble of the UDHR.
[22] United Nations, *The Universal Declaration of Human Rights*, https://www.un.org/en/universal-declaration-human-rights/.
[23] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, 2018 edition ("Handbook on DP Law"), see https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en, p. 21. See also FASTER, p. 11.
[24] Handbook on DP Law, p. 21.

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.

3.2.2 European Convention on Human Rights ("ECHR")

In the similar period as UDHR was adopted, the Council of Europe was established "to bring together the states of Europe to promote the rule of law, democracy, human rights and social development" [25]. It includes 47 members, 28 of which are members of the European Union[26].

As part of its efforts, the Council adopted the ECHR in 1950. All Council member states have signed the ECHR[27]. With its adoption, the ECHR was the first instrument "to give effect to certain of the rights stated in the Universal Declaration of Human Rights and make them binding" [28]. Contracting Parties have the obligation to ensure the protection of the rights and freedoms set out in the ECHR[29]. All Member States of the Council of Europe have now "incorporated or given effect to the ECHR in their national law" [30]. In 1959, the European Court of Human Rights ("ECtHR") was established in Strasbourg "[t]o ensure that the Contracting Parties observe their obligations under the ECHR" [31].

Article 8 of the ECHR provides for the right to respect for private and family life, home and correspondence. Though a fundamental right, it is not absolute as the second paragraph of Article 8 suggests under which circumstances the right may be limited, namely if such interference is i) in accordance with the law, ii) necessary in a democratic society, and iii) pursuing legitimate and important public interests[32]. The "exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information" [33]. When different rights are at stake, an attempt must be made to strike a balance between them[34].

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

[25] *Id.*, p. 22.
[26] Council of Europe, *Who we are*, see https://www.coe.int/en/web/about-us/who-we-are.
[27] *Ibid.*
[28] European Court of Human Rights, *European Convention on Human Rights*, see https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.
[29] Article 1, ECHR.
[30] Handbook on DP Law, p. 23.
[31] *Ibid.*
[32] Article 8(2), ECHR. See also HR-RECYCLER, p. 12; See also FASTER, p. 11.
[33] Handbook on DP Law, p. 24.
[34] *Ibid.* See also HR-RECYCLER, p. 12.

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.

Article 14 of the ECHR, which "enshrines the protection against discrimination in the enjoyment of the rights set forth in the Convention," can be also relevant because biased data and use of AI can inflict and/or reinforce discrimination[35]. The ECtHR has found Article 14 applicable to many areas, including: employment, membership of a trade union, social security, education, right to respect for home, access to justice, access to children, paternity, freedom of expression, assemble and association, and the like[36]. The ECtHR has confirmed that the scope of Article 14 and its Protocol includes "discrimination based on disability, medical conditions or genetic features" [37].

Article 14 of the ECHR – Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in [the] Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

3.2.3 Charter of Fundamental Rights of the European Union ("CFR")

Because the rights of individuals in the EU were established in different instruments at different times, the EU decided to adopt one document that included them all[38]. Accordingly, the EU adopted the Charter of Fundamental Rights of the European Union ("CFR") on 9 December 2000, though the document only became legally binding with the entry into force of the Lisbon Treaty in 2009[39].

The language of Article 7 of the CFR is almost identical to that of Article 8 of the ECHR. Once difference, whereby 'correspondence' has been replaced by 'communications', was introduced to take stock of technological developments[40]. In addition to their similarity, Article 52(3) of the CFR specifically provides that in the event the CFR contains rights that are also laid down in the ECHR, "the meaning and scope of those rights shall be the same as those laid down by the said Convention".

Article 7 of the CFR - Respect for private and family life

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

---

[35] 1. ECtHR, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention (2020), https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.
[36] *Id.*
[37] Id., page 37 (referring to *Glor v. Switzerland*, 2009, § 80; *G.N. and Others v. Italy*, 2009, § 126; *Kiyutin v. Russia*, 2011, § 57).
[38] European Commission, *Why do we need the Charter*, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_nl.
[39] *Ibid*.
[40] See HR-RECYCLER, pp. 12, 13.

Article 52(1) of the CFR sets out the conditions under which the right may be limited, namely if i) it is provided for in law, ii) respects the essence of those rights and freedoms, iii) it is proportional and necessary, and iv) it meets the objective of general interests recognised by the Union or the need to protect the rights and freedoms of others. Similar to the ECHR, where different rights and freedoms are at stake, a balance will need to be sought.

> ***Article 52 of the CFR - 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.*

It should be noted that the provisions of the CFR are directed at "the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law" [41]. Therefore, the CFR provides a basis for EU legislation, including the GDPR[42].

While some fundamental rights are considered absolute, some fundamental rights are not absolute. The right to respect for private and family life under both the ECHR and the CFR is one that is not considered as an absolute right. One of the implications of this is, a balancing between different fundamental rights will be required or allowed under particular situations.

3.3 Patients' rights in the European Union

The HosmartAI project engages patients. Their status as a patient grants them certain rights set forth under the Directive 2011/24/EU on patients' rights in cross-border healthcare ("Patients' Rights Directive" or "PRD")[43]. Much of the PRD provides a practical framework for implications of cross-border healthcare, such as reimbursement of costs and the relevant administrative procedures. Most importantly in the context of HosmartAI, however, the PRD requires healthcare providers to provide relevant information to help patients make informed choices[44]. In turn, service providers, including ICT based provider, should ensure that they

[41] Article 51(1), CFR.
[42] FASTER, p. 12.
[43] EU Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare ("EU Patients' Rights Directive"), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF.
[44] Article 4(2)(d), EU Patients' Rights Directive.

provide clear information regarding the availability, safety and quality of healthcare, the prices, the insurance cover and other protective measures regarding professional liability[45].

The PRD further recognises the obligation that Member States shall ensure the protection of "the fundamental right to privacy with respect to the processing of personal data is protected in conformity with national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC" [46] (which the former has been repealed and replaced by the General Data Protection Regulation ("GDPR")[47], and the latter is known as the ePrivacy Directive). The rights include the patient's right to access and portability of their personal data, such as being entitled to a copy of their medical file, as is provided for in the EU Patients' Rights Directive[48].

The PRD spells out some requirements concerning eHealth[49]. Article 14 of the PRD requires the EU to "support and facilitate cooperation and the exchange of information among the Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States." This "volunteer network" aims to "connect national authorities responsible for eHealth" [50] and provides an opportunity for EU countries to "give direction to eHealth developments in Europe by playing an important role in strategic e-Health related decision-making on interoperability and standardisation" [51]. The network has, for example, under its Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU[52] and related Patient summary guideline[53], developed "the minimum set of information needed to assure Health Care Coordination and the continuity of care."

3.4 Relevance to HosmartAI and SELP

In the context of HosmartAI and SELP, there are three relevant and important in terms of fundamental rights/patients' rights. First, various activities conducted as part of the Project, including applying AI and robotic technologies still at research process or collecting

[45] *Ibid*. See also PROTEIN, p. 12.
[46] Article 4(2)(e), EU Patients' Rights Directive. See also EU Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("EU Directive 95/46/EC"), see https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.
[47] EU Regulation 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) ("GDPR"), see https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[48] Article 4(2)(f), EU Patients' Rights Directive.
[49] Article 14(1), EU Patients' Rights Directive. See also PROTEIN, pp. 12, 13.
[50] See https://ec.europa.eu/health/ehealth/cooperation_en.
[51] *Ibid*.
[52] eHealth Network, *Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU (General Guidelines)*, 21 November 2016, see https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co092_en.pdf.
[53] eHealth Network, *Patient Summary Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU (Patient Summary for unscheduled care)*, 21 November 2016, see https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf.

personal/health data using monitoring devices, have the potential of "violating" fundamental rights of the participants. Second, however, these activities may be justified and are not considered a "violation" if, *inter alia*, complies with the fundamental legal principles. The fundamental legal principles most relevant in this context are the principle of necessity and the principle of proportionality. In short, the necessity principle requires that an activity interfering with the fundamental rights of the participants is strictly necessary to achieve the objective of the Project. The proportionality principle requires that an activity interfering with the fundamental rights is proportionate to achieve the objective of the Project. Any activities conducted in the Project should pass both musters (i.e., necessity test and the proportionality test) not to violate the fundamental rights of the participants.

Third, the Project must comply with the Patients' Rights Directive. Most relevant in this context is to provide patients with relevant information so that they can make informed choices. This information includes whether a particular activity (e.g., collection of a particular heath date or use of a particular device) is one that is necessary for regular medical treatment or is one that is part of the HosmartAI, which a patient can choose not to participate. This is closely related to issues discussed in Chapter 5.3 "Informed Consent".

4 Right to Privacy and Data Protection

4.1 Introduction

The origins of the concept of privacy are traditionally attributed to authors Samuel Warren and Louis Brandeis[54]. The concept was coined in response to the technological developments of that time, such as instantaneous photographs and newspaper enterprises[55], and "the state of American journalism" [56] as the authors complained about the invasion of "the sacred precincts of private and domestic life", the "unauthorised circulation of portraits of private persons" and the "evil invasion of privacy by the newspapers" [57]. In light of these developments, Warren and Brandeis called for the right to privacy, or the right to be left alone[58]. While it has been more than a century since the concept was coined, there is not one, universally accepted definition[59]. How the term is defined often depends greatly on the social, ethical and cultural context[60].

The concept of privacy is enshrined as a legal right in numerous national and international instruments. As touched above, it emerged as a fundamental right in the Universal Declaration of Human Rights ("UDHR") of 1948[61]. The right has also been recognised in the European Convention on Human Rights ("ECHR") of 1950[62]. In 2000, the right was further included in the Charter for Fundamental Rights of the European Union ("CFR")[63].

The right to the protection of personal data is, like the right to privacy, a fundamental right enshrined in a number of instruments[64]. The concept of data protection stems from the right to privacy. Both are "instrumental in preserving and promoting fundamental values and

---

[54] S. D. Warren & L. D. Brandeis, *The Right to Privacy*, Harvard Law Review Vol. 4, No. 5, 1890, p 193-220 ("Warren & Brandeis"). See also P. de Hert & S. Gutwirth, *Privacy data protection and law enforcement. Opacity of the individual and transparency of power*, in Privacy and the Criminal Law, E. Claes *et al.* (eds), 2006 ("De Hert & Gurwirth"), p. 61.

[55] Warren & Brandeis, p. 195. See also FASTER, p. 9; S. Roda, I. Böröcz, Ioulia Konstantinou (VUB), HR-RECYCLER, D2.1 Report on Security, data protection, privacy, ethics and societal acceptance, 7 June 2019 ("HR-RECYCLER"), p. 10.

[56] De Hert & Gurwirth, p. 61.

[57] Warren & Brandeis, p. 195.

[58] *Ibid*.

[59] E.g., D. J. Solove, *Understanding Privacy*, Cambridge Massachusetts: Harvard University Press, 2008 ("Solove") *Privacy: A concept in disarray* (Chapter 1), p. 1; R. C. Post, *Three Concepts of Privacy*, Faculty Scholarship Series (Paper 185), 2001, see https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers.

[60] FASTER, p. 10; HR-RECYCLER, p. 10.

[61] United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948 ("UDHR"), see https://www.un.org/en/universal-declaration-human-rights/, Article 12.

[62] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms,* 4 November 1950 ("ECHR"), see https://www.echr.coe.int/Documents/Convention_ENG.pdf, Article 8.

[63] European Parliament, Council and Commission, *Charter on Fundamental Rights of the European Union*, 7 December 2000 ("CRF"), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT, Article 7.

[64] Though it is good to note that while privacy is recognised as a universal human right, the right to data protection is not (yet) recognised as such. See European Data Protection Supervisor, *Data Protection*, see https://edps.europa.eu/data-protection/data-protection_en.

rights; and to exercise other rights and freedoms – such as freedom of speech or the right to assembly" [65]. However, they are distinct rights. While the right to privacy "consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases", the right to protection of personal data is generally viewed as a more modern and active right, "putting in place a system of checks and balances to protect individuals whenever their personal data are processed" [66].

4.2 The European data protection framework

At the European level, legal protection of personal data is guaranteed under Article 8 of the ECHR and its related case law, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 ("Convention 108")[67].

Convention 108 was the first legally binding international instrument in the data protection field, for all States ratifying it. All EU Members States have ratified the Convention[68]. The principles contained in the Convention "concern in particular fair and lawful collection and automatic processing of data, storage for specified legitimate purposes and not for use for ends incompatible with these purposes, nor kept for longer than is necessary" as well as the quality of data[69]. In 2018, the Convention was modernised (Convention 108+) to respond to the new challenges of the digital era, the globalisation of processing operations and to allow safer exchanges of personal data[70].

On the European Union level, the protection of personal data is provided under Article 8(1) of the CFR and Article 16(1) of the Treaty on the Functioning of the European Union ("TFEU")[71].

> ***Article 8 of the CFR - 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.*

[65] European Data Protection Supervisor, *Data Protection* (website), https://edps.europa.eu/data-protection/data-protection_en. See also FASTER, p. 13.
[66] Handbook on DP Law, p. 19. See also FASTER, p. 13; HR-RECYCLER, p. 13.
[67] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 108, 28 January 1981 ("Convention 108"), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. See also FASTER, p. 13.
[68] Handbook on DP Law, p. 26.
[69] Council of Europe, *Convention 108 and its Protocols - Background*, https://www.coe.int/en/web/data-protection/convention108/background.
[70] Council of Europe, *Data protection leaflet*, https://rm.coe.int/leaflet-data-protection-final-26-april-2019/1680943556.
[71] EU, *Treaty on the Functioning of the European Union*, 25 March 1957 (and as amended) ("TFEU"), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016ME/TXT.

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

Article 16 of the TFEU

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Article 39 of the TEU

In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Article 16 of the TFEU also creates a new independent legal basis for EU co-legislators (the European Council and the European Parliament) to legislate on data protection matters.

The right to the protection of personal data under the CFR is not absolute. Similar to the right to respect for private and family life under Article 7 CFR, Article 52(1) of the CFR sets out the conditions under which the right may be limited, namely if i) it is provided for in law, ii) respects the essence of those rights and freedoms, iii) it is proportional and necessary, and iv) it meets the objective of general interests recognised by the Union[72] or the need to protect the rights and freedoms of others.

4.3 General Data Protection Regulation (the GDPR) Regulation 2016/679/EU

While the EU constitutional provisions on data protection are specified in its primary law – the CFR and the TFEU – the protection of personal data in the EU relies heavily on secondary legislation: regulations and directives. The most important secondary source is the GDPR. The GDPR finds its legal basis in Article 16 of the TFEU[73] and repeals the Directive 95/46/EC.

[72] Article 3 of the TFEU and Article 23(1) of the GDPR list a series of objectives of general interest.
[73] Preamble of the GDPR ("Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof").

While the GDPR intended to harmonise the rules related to data protection across Europe, it is important to note that the GDPR leaves room for derogations by the Member States in certain areas, including the processing of special categories of personal data, which can be subject to stricter rules in national law[74].

The European Data Protection Supervisor ("EDPS") and the European Data Protection Board ("EDPB") are important in terms of compliance with the GDPR[75]. The EDPS is the EU's independent data protection authority, which, among others, supervises the processing of personal data by EU Institutions and bodies, advises those entities on data protection issues, monitors new technology that might affect data protection[76]. The EDPB was established by the GDPR as "an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities" [77]. The EDPB replaced the Article 29 Data Protection Working Party[78].

4.3.1 Definitions

A number of definitions under the GDPR will be important in the context of HosmartAI.

Table 7: Definitions under the GDPR relevant to HosmartAI

Term	Definition
personal data	any information relating to an identified or identifiable natural person ('data subject')
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
profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
pseudonymisation	the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and

[74] See PROTEIN, p. 19.
[75] See FASTER, p. 13; HR-RECYCLER, p. 16; PROTEIN, p. 19.
[76] EDPS, *About*, https://edps.europa.eu/about-edps_en.
[77] EDPB, *About EDPB*, https://edpb.europa.eu/about-edpb/about-edpb_en.
[78] See also PROTEIN, p. 20.

Term	Definition
	organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
data controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
data processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
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
genetic data	personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
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 person, such as facial images or dactyloscopic data
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
supervisory authority	an independent public authority which is established by a Member State pursuant to Article 51. It is responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data and to facilitate the free flow of personal data within the EU.
sensitive data	Personal data which is, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms. Article 9 of the GDPR prohibits processing of such sensitive data unless exceptions apply. The three categories of sensitive date, namely genetic data, biometric data, and data concerning health, are defined in Article 4, *supra*; the GDPR does not provide definitions for the other five categories, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning a natural person's sex life or sexual orientation[79]. They are interpreted in conjunction with CFR, TFEU, and ECHR[80].

[79] The EU General Data Protection Regulation (GDPR): a commentary, (Christopher Kuner, Lee A. Bygrave, & Christopher Docksey eds., 2019), page 374.
[80] *Id.* See also Article 21(1) CFR, Article 19 TFEU, and Article14 ECHR for racial or ethnic origin; Article 11 CFR and Article 10 ECHR for political opinions; Article 10 CFR and Article 9 ECHR for religious or philosophical beliefs;

Term	Definition
anonymous data	Data does not relate to an identified or identifiable natural person or personal data which rendered anonymous in such a manner that the data subject is not or no longer identifiable. The concept is not defined in the GDPR but is stipulated in Recital 26.
automated individual decision-making	Information which does not relate to an identified or identifiable natural person or personal data which rendered anonymous in such a manner that the data subject is not or no longer identifiable.

4.3.2 The data protection principles

Article 1 of the GDPR sets out its two main objectives, namely i) to protect fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data, and ii) the free movement of personal data within the EU. Article 5 of the GDPR lays out the data protection principles that must be complied with when processing personal data. In other words, any time personal data will be processed (e.g., collected, stored, used, transferred, disclosed, and the like), each and all of these principles must be taken into account.

Table 8: Data protection principles.

Principle (Article)	**Description**
Lawfulness, fairness and transparency (Art. 5(1)(a) GDPR)	Personal data shall be processed lawfully, fairly and in a transparent manner. These requirements should be fulfilled in relation to the data subject. Lawfulness means that personal data should be processed under one of the legal grounds specified in Article 6 of the GDPR. Fair processing governs primarily the relationship between the controller and the data subject[81]. Controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner and must be able to demonstrate the compliance of processing operations with the GDPR. Data subjects should be aware of potential risks[82]. The requirement of transparency establishes an obligation for the controller to take appropriate measures to keep the data subjects informed, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, about how their data are being used[83].
Purpose limitation (Art. 5(1)(b) GDPR)	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is

Article 28 CFR and Article 11 ECHR for trade union membership; Article 7 CFR and Article 8 ECHR, and Article 21(1) CFR for natural person's sex life or sexual orientation.

[81] Handbook on DP Law, p. 118

[82] *Ibid.*

[83] Article 12(1), GDPR. See also Handbook on DP Law, p. 120.

Principle (Article)	**Description**
	incompatible with those purposes. The purpose of processing data must be defined before processing is started[84]. For example, where the original legal basis for the collection and processing of data was consent, the scope for further research is limited to that outlined in the original consent materials unless new consent is obtained.
Data minimisation (Art. 5(1)(c) GDPR)	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Accordingly, collecting data that is not strictly necessary for the realisation of the specified purpose would infringe the data minimisation principle.
Accuracy (Art. 5(1)(d) GDPR)	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 (Art. 5(1)(e) GDPR)	Personal data kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed[85]. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[86].
Integrity and confidentiality (Art. 5(1)(f) GDPR)	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures[87].
Accountability (Art. 5(2) GDPR)	The controller shall be responsible for, and be able to demonstrate compliance with, all the previously mentioned principles. To facilitate such compliance, controllers can i) record the processing activities, making them available to the supervisory authority upon request (Article 30 GDPR); ii) adhere to approved codes of conduct or certification mechanism; iii) designate a Data Protection Officer; iv) undertake a Data Protection Impact Assessment; iv) ensure data protection by design and by default; v) adopt policies and procedures, and implement them, to allow the exercise of the rights of data subjects[88].

[84] Handbook on DP law, p. 122.
[85] *Ibid.*
[86] *Ibid*.
[87] *Ibid*.
[88] See FASTER, p. 18; HR-RECYCLER, p. 19.

4.3.3 Legitimate basis for processing

Pursuant to the principle of lawfulness, all processing of personal data shall be based on one or multiple grounds set out in Article 6(1) of the GDPR:

1. the data subject has given free, voluntary and specific **consent**;
2. **performance of a contract** to which data subject is a party;
3. **compliance** with a **legal obligation** of the controller;
4. **protection the vital interests** of the data subject or of another natural person;
5. activity carried out **in the public interest** or in the **exercise of official authority**;
6. **legitimate interests** pursued by the controller or third party, as long as it is not overridden by fundamental rights and freedoms of the data subject.

It is important to note that while these legal grounds generally apply to all types of personal data, there is an exception when it comes to special categories of personal data under Article 9(1) of the GDPR. For such sensitive data[89], the GDPR sets more stringent requirements for their processing. In fact, the GDPR prohibits the processing of such data, unless one of the grounds set out in Article 9(2) applies, including:

- **Explicit consent (article 9(2)(a) of the GDPR)**: the data subject has given explicit consent to the processing of personal data for one or more specific purposes;
- **Vital interests of the data subject or other person (Article 9(2)(c) of the GDPR)**: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent[90];
- **Processing of data by health care professionals (Article 9(2)(h) of the GDPR)**: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the obligation of professional secrecy;
- **Public interest in the area of public health (Article 9(2)(i) of the GDPR)**: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

[89] Including "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."

[90] Recital 46 of the GDPR further explains that "[p]rocessing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject."

- **Archiving, scientific, historical or statistical purposes (Article 9(2)(j) of the GDPR)**: must 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.

In defining consent, the GDPR sets out its four elements[91]. Valid consent must be:

- **Freely given**: the validity of consent depends on whether "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" [92].
- **Specific**: the GDPR requires that (explicit) consent is given "for one or more specific purposes" [93]. The consent "should refer clearly and precisely to the scope and the consequences of the data processing" and it can therefore not "apply to an open-ended set of processing activities" [94].
- **Informed**: the provision of information "to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent" [95].
- **An unambiguous indication of the data subject's wishes**: "consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration" [96].

It is generally accepted that the GDPR implies that consent should be obtained before the controller commences the processing of personal data for which consent has been given[97]. While consent may be given in writing as well as digitally and orally[98], there rests a duty on the controller to be able to demonstrate that consent for the processing of data has been obtained[99]. Accordingly, documenting consent in writing can provide evidence that consent was indeed obtained.

As explained above, in case of processing sensitive data, explicit consent is required. The term explicit relates to the manner in which consent was expressed by the data subject and means that "the data subject must give an express statement of consent" [100]. Explicit consent may

[91] Article 4(11), GDPR. See also Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, 28 November 2017 (last revised on 1 April 2018) ("Art. 29 Working Party Guidelines"), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030, p. 5.
[92] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011 ("Art. 29 Working Group Opinion 15/2011"), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
[93] See Articles 6(1)(a) and 9(2)(a), GDPR.
[94] Art. 29 Working Group Opinion 15/2011, p. 17.
[95] Art. 29 Working Party Guidelines, p. 13.
[96] Art. 29 Working Party Guidelines, p. 15.
[97] Art. 29 Working Party Guidelines, p. 17.
[98] Art. 29 Working Group Opinion 15/2011, pp. 21, 22.
[99] Recital 42, GDPR.
[100] Art. 29 Working Party Guidelines, p. 18.

be obtained in writing as well as digitally[101] and orally[102]. However, like with consent, the controller has a duty to demonstrate consent was obtained. For that reason, documenting consent in writing holds clear benefits and it is recommended that all pilot-partners in the Project obtain written consent.

Some data subjects might not be in a position, whether due to mental or physical causes, to give informed consent. In such cases, the collection and processing of personal data may not be carried out, unless it is demonstrated that it is for the benefit of the person or poses no harm, and that authorisation has been given by their legal representative or by an authority, person or body provided for by law[103].

4.3.4 The rights of the data subject

The GDPR recognises a number of rights of data subjects, many corresponding with obligations of the data controllers (and processers):

Table 9: Rights of the data subject.

Right (Article)	**Description**
Right to be informed (Art. 12, 13 14 GDPR)	The controller shall take appropriate measures to provide to 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.
Right of access (Art. 15 GDPR)	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information: 1. the purpose of processing; 2. the categories of personal data concerned; 3. the recipients of personal data; 4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; 5. the existence of the right to request from the controller rectification or erasure of personal data; 6. the right to lodge a complaint with a supervisory authority; 7. where the personal data are not collected from the data subject, any available information as to their source;

[101] For instance, by filling in an electronic form, by sending an email or by using an electronic signature, see Art. 29 Working Party Guidelines, p. 18.
[102] Art. 29 Working Party Guidelines, p. 18.
[103] However, individuals who cannot provide valid consent should be excluded from automated decision-making, including profiling, unless there is a substantial public interest as the legal basis. Article 22(4). See also PROTEIN, p. 25.

Right (Article)	**Description**
	8. 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.
Right to rectification (Art. 16 GDPR)	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. 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.
Right to erasure ('right to be forgotten') (Art. 17 GDPR)	The data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay where one of the following applies: 1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; 2. the data subject withdraws consent on which the processing is based and where is no legal grounds of processing; 3. the data subject objects to the processing and there is no other legitimate ground of processing; 4. the personal data have been unlawfully processed; 5. 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; 6. the personal data have been collected in relation to the offer of information society services.
Right to restriction of processing (Art. 18 GDPR)	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: 1. the accuracy of the personal data is contested by the data subject; 2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; 3. 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; 4. 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.
Right to data portability	The data subject shall have the right to receive the personal data concerning them, which they have provided to a controller, in a

Right (Article)	**Description**
(Art. 20 GDPR)	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 (Art. 21 GDPR)	The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them 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 not to be subject to a decision based solely on automated processing, including profiling (Art. 22 GDPR)	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
Right to lodge a complaint with a supervisory authority (Art. 77 GDPR)	Data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to them infringes this Regulation.
Right to an effective judicial remedy against a supervisory authority and to receive compensation (Art. 78, 82 GDPR)	Whenever the data subject considers that their rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR, they have the right to an effective judicial remedy and the right to receive compensation[104].

4.3.5 Role and obligations of the data controller

To comply with the GDPR, the data controller must fulfil its responsibilities in multiple ways. The obligations of the data controller (and processor, *infra*) are laid out in Chapter IV of the GDPR, and this Section will follow its organization.

4.3.5.1 General obligations

Responsibility of the controller (Article 24)

The data controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate compliance with the GDPR when processing personal

[104] See FASTER, p. 23; HR-RECYCLER, p. 23.

data (also pursuant to the accountability principle)[105]. This requires the data controller to implement appropriate data protection policies[106].

Data Protection by design and by default (Article 25)

The GDPR requires that "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection *by design* and data protection *by default*," taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of processing as well as the risk of varying the likelihood and severity or the rights and freedoms of natural persons[107].

The principle of data protection *by design* requires that "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures […] which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects" [108].

The principle of data protection *by default* requires that "the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" [109]. This specifically applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Joint Controllers (Article 26)

The GDPR recognises the concept of joint controllers, where two or more controllers "jointly determine the purposes and means of processing" [110]. The concept of joint controllers is a variant of controller defined under Article 4(7).

Joint controller is relevant in the context of HostmartAI Project because the Pilots will be conducted at multiple sites, by multiple partners, and some of the partners will be jointly involved in determining the purpose and means of processing personal data. They are likely that to be considered as joint controllers. In the event of such joint controllers, it is important that they make arrangements to clearly identify and allocate responsibilities under the GDPR[111].

Record of processing activities (Article 30)

All data controllers shall maintain a record of processing activities under its responsibility, including information about the data controller, the data processor, if any, and the processing

[105] Articles 24(1) and 5(2), GDPR.
[106] Article 24(2), GDPR.
[107] Article 25 and recital 78, GDPR.
[108] Article 25(1), GDPR.
[109] Article 25(2), GDPR.
[110] Article 26, GDPR.
[111] Article 26(1), GDPR. See also Recital 79, GDPR.

operation. While some exceptions may apply to this obligation, including when a controller has less than 250 employees and in cases of processing sensitive data[112], such a register can nevertheless be beneficial to better assess risks and serve as a demonstration of compliance.

4.3.5.2 Security of personal data

Security of processing (Article 32)

Data controllers (and processors, *infra*) must implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risks that are presented by processing, in particular from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Measures should be identified taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of processing as well as the risk of varying the likelihood and severity or the rights and freedoms of natural persons[113].

Technical measures

Technical measures that a data controller may implement could include anonymisation, pseudonymisation and encryption of data. Moreover, this could include the implementation of a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of that processing[114].

It is important to distinguish between anonymisation and pseudonymisation. As set out above in the definitions, pseudonymisation refers to the efforts made that personal data can no longer be attributed to a specific data subject without the use of additional information. This could include removing unique identifiers such as names, dates of birth and social security number[115]. In contrast, anonymisation requires that the data subject is no longer identifiable. To determine whether a person is identifiable, "all the means reasonably likely to be used" for the identification of a person should be taken into account[116]. According to an Opinion of the Article 29 Data Protection Working Party, the 'means reasonably likely to be used'-test is applied to determine whether "identification has become 'reasonably' impossible" [117]. To establish whether means are reasonably likely to be used to identify a person, consideration should be given to factors including "the costs of and the amount of time required for identification […] the available technology at the time of the processing and technological developments" [118].

---

[112] Article 30(5), GDPR.
[113] Article 32(1), GDPR.
[114] See Article 32(1), GDPR.
[115] See P. Quinn, P. de Hert (VUB), PICASSO, D3.5 Privacy Compliance Laws Associated with Surveillance, 22 December 2017 ("Picasso"), p. 26.
[116] Recital 26, GDPR.
[117] Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014 ("Opinion 05/2014 on Anonymisation") https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm, p. 8.
[118] Recital 26, GDPR.

Accordingly, there is a considerably high standard for anonymisation[119]. Pseudonymisation is not a method of anonymisation, but rather only "reduces the linkability of a dataset with the original identity of a data subject" [120]. As pseudonymisation therefore continues to allow for identifiability of the data subject, it stays inside the scope of the GDPR[121], unlike truly anonymised data which falls outside of the scope of the GDPR[122].

Data breach notification (Articles 33 and 34)

If a data breach occurs, the data controller must, without undue delay and preferably not later than 72 hours after having become aware of the breach, notify the relevant supervisory authority. In an event the notification is not made within 72 hours, it should be accompanied by reasons for the delay. No notification is required in case the breach is not likely to result in a risk to the rights and freedoms of natural persons. The controller must document such personal data breaches, including the relevant facts, their effects and the remedy taken.

If the breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the occurrence thereof to the affected data subject without delay.

4.3.5.3 Data protection impact assessment and prior consultation

Data protection impact assessment (Article 35)

The GDPR provides that "[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, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data" [123] (emphasis added).

Article 35(3) of the GDPR provides a number of situations of where a DPIA is required:

1. a systematic, 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;
2. processing on a large scale of sensitive data or of personal data relating to criminal convictions;
3. a systematic monitoring of a publicly accessible area on a large scale.

In determining whether processing is likely to result in a high risk, the GDPR offers some examples where there is the potential for a higher risk to rights and freedoms:

- where personal data are processed which reveal data concerning health;

[119] PICASSO, p. 26.
[120] Opinion 05/2014 on Anonymisation, p. 3.
[121] *Id*., p. 10.
[122] Recital 26, GDPR.
[123] Article 35(1), GDPR.

- where personal data are evaluated, in particular analysing or predicting aspects concerning health;
- where personal data of vulnerable persons are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects[124];
- where processing operations include new technologies[125].

The more of these elements are present, the more likely it is that processing presents a high risk to the rights and freedoms of natural persons, thereby warranting a DPIA[126]. Even where it is unclear whether a DPIA is to be conducted, it might be advisable that a DPIA is carried out nevertheless as "a DPIA is a useful tool to help controllers comply with data protection law" [127].

According to the GDPR, a DPIA may address a single data processing operation or, it may address a set of similar processing operations that present similar high risks[128].

Article 35(7) of the GDPR provides that a DPIA should, at least, contain the following elements:

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

Stakeholder consultations (Article 35(9))

This provision requires that "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."

Cooperation and consultation with supervisory authority (Articles 31 and 36)

Data controllers are required to cooperate with the supervisory authority in the performance of its tasks. Moreover, where a DPIA conducted pursuant to Article 35 of the GDPR indicates that the processing of personal data would result in a high risk in the absence of measures

[124] Recital 75, GDPR. See also Art. 29 Working Party Guidelines on DPIA, p. 10 ("Vulnerable data subjects may include […] more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients)").
[125] Recitals 89, 91, GDPR.
[126] Art. 29 Working Party Guidelines on DPIA, p. 11.
[127] Art. 29 Working Party Guidelines on DPIA, p. 8.
[128] Article 35(1), GDPR.

taken by the controller to mitigate the risk, the controller must consult the supervisory authority prior to processing.

4.3.5.4 Remedies (for the data subject), liability and penalties

Non-compliance by controllers (Articles 82(2) and 83)

Data controllers involved in processing of personal data are liable for any damage caused by processing that infringes the GDPR. Only in case the controller can prove that they are not in any way responsible for the event resulting in damage, they may be exempt from such liability.

Article 83(1) of the GDPR provides that any administrative fines imposed should be "effective, proportionate and dissuasive." Such fines can be up to 20 million euros, or up to 4% of the total worldwide annual turnover[129].

4.3.6 The role and obligations of data processors

Data processor is a concept closely related to, but distinct from data controller. It processes personal data on behalf of the controller. The scope of obligations and responsibilities will vary, depending on which role, if any, a partner has under the GDPR. In discerning between the two roles, a number of criteria can be considered, including the role and expertise of the parties, monitoring by the data controller, visibility of the controller by the data subject, and the expectations of the data subject on the basis of that visibility[130].

While the data controller is primarily responsible for compliance with the GDPR and determines the purpose and means of processing, the data processor carries out processing on behalf of the controller and under its instruction[131]. Although they act under the supervision of a controller, the GDPR imposes many of the obligations placed on controllers also on data processors[132]. The lawfulness of the data processor's processing activity is solely determined by the mandate set by the controller[133]. Article 82(2) provides that a processor can also be held liable for damage caused by processing, but only where the processor has not complied with obligations under the GDPR (where they are specifically directed at the processor) or where it has acted outside or contrary to lawful instructions from the controller.

The GDPR stipulates that "controllers shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [the GDPR] and ensure the protection of the rights of the data subject" [134]. In case the controller engages a processor, the processing by the data processor will be governed by an agreement that sets out the subject-matter and

[129] Article 83(4), (5), GDPR.
[130] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 February 2010 ("Art. 29 Working Party Opinion 1/2010"), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, p. 28.
[131] Article 28(1), 29 GDPR. See also Handbook on DP Law, p. 101.
[132] Handbook on DP Law, p. 101. Including Articles 30, 31, 32, 33.
[133] Art. 29 Working Party Opinion 1/2010, p. 25. See also FASTER, p. 27.
[134] Article 28(1), GDPR.

duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller[135].

4.3.7 Transfer of personal data within and outside the European Union

The GDPR makes a distinction between the transfer of data within the EU where, in principle, the principle of free flow of personal data applies[136], and transfer of data outside of the EU (third countries).

For the transfer of personal data to third countries, the GDPR poses specific requirements. In short, transfer to a third country may take place based on: (1) an adequacy decision by the European Commission[137], (2) in the absence thereof, the controller or processor provides appropriate safeguards, enforceable rights and legal remedies for the data subject[138], or (3) in the absence of both an adequacy decision and appropriate safeguards, a number of specific derogations are possible[139].

4.4 Key national laws/provisions linked to data protection

Article 6(2) of the GDPR provides that Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to processing[140]. With regard to processing of sensitive data, Member States may further incorporate derogations from the GDPR, including prohibition to process sensitive data on the basis of data subject's consent, processing necessary for the purposes of occupational or preventive medicine and for public interest in the area of public health[141]. Member States may also "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health" [142].

In Phase 3 (Validation phase), the prototype systems of the 8 Pilots will be used in the real environments, and the tests are planned to be performed in the following countries: Greece (Pilot 1-AHEPA), Belgium (Pilot 2-CHUL), Italy (Pilot 3-IRCCS), Spain (Pilot 4-SERMAS), Slovenia (Pilot 5-UKCM), Spain (Pilot 6-INTRAS), Belgium (Pilot 7-Philips) and Belgium (Pilot 8-VUB) [143].

[135] Article 28(3), GDPR.
[136] Article 1(3), GDPR.
[137] Article 45, GDPR. The Court of Justice of the European Union ("CJEU") has clarified that the country in question needs to offer an adequate level of protection, meaning that is must be 'essentially equivalent' as the EU level, see HR-RECYCLER, p. 28 referring to CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015, para. 96.
[138] Article 46, GDPR.
[139] Article 49, GDPR. See also HR-RECYCLER, p. 28.
[140] See also TENDER D1.1 Fundamental Rights, Ethical and Legal Implications and Assessment, p. 63 or FASTER, p. 46.
[141] Article 9(2), GDPR. See also TENDER D1.1 Fundamental Rights, Ethical and Legal Implications and Assessment, p. 63 or FASTER, p. 46.
[142] Article 9(4), GDPR. See also TENDER D1.1 Fundamental Rights, Ethical and Legal Implications and Assessment, p. 63 or FASTER, p. 46.
[143] HosmartAI, Proposal Technical Annex (PartB), Sections 1 - 3, Page 25 of 70.

4.4.1 Germany

The German Federal Data Protection Act (Bundesdatenschutzgesetz - "BDSG") is the primary source of data protection law in Germany. It has been amended on 5 July 2017, and came into force together with the GDPR on 25 May 2018[144].

The BDSG sets for the general framework for the processing of sensitive data, including rules on health data[145]. Such processing is possible only if "suitable and specific" safeguards are taken to protect such data. The safeguards may include technical and organisational measures, pseudonymisation, encryption, or the appointment of a Data Protection Officer[146].

The BDSG provides derogations in relation to the processing of sensitive data without consent. Such processing is permitted for scientific, historical or statistical purposes if the processing is necessary for these purposes and the data controller's interest in processing such data significantly outweighs the data subject's interests[147]. The data controller is required to apply certain "suitable and specific" measures to ensure that the data is correctly protected. Further restrictions of data subjects' rights in the context of processing for research and statistical purposes are included in the BDSG which also sets out requirements for the publication of such data[148]. In line with Article 23 of the GDPR, paragraphs 32 to 37 of the BDSG include other restrictions of data subjects' rights[149].

On 20 September 2019, the German Bundesrat voted on the Second German Data Protection Amendment and Implementation Act ("Second Amendment") (which was passed by the German Bundestag on 27 June 2019). This Second German Data Protection Amendment and Implementation act will adapt more than 150 federal laws to the GDPR requirements[150]. Similar amendments are taking place at the regional German Federal States ('Bundesländer')[151].

The vast majority of changes under the Second Amendment involve aligning the terminology in the German Federal acts with terms used in the GDPR. However, a number of more substantive changes have also been implemented. For example, the BDSG has been amended to create a new exemption for companies processing special types of personal data (e.g. private companies are now also permitted to process political opinions, religious beliefs or trade union membership and data concerning health where there is a significant public

---

[144] Law in Germany - DLA Piper Global Data Protection Laws of the World, https://www.dlapiperdataprotection.com/index.html?t=law&c=DE; GA, Annex I, Part B, p. 100. See also Bird&Bird, GDPR Tracker (Germany) ("GDPR Tracker Germany") https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/germany.

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] PWC, *Reform of German data protection legislation: Second EU Data Protection Amendment and Implementation Act passed*, 23 September 2019 ("PWC"), https://www.pwc.de/en/newsletter/it-security-news-en/reform-of-german-data-protection-legislation-second-eu-data-protection-amendment-and-implementation-act-passed.html. See also GDPR Tracker Germany.

[151] GDPR Tracker Germany.

interest and the processing is absolutely necessary)[152]. Section 38 of the BDSG (as amended by Article 16 of the Second Amendment), now states that a data protection officer must only be appointed by companies with at least twenty employees continuously engaged in automated processing of personal data, instead of the current ten employees.

The relevant data protection authority in Germany is Bayerisches Landesamt für Datenschutzaufzicht (BayLDA)[153].

Genetic, biometric or health data

§ 22 FDPA permits the processing of sensitive data for a number of specific purposes including the following: preventive medicine, employee work capability assessment, medical diagnosis, health and social care treatments, management of systems, agreements with health professionals (and their staff) where data is provided under the obligation of professional secrecy, and for reasons of public interest in the area of public health (as required, for example, to ensure high quality and security standards for health services, drugs or medical products). However, such processing is only possible if certain safeguards are put in place to protect such data ("suitable and specific" safeguards)[154].

§ 22 FDPA provides a general framework for the processing of sensitive data, including rules on health data[155]. There is no explicit restriction to genetic or biometric data[156]. Such processing is, however, only possible if “suitable and specific” safeguards are taken to protect such data. The safeguards may include technical and organisational measures, pseudonymisation, encryption, or the appointment of a Data Protection Officer (“DPO”), and the like.

4.4.2 Italy

The Italian Data Protection Act (“IDPA”) was amended by the Legislative Decree 101/2018 ("Decree"), which entered into force on 19 September 2018, to modify provisions of the IDPA conflicting the GDPR[157]. The data protection authority in Italy (Italian DPA) is “Garante per la protezione dei dati personali” [158].

There are a number of derogations from the GDPR included in the relevant Italian law, including with respect to processing of special categories of data. For example, a “substantial public interest” is a viable lawful basis for the processing of special categories of personal data[159].

[152] PWC.
[153] GA, Annex I, Part B, p. 100.
[154] GDPR Tracker - Germany, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/germany.
[155] *Id.*
[156] *Id.*
[157] GA, Annex I, Part B, p. 100. See also Bird&Bird, GDPR Tracker (Italy) (“GDPR Tracker Italy”) https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/italy.
[158] GA, Annex I, Part B, p. 100.
[159] GDPR Tracker Italy.

The IDPA allows personal data to be processed, stored, and transferred to another controller after the normal period for processing and even after the termination of the main processing if carried out for scientific, historical or statistical purposes as well as archiving in the public interest[160]. Guidance will be issued for the processing of personal data for this purpose, aiming to identify adequate guarantees for the rights and freedoms of the data subject in accordance with Article 89 GDPR[161].

Genetic, biometric or health data

With regard to processing of genetic, biometric and health data, the IDPA requires Guidance be issued every 2 years, and the Italian DPA defines the applicable safeguards for processing of these categories of data. In case high-risk processing of genetic data exists, consent can be a further safeguard, and/or others should be applied. Genetic, biometric and health data cannot be disseminated[162]. To date, the Italian DPA has published several guidelines and opinions on the processing of data concerning health, biometric and genetic data[163].

4.4.3 Spain

The Organic Law 3/2018 of December 5, on the Protection of Personal Data and Guarantee of Digital Rights ("Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales" or "LOPDGDD") implements the GDPR and is the national data protection law of Spain[164].

The Spanish law introduces a number of lawful derogations from the GDPR. For example, it establishes particular rules for processing special categories of data (in order to avoid discriminatory practices, the consent of the data subject shall not be sufficient to overcome the prohibition on the processing of this type of data when the principal purpose of this processing is to identify their ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin)[165]. Moreover, the law establishes that the processing of special categories of personal data based on the public interest, for the purposes of

[160] *Id.*
[161] *Id.*
[162] *Id.*
[163] IDPA, General Application Order Concerning Biometrics as of November, 2014, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3590114; IDPA, Guidelines on Processing Personal Data to Perform Customer Satisfaction Surveys in Healthcare Sector as of May 5, 2011, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3853781; IDPA, Authorization №2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life as of December 30, 2014, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3800455; IDPA, Guidelines on the Electronic Health Record and the Health File as of July 16, 2009, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821; IDPA, General Authorization №8/2012 for the Processing of Genetic Data as of December 13, 2012, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2474250.
[164] Spain - Data Protection Overview | Guidance Note | DataGuidance, https://www.dataguidance.com/notes/spain-data-protection-overview; GA, Annex I, Part B, p. 100. See also https://delajusticia.com/wp-content/uploads/2018/12/Ley-proteccion-datos.pdf. See also Bird&Bird, GDPR Tracker (Spain) ("GDPR Tracker Spain"), https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/spain.
[165] GDPR Tracker Spain. See also FASTER, p. 46.

preventive or occupational medicine or public interest in the area of public health, shall be based on a standard with the rank of law, and this law could establish additional requirements for their security and confidentiality[166]. Additionally, Article 9 of the Spanish law specifies that the health data may be processed when required for the management of health care systems or the execution of an insurance contract to which the data subject is party[167].

The data protection national authority in Spain is Agencia Española de Protección de Datos (AEPD)[168].

Genetic, biometric or health data

LOPDGDD does not have its own definition of sensitive data, health data, or biometric data and makes reference to the definitions provided by the GDPR[169].

Article 9 of the LOPDGDD also addresses the processing of health data. Such data may be processed when required for the management of health care systems or the execution of an insurance contract to which the data subject is party[170].

Consent of a data subject is insufficient for the legal basis for processing of special categories of data if the main purpose is to identify an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or genetic data[171].

4.4.4 Slovenia

The latest amendment of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, no. 86/04, 113/05, 51/07, 67/07 and 94/07; Zakon o varstvu osebnih podatkov), originally adopted in 2004, and subsequently amended a number of times, entered into force in 2007 ("ZVOP")[172]. In 2018, the Ministry of Justice Presented the Data Protection Act-2 (Zakon o varstvu osebnih podatkov-2, "ZVOP-2") which would ensure GDPR compliance[173]. According to the Information Commissioner of the Republic of Slovenia (Slovenia's data protection authority), this law has not yet been adopted and therefore, currently, in addition to the GDPR, the ZVOP continues to apply, specifically "those provisions which are not regulated by the Regulation and which do not conflict with it" [174].

---

[166] *Ibid*.
[167] *Ibid*.
[168] GA, Annex I, Part B, p. 100.
[169] Spain - Data Protection Overview | Guidance Note | DataGuidance, https://www.dataguidance.com/notes/spain-data-protection-overview.
[170] GDPR Tracker - Spain, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/spain.
[171] Spain - Data Protection Overview | Guidance Note | DataGuidance, https://www.dataguidance.com/notes/spain-data-protection-overview.
[172] GA, Annex I, Part B, p. 100. See also http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906.
[173] See https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208. See also an Analytics Framework for Integrated and Personalised Healthcare Services in Europe (AEGLE), *AEGLE in Your Country – Slovenia*, 30 March 2018 ("AEGLE Report"), http://www.aegle-uhealth.eu/imagem/AEGLEinyourcountry_Slovenia.pdf, p. 6.
[174] Information Commissioner of the Republic of Slovenia, *Personal Data Protection Act*, https://www.ip-rs.si/en/legislation/personal-data-protection-act/. See also DLA Piper, *Data Protection Laws of the World –*

Processing may generally only take place if such processing is provided for by statute or if personal consent has been obtained[175]. Article 13 of the ZVOP sets out explicit consent as one of the legal bases of processing sensitive data. Irrespective of the initial purpose of collection, personal data may be further processed for historical, statistical and scientific research purposes under the condition that such personal data are supplied to the data recipient in anonymised form unless otherwise provided by statute or if the individual to whom the personal data relate gave prior written consent for the data to be processed without anonymising[176].

A relevant act in relation to the processing of health data is the Patient Rights Act, which contains a number of provisions relevant to data processing, including related to patients' right to access medical files, right to privacy and personal data protection (including scientific research) and protection of professional secrecy[177]. It indicates that while the processing of a patient's health data and other personal data outside procedures of medical treatment always requires the consent of the patient (or an authorised person in the event the patient is unable to provide consent), it does not require consent when such processing is performed for epidemiological and other research, education, medical publications or other purposes and as long as the patient is not identifiable[178]. Similarly, the Health Services Act provides that when personal health data is used for scientific research purposes, the relevant patient must be unidentifiable[179]. The Health Services Act further provides that testing of unverified methods of prevention, detection, treatment and rehabilitation, testing of medicines and other biomedical research is allowed only with the consent of the ministry responsible for health and with the written consent of the patient, and for the minors and persons under guardianship with the written consent of the parents or guardian[180]. Such testing will generally be subject to the consent of the Medical Ethics Commission of the Republic of Slovenia under its relevant Regulation[181]. "When consent has not been obtained from the data subject, NMEC has the power to make decisions about when research is justified in the public interest. Where unreasonable effort would be necessary to contact the data subjects, the potential risk of damage to the data subject appears remote, and the study is expected to

Slovenia, 14 January 2020 ("DLA Piper Slovenia Report"), see https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=SI, p. 2.

[175] E.g., Articles 8, ZVOP.

[176] Article 17(1), (2), ZVOP. See also AEGLE Report, p. 8.

[177] AEGLE Report, p. 4.

[178] Article 44(4) & (6), Patient Rights Act (Official Gazette of the Republic of Slovenia, no. 15/08 and 55/17; Zakon o pacientovih pravicah), http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4281. See also AEGLE Report, p. 8.

[179] Article 54, Health Services Act (Official Gazette of the Republic of Slovenia, no. 23/05, 15/08, 23/08, 58/08, 77/08, 40/12, 14/13, 88/16 and 64/17; Zakon o zdravstveni dejavnosti), http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO214. See also AEGLE Report, pp. 5, 8.

[180] Article 57, Health Services Act.

[181] See Rules on the Composition, Tasks, Competencies and Manner of Work of the Medical Ethics Commission of the Republic of Slovenia (Official Gazette RS, Nos. 30/95 , 69/09 , 47/17 , 64/17 - ZZDej-K and 21/18), 1995, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-0896?sop=2018-01-0896. See also AEGLE Report, p. 9.

provide important new scientific information, the NMEC may exempt the research proposer from the duty to seek consent" [182].

Finally, of relevance is also the Healthcare Databases Act, which "governs the processing of data and databases in the field of healthcare and shared electronic health records […], their controllers and data users" [183].

Following some concerns expressed from academia and other stakeholders on a previous version of the proposed ZVOP-2, the draft law has reportedly undergone several revisions. The current draft consequently brings a better alignment of the proposal with the provisions of the GDPR. Further major revisions are not expected" [184]. A number of sources provide that the language of the proposed ZVOP-2, at their time of writing, does not include any relevant derogations of the GDPR in areas where that is allowed, including on specific limitations for processing of genetic data, biometric data or data concerning health[185], or derogations on the rights of data subjects[186]. It is further provided that "[t]he current draft mostly follows the GDPR and only amends a few aspects, mostly of a systemic and procedural nature and adds some provisions in areas where GDPR allows to do so. Another source indicates that the proposed ZVOP-2 extends some of the obligations of data controllers under the GDPR also to data processors and also requires that processing of special categories of personal data is only permitted if an individual consents to it in writing, whereas the GDPR does not require the consent to be written (and does not allow derogation at this point)[187].

The Slovenian data protection authority is the Information Commissioner of the Republic of Slovenia[188]. It is expected that this will not change with the proposed ZVOP-2[189].

4.4.5 Greece

The primary sources of law of data protection in Greece are the GDPR and the national implementation law[190]. The implementing law -- Law No. 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) and Transposing into National Law Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) and Other Provisions ("Greek Law 4624/2019") -- was

[182] AEGLE Report, p. 10.
[183] Official Gazette of the Republic of Slovenia, no. 65/00 and 47/15. See also AEGLE Report, p. 5.
[184] DLA Piper Slovenia Report, p. 2.
[185] AEGLE Report, p. 6; Jadek & Pensa Law Firm (Slovenia), *The Slovenian Personal Data Protection Act (ZVOP-2) proposal – overstepping the GDPR boundaries?*, 20 March 2018, https://www.jadek-pensa.si/en/the-slovenian-personal-data-protection-act-zvop-2-proposal-overstepping-the-gdpr-boundaries/.
[186] AEGLE Report, p. 17.
[187] Rojos Peljhan Prelesnik & Partners Law Firm (Slovenia), *Analysis of the Slovenian GDPR Implementation Law in Light of its Main Deviations from, or Supplements to, Default Rules Set out in the GDPR*, 6 May 2019, https://www.rppp.si/wp-content/uploads/2019/05/20190506_GDPR-National-implementation.pdf, p. 2.
[188] GA, Annex I, Part B, p. 100.
[189] AEGLE Report, p. 7.
[190] DataGuidance, Greece - Data Protection Overview | Guidance Note, https://www.dataguidance.com/notes/greece-data-protection-overview.

adopted by the Greek Parliament in August 2019[191]. The Hellenic Data Protection Authority ('HDPA') is the competent regulatory authority of Greece.

There is no national variation of key definitions relevant to HosmartAI project, such as sensitive data, health data, or biometric data[192]. However, there is a deviation from the GDPR in terms of permissible grounds of processing of such special categories of personal data. Notwithstanding Article 9(1) of the GDPR, the Greek Law 4624/2019 allows processing of special categories of data by public and private bodies, provided it is necessary for enumerated grounds. One of the grounds is: "the purposes of preventive medicine, the assessment of an employee's ability to work for medical diagnosis, the provision of health and social care or the management of health and social care systems and services, or by means of an agreement with a health care professional or another person also bound by professional secrecy or is under latter's supervision" [193].

There are also some notable deviations from the GDPR with regard to processing for scientific or historical research purposes. Pursuant to Article 30 of the Greek Law 4624/2019, by way of derogation from Article 9 (1) of the GDPR, the processing of specific categories of personal data within the meaning of paragraph 1 of Article 9 of the GDPR is be permitted, without the consent of the subject, provided that: (1) the processing is necessary for the purposes of scientific or historical research, or for purposes related to the collection and maintenance of statistical data; and (2) controller's interest overrides the data subject's interests[194]. In such cases, the controller is obliged to take appropriate and specific measures to protect the legal interests of the data subject, including: (a) access restrictions for controllers and processors; (b) pseudonymization of personal data; (c) encryption of personal data; (d) appointment of DPO. Moreover, notwithstanding the provisions of Article 15, 16, and 21 of the GDPR, the rights of data subjects can be restricted provided: (1) the exercise of data subjects' rights could make impossible or significantly impede the performance of the scientific or historical research; and (2) restrictions in questions are deemed necessary for their performance. Furthermore, when special categories of data are processed for the above purposes, they must be anonymised, once the scientific or statistical purposes allow it, unless contrary to data subject's legitimate interest[195].

4.4.6 Belgium

The primary sources of law of data protection in Belgium are the GDPR and the Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data ("the GDPR Implementing Law") [196]. The "Data Protection Authority" or "Belgian DPA" (Autorité de protection des données in French or Gegevensbeschermingsautoriteit in Dutch),

[191] *Id.*
[192] *Id.*
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] DataGuidance, Belgium - National GDPR Implementation Overview | Guidance Note, https://www.dataguidance.com/notes/belgium-national-gdpr-implementation-overview.

established by the Act of 3 December 2017 Establishing the Data Protection Authority ('the DPA Law')[197], is the competent regulatory authority in Belgium.

For the purpose of HosmartAI Project, the Belgium data protection law deviates from the GDPR in the following way. By virtue of Article 9(4) of the GDPR, the GDPR Implementing Law sets higher conditions with regard to the processing of genetic data, biometric data or data concerning health[198]. Specifically, the GDPR Implementing Law obliges the data controller (and the processor where applicable) to take additional measures:

- designate the categories of persons who have access to such personal data, "specifying their status in relation to the processing of the data concerned;"
- "keep a list of the categories of designated persons at the disposal of the competent supervisory authority; and"
- "ensure that the designated persons are bound by a legal or statutory obligation, or by an equivalent contractual provision, to respect the confidentiality of the information in question" [199].

4.5 Relevance to HosmartAI and SELP

This Section provides some specific considerations relevant to the Project in light of rules under the GDPR.

4.5.1 Processing of Personal Data

The first step for the Project, before actually processing any personal data, is to understand and determine whether the particular data that will be processed (e.g., collected, used, stored, transferred, etc) by the project is "personal data," "sensitive data (special categories of personal data)," or non-personal data. If the data in question is "personal data" (which includes "sensitive data"), then the requirements under the GDPR apply and organizations must comply with the requirements when processing personal data. It is important to note that the definitions of personal data and processing under the GDPR are broad and encompass any activity with data about identified or identifiable person.

Data inventory of the Project is listed in 1.1 Data Management Survey of D6.7 - Data Management Handling Plan. The list includes: type of data to be processed, purpose, responsible partner and collaborating partner, and whether it is identifiable.

From a legal perspective, "anonymous data" is an attractive concept as the processing of such anonymous data does not fall under the scope of the GDPR[200]. This option, however, is not always easily achievable in research contexts because data that is truly anonymous may often

[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] Recital 26, GDPR. See also P. Quinn, *The Anonymization of Research Data – A Pyric Victory for Privacy that Should not be Pushed Too Hard by the EU Data Protection Framework?*, European Journal of Health Law (2017) ("Quinn"), pp. 2, 15.

offer little or no potential in terms of research or practical value[201]. Data is often only of use "where it contains personal (or quasi personal identifiers) that allow the data in question to be analysed within specific contexts" [202]. Nevertheless, the concept shall be taken into account depending on the nature of the data and the conditions of its processing within the project.

4.5.2 Data Controllers, Joint controllers, and data processors

The next step is to identify which partner is the data controller, and possibly the data processor(s), of the envisaged data processing. The question to ask: which entity, alone or jointly with others, can determine the purposes and means of the processing of personal data. In some instances, a single entity may not solely determine the purposes and means of processing; instead, two or more entities may jointly determine. If so, they are joint controllers, and it is important that arrangements are made that clearly identify and allocate responsibilities under the GDPR[203]. Also, if any processing activities, including IT solutions and cloud storage, are conducted by parties external to the HosmartAI consortium, it is recommended that a data processing agreement is signed[204].

4.5.3 Legal Basis and Informed Consent

To process personal data, the GDPR requires a legal basis. While the GDPR lists possible legal bases, consent -- freely given, specific, informed, and unambiguous -- by the data subject would be an option. This option allows the patient to be informed, determine whether or not to participate processing conducted under the Project, and importantly withdraw from the processing (i.e., revoke prior consent). As a practical matter, the Project should identify what is the exact legal basis for a particular processing, and to keep the record of when/who/how the consent was obtained (including when withdrawn).

4.5.4 Data Protection Impact Assessment ("DPIA")

DPIA is not required for all processing operation. In general, DPIA is required if the processing in question is likely to result in a high risk to the rights and freedoms of the natural persons, or if the processing meets one of the cases listed in Article 35 of the GDPR[205].

The Project intends to use various new technologies, such as AI, robotics, wearables, and sensors, to range of functions and medical tasks. These functions and tasks include screening of high-risk patients, computer-aided diagnosis, treatment and surgical support, personalized rehabilitation, and provision of assistive care. The use of new technologies has the potential to inflict unintended harm to the data subjects because "the personal and social

[201] Quinn, pp. 2, 15, 16.
[202] Quinn, p. 15.
[203] Article 26(1), GDPR. See also Recital 79, GDPR.
[204] Recital 81, GDPR. See Annex A, template Data Processing Agreement, https://gdpr.eu/data-processing-agreement/.
[205] See Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April 2017 ("Art. 29 Working Party Guidelines on DPIA"), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, p. 8.

consequences of the deployment of a new technology may be unknown"[206]. The use of AI, robotics, and wearable sensor technologies has the potential to affect the rights of the data subject substantially. This is even so because many of the types of data processed in the Project are sensitive in nature. In addition, DPIA can help the data controller to better understand the potential risks of new technology, and importantly mitigate them[207].

4.5.5 Use of AI technology and Profiling Regulation

In HosmartAI, many of the medical tasks or functions involve technology that falls within the definition of automated decision-making or profiling[208], and these technologies are regulated under the GDPR. Automated decisions are defined as "decisions taken using personal data processed solely by automatic means without any human intervention" [209]. Profiling is a form of automated decision-making and means "the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" [210]. Profiling consists of three elements: (i) an automated form of processing is utilised; (ii) the processing is carried out on personal data; and (iii) the profiling must be to evaluate certain personal aspects of the natural person[211].

The Guidelines on Automated Decision-Making and Profiling note that "[a]utomated decision-making has a different scope and may partially overlap with or result from profiling" and that "[a]utomated decisions can be made with or without profiling; profiling can take place without making automated decisions" [212]. The Guidelines further specify that "[s]olely automated decision-making is the ability to make decisions by technological means without human involvement."

In principle, controllers may carry out profiling and automated decision-making as long as they meet all the relevant principles of data processing and have a lawful basis for the processing [213]. However further restrictions and safeguards apply to solely automated individual decision-making.

Article 22 of the GDPR provides that, unless an exception under either subparagraph (2) or (4) applies, data subjects have the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or

[206] Art. 29 Working Party Guidelines on DPIA, p. 10.
[207] *Ibid*.
[208] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 3 October 2018 (last revised 6 February 2018) ("Guidelines on Automated Decision-Making and Profiling"), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, p. 5.
[209] Handbook on DP Law, p. 233.
[210] Article 4(4), GDPR.
[211] See Guidelines on Automated Decision-Making and Profiling, pp. 6, 7. See also FASTER, p. 30.
[212] Guidelines on Automated Decision-Making and Profiling, p. 8. See also FASTER, p. 30.
[213] Guidelines on Automated Decision-Making and Profiling, p. 9.

significantly affects them. One of the exceptions is based on the data subject's informed consent.

In relation to sensitive data, automated individual decision making, may only be allowed in case the legal basis for processing is either explicit consent or a substantial public interest[214]. In the event one of these exceptions applies, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests should be put in place[215].

In case of automated decision-making, including profiling, the data subject is entitled to be provided with "to be provided with the meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" [216]. Because the automated decision making and profiling are subject to further restrictions and safeguards, the Project should identify which processing will fall within the definition of automated decision making or profiling.

[214] Article 22(4) GDPR, referring to Article 9(2)(a) and (g).
[215] Article 22(4) GDPR.
[216] Article 13(2)(f), GDPR.

5 Ethical and Social Issues

5.1 Introduction

Generally, issues covered in this Report cannot be disintegrated separately into three distinct groups, namely ethical, legal, or social issues. Instead, each of these issues consists of ethical, legal, and/or social aspects. When a particular issue raises an ethical or social concern, typically a law or regulation is enacted to address these concerns. This makes it quite common that a particular issue is simultaneously ethical, social, and/or legal in nature. Having said that, however, one way to categorize these issues is to look whether or not there's a legally binding instrument on the issue. Taking this view, Chapters 3 and 4 touched upon issues that are regulated by a law or regulation (i.e., legal issues). This Chapter addresses issues that do not fall in the category of legal issues (i.e., ethical and social issues).

This, however, does not mean the issues addressed and the frameworks touched in this Chapter are less significant. A potential reason why particular issues in this Chapter are not subject to a legally binding instrument is because a regulation is being drafted and discussed by the legislative bodies of the EU. The 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 ("Draft AI Regulation")[217], published on 21st of April, 2021, is a good example of this. While it is not legally binding as of now, it is possible that the Draft AI Regulation, with modifications, becomes the law and be applicable to the Project. As the Draft AI Regulation is built upon existing frameworks, including non-legally binding frameworks (e.g., "Ethics guidelines for trustworthy AI" by High Level Expert Group on Artificial Intelligence, *infra*), complying with existing but non-legally binding frameworks would allow the Project to be more efficient and effective.

5.2 Medical Ethics

5.2.1 Sources for principles of ethics in research with humans

The principle of medical ethics is one of the most important principles for any research engaging directly with human participants. Many of these principles have a long tradition dating back centuries, some even back to Hippocrates of ancient Greece[218]. In more recent years, some of these ethical principles have been codified in various instruments.

For instance, in the wake of World War II, in August 1947, a judgement in the 'Doctors' Case' before the Nuremburg Tribunal, dealing with human experimentation, set out "certain basic principles that must be observed in order to satisfy moral, ethical and legal concepts" [219], now

[217] European Commission, 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 (2021) [hereinafter *Draft AI Regulation*], https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.
[218] Hippocrates, *The history of epidemics*, Samuel Farr (trans.), London: T. Cadell (1780).
[219] Trials of War Criminals before the Nuremberg Military Tribunals, under Control Council Law No. 10, Vol. 2, pp. 181-182, Washington, D.C.: U.S. Government Printing Office (1949), https://www.loc.gov/rr/frd/Military_Law/pdf/NT_war-criminals_Vol-II.pdf ("Nuremberg Code").

known as the Nuremberg Code**.** The Nuremberg Code centres around "the protection of the individual's rights and welfare through autonomy, human dignity and self-determination" [220]. This emphasis on autonomy is illustrated, for instance, by Principle 1, which makes voluntary consent absolutely essential to the conduct of medical experiments, and Principle 9, which gives the human subject the power to end the experiment at any time[221]. The Code further requires that the risks of the experiment weigh against the expected benefits (Principle 6)[222] and that the researcher should be prepared to terminate the experiment if continuation would dangerous (Principle 10)[223].

With the Nuremberg Code as a strong foundation, various other instruments have since been codified that set out important ethical principles related to the participation of human participants in research. One of such instruments is the Declaration of Helsinki, first adopted by the World Medical Association in 1964 and subsequently amended, which was adopted "as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data" [224]. While the Declaration of Helsinki is mainly aimed at physicians, it encourages others involved in medical research with human participants to adopt these principles[225]. Even though the Declaration of Helsinki is not a legally binding document, it is widely considered to set out the ground principles for conducting research with human participants[226]. 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 relevant instruments include the International Ethical Guidelines for Health-Related Research Involving Humans by the Council for International Organizations of Medical Sciences ("CIOMS" and "CIOMS Guidelines" respectively) which sets out to "provide internationally vetted ethical principles and detailed commentary on how universal ethical principles should be applied" [227]. The Guideline for Good Clinical Practice by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use

[220] *Ibid*. See also A.M. Lachapelle-Henry, P. D. Jethwani, M. A. Grodin, *The complicated legacy of the Nuremberg Code in the United States*, in: Medical Ethics in the 70 Years after the Nuremberg Code, 1947 to the Present, Czech, H., Druml, C. & Weindling, P (eds.), Wien Klin Wochenschr 130, 180 (2018), https://doi.org/10.1007/s00508-018-1343-y.
[221] Principles 1 and 9, Nuremberg Code.
[222] Principle 6, Nuremberg Code ("The degree of risk to be taken should never exceed that determined by the humanitarian importance of the problem to be solved by the experiment").
[223] Principle 10, Nuremberg Code ("During the course of the experiment the scientist in charge must be prepared to terminate the experiment at any stage, if he has probably cause to believe, in the exercise of the good faith, superior skill and careful judgment required of him that a continuation of the experiment is likely to result in injury, disability, or death to the experimental subject.").
[224] World Medical Association, Declaration of Helsinki – Ethical principles for medical research involving human subjects (June 1964, and most recently amended October 2013) ("Declaration of Helsinki"), Preamble, para. 1.
[225] Preamble, para. 2, Declaration of Helsinki.
[226] See also PROTEIN, p. 13.
[227] 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"), preface, p.viii.

("ICH" and "ICH GCP" respectively) can also provide useful guidance[228]. While the activities anticipated in the HosmartAI project do not fall within the notion of a clinical trial for pharmaceutical products, compliance with this standard should provide assurances that the rights, safety and well-being of research participants are protected in line with the principles that have their origin in the Declaration of Helsinki[229]. In this regard, the WHO's Handbook for Good Clinical Research Practice ("WHO GCP") is another important source. The WHO GCP is based on major international guidelines, including the ICH GCP[230], but is intended to generally be applicable to all research studies on human participants, "not just research involving pharmaceutical or other medical products" [231]. Even if certain principles may not apply to all types of research on human participants, the WHO encourages consideration of its principles wherever applicable "as a means of ensuring the ethical, methodologically sound and accurate conduct of human subjects' research" [232].

Of further relevance are the International Covenant on Civil and Political Rights ("ICCPR") which enshrines the right to refuse to participate in research in Article 7[233], the UNESCO's Universal Declaration on Bioethics and Human Rights [234], and the Council of Europe's Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine ("Oviedo Convention")[235] and its Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research ("Oviedo Additional Protocol")[236].

5.2.2 Basic principles of medical ethics

In 1979, Beauchamp and Childress developed a generally accepted approach to biomedical ethics which identifies four main ethical principles; autonomy, beneficence, non-maleficence, and justice[237].

---

[228] International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use ("ICH"), *Guideline for Good Clinical Practice*, 10 June 1996 ("ICH GCP").
[229] See also PROTEIN, pp. 13, 14.
[230] WHO, *Handbook for Good Clinical Research Practice*, 2005 ("WHO GCP"), https://apps.who.int/iris/handle/10665/43392 (last accessed on 21 January 2020), p. 1.
[231] *Id.*, pp. 5, 6.
[232] *Id.*, p. 7.
[233] United Nations General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171 ("ICCPR"), Article 7, ("In particular, no one shall be subjected without his free consent to medical or scientific experimentation.").
[234] United Nations Educational, Scientific and Culture Organisation ("UNESCO"), *Universal Declaration on Bioethics and Human Rights,* 19 October 2005 ("UNESCO Declaration"), http://portal.unesco.org/en/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html.
[235] Council of Europe, *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, 4 April 1997, ETS No. 164 ("Oviedo Convention"), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98.
[236] Council of Europe, *Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research*, 25 January 2005, CETS No. 195 ("Oviedo Additional Protocol"), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008371a.
[237] T. L. Beauchamp, J. F. Childress, *Principles of biomedical ethics*, Oxford University Press, USA, 2001 (the book has been revised subsequently).

The principle of autonomy relates to self-determination and the notion that individuals have the authority and the right to make their own choices and develop their own life[238]. In healthcare, the principle of autonomy requires that only upon an informed decision by the patient may any intervention to their body be made[239]. For such a decision to be truly autonomous, it will be intentional, with full understanding and without undue influence from others that might impair the free and voluntary nature of the decision[240]. Informed consent plays an important role in the protection of patient (and research participant) autonomy. It constitutes a way in which patients and research participants can exercise their autonomy[241]. In general, informed consent can both be expressed and implied[242]. While express consent often occurs in a hospital setting, where the patient expressly agrees to the proposed procedure, in many other "medical encounters where a patient presents for evaluation and care", consent can often be considered implied[243]. Nevertheless, in research with human participants, it is generally considered that informed consent should be express and documented[244].

The principle of beneficence requires a physician to do good and act in the best interest of the patient. This principle is central to the patient-doctor relationship which entails "special obligations for the physician to serve the patient's interest because of the specialized knowledge that [they] possess, the confidential nature of the relationship, the vulnerability brought on by illness, and the imbalance of expertise and power between patient and physician" [245].

The principle of non-maleficence requires a physician to do no harm and to avoid acting against the patient's interests. It requires the physician to "weigh the expected bad effects of any proposed intervention against the intended beneficial effects" [246].

The principle of justice must inform the physician's decisions about resource allocation and requires an equitable distribution of medical goods and services[247]. This principle also implies a prohibition to discriminate and warns the physician against taking decisions based on negative stereotypes, such as blaming an overweight person for failing to keep to a prescribed

[238] Garrett *et. al.*, *Health Care Ethics*, Prentice Hall, 2nd Edition (1993), p. 28. See also PROTEIN, p. 14.
[239] See also PROTEIN, p. 14.
[240] See also PROTEIN, p. 14.
[241] E.g., Article 5, UNESCO Declaration; Guideline 9, CIOSM Guidelines, p. 34; Principle 7, WHO GCP, pp. 59, 60, 67.
[242] L. S. Sulmasy, T. A. Bledsoe, for the ACP Ethics, Professionalism and Human Rights Committee, *American College of Physicians Ethics Manual* (Seventh Edition), Ann Intern Med., (2019) 170:S1–S32 ("ACP Ethics Manual"), https://doi.org/10.7326/M18-2160, p. 6.
[243] *Ibid*.
[244] E.g., para. 26, Declaration of Helsinki; Article 14(1), Oviedo Additional Protocol; Article 6(1), UNESCO Declaration; Principle 9, CIOMS Guidelines, p. 33; Principle 7, WHO GCP, p. 67.
[245] APC Ethics Manual, p. 3. See also PROTEIN, p. 14.
[246] *Id*., p. 45.
[247] APC Ethics Manual, p. 2. See also PROTEIN, p. 14.

treatment or considering an older person a burden rather than someone deserving of medical intervention[248].

It has been argued that the principle of beneficence, to do good, is necessarily tempered by the duty to respect autonomy, the duty to do no harm (non-maleficence) and the duty of justice[249], thereby striking a balance between these, sometimes competing, interests.

5.3 Informed Consent

Informed consent is a cornerstone of the principle of autonomy and is relevant to the conduct of research with human participants. While the Nuremberg Code refers to "voluntary consent" [250], the Declaration of Helsinki provides that "after ensuring that the potential subject has understood the information, the physician or another appropriately qualified individual must then seek the potential subject's freely-given informed consent, preferably in writing" (emphasis added)[251]. Paragraph 26 of the Declaration of Helsinki lists the sort of information that needs to be provided to the research participant for the consent to be informed [252]. The Declaration requires that special attention is given "to the specific information needs of individual potential subjects as well as to the methods used to deliver the information" [253].

Traditionally, the following elements are usually considered necessary for competent judgement: the ability to receive, process and understand information, the ability to appreciate the situation and its consequences, the ability to weigh benefits, risks and alternatives, and the ability to make and communicate a decision.

The importance of the notion of informed consent in research with human participants is further evidenced by its inclusion in numerous instruments, including in the ICCPR[254], CIOMS Guidelines[255], the ICH GCP[256], the WHO GCP[257], and the UNESCO Declaration[258].

It is also a central element of both the Oviedo Convention and the Oviedo Additional Protocol. Article 16(v) of the Oviedo Convention sets out the conditions for undertaking research on a person, including that "the necessary consent as provided for under Article 5 has been given

[248] See also PROTEIN, p. 14.
[249] R. Gillon, *Beneficence: doing good for others*, British Medical Journal Vol. 291, 6 July 1985, p. 44.
[250] Principle 1, Nuremberg Code.
[251] Para. 26, Declaration of Helsinki.
[252] *Ibid*. ("In medical research involving human subjects capable of giving informed consent, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study. The potential subject must be informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without reprisal.").
[253] Para. 26, Declaration of Helsinki.
[254] Article 7, ICCPR.
[255] Guideline 9, CIOMS Guidelines, p. 33.
[256] Principle 2.9, ICH GCP, pp. 9, 15 to 18.
[257] Principle 7, WHO GCP, p. 59 to 71.
[258] Article 6, UNESCO Declaration.

expressly, specifically and is documented. Such consent may be freely withdrawn at any time" [259]. The Oviedo Additional Protocol deals in more detail with the issue of informed consent in biomedical research. Article 13 requires that all potential research participants be provided with "adequate information in a comprehensible form" and lists the elements that they should be informed of, including the nature, extent, duration of the study, risks and benefits of participation, the handling of personal data and compensation in case of damage[260]. Article 14 then reiterates that "no research on a person may be carried out […] without the informed, free, express, specific and documented consent of the person" and that "such consent may be freely withdrawn by the person at any phase of the research" [261].

5.3.1 Vulnerable persons

Vulnerable persons are described as those who are, relatively or absolutely, incapable of protecting their own interests[262]. This may be the result of relative or absolute impairment in "decisional capacity, education, resources, strength, or other attributes needed to protect their own interests" or "because some feature of the circumstances (temporary or permanent) in which they live makes it less likely that others will be vigilant about, or sensitive to, their interests" [263]. While it is recommended not to automatically label a member of a certain group as vulnerable, some characteristics make it reasonable to assume that certain individuals are vulnerable[264], for instance persons in nursing homes, those incapable of giving consent or with diminished mental capacities, people with incurable diseases, people with physical frailty (e.g., due to age or co-morbidities), children or economically disadvantaged persons[265]. It is recommended to make the determination of whether a participant is to be considered a vulnerable person based on the specific context of their case.

While research with a vulnerable group is generally allowed, there are some specific considerations to make. According to the Declaration of Helsinki "[m]edical research with a vulnerable group is only justified if the research is responsive to the health needs or priorities of this group and the research cannot be carried out in a non-vulnerable group. In addition, this group should stand to benefit from the knowledge, practices or interventions that result from the research" [266]. It further provides that "[a]ll vulnerable groups and individuals should receive specifically considered protection" [267].

This principle of providing specific protections and safeguards to vulnerable persons is reiterated in the UNESCO Declaration, the WHO GCP and the CIOSM Guidelines[268]. Such

[259] Article 16, Oviedo Convention, referring to Article 5 of the Oviedo Convention which sets out that "[a]n intervention in the health field may only be carried out after the person concerned has given free and informed consent to it."
[260] Article 13(1), (2), Oviedo Additional Protocol.
[261] Article 14(1), Oviedo Additional Protocol.
[262] Principle 7, WHO GCP, p. 65.
[263] Guideline 15, CIOSM Guidelines, p. 57. See also Principle 7, WHO GCP, 65.
[264] Guideline 15, CIOSM Guidelines, p. 57.
[265] E.g., ICH GCP, p. 8; Principle 7, WHO GCP, pp. 65, 66; Guideline 15, CIOSM Guidelines, p. 58.
[266] Para. 20, Declaration of Helsinki.
[267] *Id*., para. 19.
[268] E.g., Article 8, UNESCO Declaration; Principle 1, WHO GCP, p. 22; Guideline 15, CIOSM Guidelines.

protections could include "allowing no more than minimal risks for procedures that offer no potential individual benefits for participants; supplementing the participant's agreement by the permission of family members, legal guardians, or other appropriate representatives; or requiring that the research be carried out only when it is targeted at conditions that affect these groups" [269]. As for other safeguards, it is recommended that they "can be designed to promote voluntary decision-making, limit the potential for confidentiality breaches, and otherwise work to protect the interests of those at increased risk of harm" [270].

5.3.2 Human participants who are unable to give consent

HosmartAI Proposal specifically touches upon issues with regard to obtaining consent from human participants who are unable to give consent and the Recommendation No. R (99) of the Committee of Ministers to Member States on Principles Concerning the Legal Protection of Incapable Adults[271].

The Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults, adopted by the Committee of Ministers on 23 February 1999, describes incapable adults as adults who, "by reason of an impairment or insufficiency of their personal faculties, are incapable of making, in an autonomous way, decisions concerning any or all of their personal or economic affairs, or understanding, expressing or acting upon such decisions, and who consequently cannot protect their interests" [272]. While the Recommendation No. R(99)4 does not directly deal with the question of scientific research [273], it provides important guidance on the legal protections for persons incapable of giving consent, including the application of the notion of consent in such cases.

The Declaration of Helsinki[274], the Oviedo Convention and its Additional Protocol provide that research may not be conducted on persons without the capacity to provide consent unless a number of stringent requirements are fulfilled[275]. Central to these requirements are that, generally, the results of the research should have the potential to produce a real benefit to the health of the person who is unable to provide consent, "research of comparable effectiveness cannot be carried out on individuals capable of giving consent", authorisation from a legal representative or an authority/body/person provided for by law has been obtained, and the person does not object[276].

---

[269] E.g., Guideline 15, CIOSM Guidelines, p. 59; Principle 1, WHO GCP, p. 22.
[270] Guideline 15, CIOSM Guidelines, p. 59.
[271] HosmartAI, Proposal Technical Annex (PartB), Sections 4 – 5, at 127 of 155.
[272] Council of Europe, *Recommendation No. R(99)4 of the Committee of Ministers of the Member States on Principles Concerning the Legal Protection of Incapable Adults, 23 February 1999* ("Recommendation No. R(99)4"), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e303c, Part I, para. 1.
[273] Rather, the Recommendation deals with "intervention in the health field" which is defined as those interventions for the purpose of preventive care, diagnosis, treatment, rehabilitation or research (see Part I, para. 5).
[274] Para. 28, Declaration of Helsinki.
[275] Article 17(1), Oviedo Convention; Article 15(1), Additional Protocol.
[276] *Ibid*. See also paras. 28, 29, Helsinki Declaration; Guideline 16, CIOSM Guidelines, p. 61; Article 7(b), UNESCO Declaration.

The Declaration of Helsinki further adds that research with persons physically or mentally incapable of providing consent may "be done only if the physical or mental condition that prevents giving informed consent is a necessary characteristic of the research group" [277].

The CIOSM Guidelines, *supra*, emphasise the importance of including adults not capable of giving informed consent, "unless a good scientific reason justifies their exclusion", especially because they might have distinct physiologies or health needs that would warrant special consideration by research[278]. The CIOSM does recognise that such individuals "may not be able to protect their own interests due to their lack of capacity to provide informed consent" and that this requires protections and safeguards to be put in place[279].

Some important legal protections for persons incapable of giving consent are set out in the Recommendation No. R(99)4, which is governed by the principles of necessity, subsidiarity, maximum preservation of capacity and proportionality [280]. Especially the principle of maximum preservation of capacity is interesting to note here as this shows that the Recommendation No. R(99)4 favours the idea of 'actual capacity' versus 'legal capacity' where possible, especially in light of the fact that incapacity can be temporary or partial[281]. This is also echoed by the CIOSM Guidelines, which states that "a lack of decisional capacity is time-, task- and context-specific" [282].

However, even in cases where the participant is indeed unable to consent, Recommendation No. R(99)4 sets out the need for respect for the wishes of the person concerned, whereby, as much as possible, due consideration should be given to "the past and present wishes and feelings" of an adult unable to provide consent [283]. This also requires that the legal representative should give such adults adequate information, wherever possible and appropriate, in particular concerning any major decision affecting them, so that they may express their views[284].

This principle is mirrored in numerous instruments. The Declaration of Helsinki, for instance, provides that "[w]hen a potential research subject who is deemed incapable of giving informed consent is able to give assent to decisions about participation in research, the physician must seek that assent in addition to the consent of the legally authorised

[277] Para. 30, Declaration of Helsinki. See also Principle 7, WHO GCP, p. 68.
[278] Guideline 16, CIOSM Guidelines.
[279] Guideline 16, CIOSM Guidelines.
[280] See Principles 1, 3, 5 and 6, Recommendation.
[281] Council of Europe, *Explanatory Memorandum – Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults*, 23 February 1999 ("Explanatory Memorandum R(99)4"), https://rm.coe.int/09000016805e302a, paras. 35, 73. See also S. Jansen, *Recommendation No. R(99)4 of the Committee of Ministers to Member States on Principles concerning the Legal Protection of Incapable Adults, and Introduction in Particular to Part V Interventions in the Health Field*, 7 Eur. J. Health L. 333 (2000), pp. 336, 337.
[282] Guideline 16, CIOSM Guidelines, p. 62.
[283] Principle 9(1), Recommendation.
[284] Principle 9(3), Recommendation ("a person representing or assisting an incapable adult should give him or her adequate information, whenever this is possible and appropriate, in particular concerning any major decision affecting him or her, so that he or she may express a view").

representative" [285]. The UNSESCO Declaration also finds that in case of inability to consent, the participant should still be involved in the decision-making process "to the greatest extent possible" [286]. The CIOSM Guidelines also advocate for a process of involvement, stating that "must be engaged in the research discussion at the level of their capacity to understand, and they must be given a fair opportunity to agree to or to decline participation in the study" [287].

5.4 AI and Robotics

AI, or artificial intelligence, is commonly referred to as a technology consisting of one or more of the following elements: "*machine learning techniques* used for searching and analysing *large volumes of data*; *robotics* dealing with the conception, design, manufacture and operation of programmable machines; and *algorithms* and automated decisionmaking systems (ADMS) able to *predict* human and machine behaviour and to make autonomous decisions" (emphasis added)[288]. The term "artificial intelligence" is not defined under the law. The European Parliament expressed that "there is a need to create a generally accepted definition of robot and AI that is flexible and is not hindering innovation" [289].

As the HosmartAI Proposal touches[290], regulatory framework for AI is still at the stage of development. However, there are a number of guidelines and recommendations helpful for the HosmartAI Project.

5.4.1 Ethics and trustworthy AI (AI HLEG)

In April 2019, the EU published its guidelines on ethics in AI entitled "Ethics guidelines for trustworthy AI" drafted by High Level Expert Group on Artificial Intelligence (AI HLEG)[291].

The AI HLEG considers that AI has the potential to "significantly transform society", "a promising means to increase human flourishing, thereby enhancing individual and societal well-being and the common good, as well as bringing progress and innovation" [292]. To that end, AI HLEG considers that AI needs to be human-centric, and rest on a commitment to its use in the service of the common good and humanity, aiming to improve human welfare and freedom[293]. The "human-centric" approach, the core principle of the EU Ethics Guidelines on AI, is explained as the following:

---

[285] Para. 29, Declaration of Helsinki. See also, for instance, Meulenbroek *et al*., p. 62.
[286] Article 7(a), UNESCO Declaration.
[287] Guideline 16, CIOSM Guidelines, p. 62.
[288] MADIEGA Tambiama, EU guidelines on ethics in artificial intelligence: Context and implementation 13 (2019), https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)640163. See also High-Level Expert Group on Artificial Intelligence (glossary section of the Ethics Guidelines for Trustworthy AI).
[289] European Parliament, *Report with Recommendations on Civil Law Rules on Robotics*, 27 January 2017 ("EP Recommendations on Civil Law Rules on Robotics"), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN, Recital C. See also FASTER, p. 30.
[290] HosmartAI, at 31 of 70 (stating "(iii) uncertain standardization and a fragmented regulatory frame for AI, covering standardization issues as well as human rights").
[291] High-Level Expert Group on Artificial Intelligence, Ethics guidelines for trustworthy AI (2019), https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai [hereinafter *EU Ethics Guidelines on AI*].
[292] Ethics Guidelines Trustworthy AI, p. 4.
[293] *Ibid*.

> The human-centric approach to AI strives to ensure that human values are central to the way in which AI systems are developed, deployed, used and monitored, by ensuring respect for fundamental rights, including those set out in the Treaties of the European Union and Charter of Fundamental Rights of the European Union, all of which are united by reference to a common foundation rooted in respect for human dignity, in which the human being enjoys a unique and inalienable moral status. This also entails consideration of the natural environment and of other living beings that are part of the human ecosystem, as well as a sustainable approach enabling the flourishing of future generations to come.[294]

Acknowledging the risks associated with AI, the AI HLEG seeks to maximise the benefits of AI and minimising or preventing risks through the concept of trustworthy AI. Three key components of trustworthy AI that should be met throughout the system's lifecycle require that AI should be:

- *Lawful, complying with all applicable laws and regulations;*
- *Ethical, ensuring adherence to ethical principles and values; and*
- *Robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.*[295]

The AI HLEG highlights that, ideally, these components should work in harmony and overlap in their operation, though it recognises that tension may exist between them (e.g., "at times the scope and content of existing law might be out of step with ethical norms")[296].

Four ethical principles that are at the foundation of trustworthy AI are: (i) respect for human autonomy, (ii) prevention of harm, (iii) fairness, and (iv) explicability[297]. While some of these ethical principles are also reflected in legal requirements, thereby falling into the scope of lawful AI, it is important to recall that adherence to ethical principles "goes beyond formal compliance with existing laws" [298].

The Expert Group further identifies a non-exhaustive list of requirements that can assist in translating the identified principles into practical means of achieving trustworthy AI[299]. Some of the key requirements relevant in the context of SELP follow:

Human agency and oversight

- A fundamental rights impact assessment should be undertaken prior to its development.
- Users should be able to understand and interact with AI systems to a satisfactory degree. The right of end users not to be subject to a decision based solely on automated processing.

[294] Id., at 37.
[295] Ethics Guidelines Trustworthy AI, p. 5.
[296] *Ibid*.
[297] Ethics Guidelines Trustworthy AI, pp. 11, 12.
[298] *Id.*, p. 12.
[299] *Id.*, p. 14.

- Humans should always have the possibility ultimately to override a decision made by a system.

Privacy and data protection

- Individuals should have full control over their own data.
- Their data should not be used to harm or discriminate against them.
- AI developers should apply design techniques, such as data encryption and data anonymisation, so that AI systems is designed to guarantee privacy and data protection.
- AI developers should ensure the quality of the data, i.e., avoid socially constructed biased, inaccuracies, errors and mistakes. To that end, AI developers should put in place oversight mechanisms to control the quality of data sets.

Transparency

- The data sets and processes that are used in building AI systems should be documented and traceable.
- AI systems should be identifiable as such, and humans need to be aware that they are interacting with an AI system.
- AI systems and related human decisions are subject to the principle of explainability, according to which it should be possible for them to be understood and traced by humans.

Diversity, non-discrimination and fairness

- AI developers should make sure that the design of their algorithms is not biased.
- Stakeholders that maybe directly or indirectly affected by AI systems should be consulted and involved in their development and implementation.
- AI systems should be conceived with consideration for the whole range of human abilities, skills and requirements, and ensure accessibility to persons with disabilities.

Societal and environmental wellbeing

- AI systems should be used to enhance positive social change and encourage sustainability and environmental responsibility of AI systems.
- The social impacts of these systems (i.e., on people's physical and mental wellbeing) must be monitored and considered.
- The effects of AI systems on society and democracy (including regarding the electoral context) should be assessed.

Accountability

- Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.
- Reporting of the AI systems' negative impacts should be available (including for whistle-blowers), and impact assessment tools should be used to that end.

- In situations where the implementation of the key ethical requirements creates conflicts between them, decisions on the trade-off (i.e., the decision to choose to fulfil one ethical requirement over another) should be evaluated continuously.
- Accessible redress mechanisms should be implemented.

There are critiques from a number of members of the Commission's expert group on AI and from civil society groups, which one being it is not legally binding.

5.4.2 Note on Explanainability

HosmartAI explicitly mentions about Explainable AI framework and explainable computer-aided diagnosis systems[300]. Due to the nature of how machine learning works, complex machines and algorithms often do not provide information as to their behaviours and processes[301]. This is referred to as the "black box effect," and the concept and requirement of explainable AI is purported to address this issue. While the GDPR provide some level of "explanainability" under the transparency obligation[302], the more extensive discussions take place not only under the GDPR, but also outside of the context of data protection law. The concept and requirement of explanainability is touched in this Section partly because the issue goes beyond the existing legal regulatory framework, and those requirements currently discussed are mostly not legal requirements as of now.

The concept of explanainability is about 'making explanations on an algorithmic decision-making system ("ADS") available' [303]. The study conducted by EP and published in March 2019 defines explanainability as the availability of explanations about the ADS, and is contrasted to transparency because explanainability requires delivery of information beyond ADS itself[304].

The explanainability is particularly important to ensure fairness in the use of algorithms and to identify potential bias in the training data[305]. To that end, "an explanation should be available on **how AI systems influence and shape the decision-making process**, on how they are **designed**, and on what is the **rationale** for deploying them" (emphasis in original)[306].

The study by the EP lays out three main approaches to implement the requirements of explanainability:

- **The black box approach**: analyses the behaviour of the ADS without 'opening the hood', i.e., without any knowledge of its code.
- **The white box approach**: in contrast to the black box approach, this approach assumes that analysis of the ADS code is possible.

---

[300] E.g., HosmartAI Proposal, pages 6 and 7 of 70.
[301] EP Briefing on EU guidelines on ethics in AI, at 5.
[302] Articles 13(2)(f) and 14(2)(g) as well as Article 22 of the GDPR. See also Article 29 Data Protection Working Party (WP29), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
[303] EP Briefing on EU guidelines on ethics in AI, at 5.
[304] Claude Castelluccia & Daniel Le Métayer, Understanding algorithmic decision-making: opportunities and challenges (2019), at III, https://data.europa.eu/doi/10.2861/536131.
[305] EP Briefing on EU guidelines on ethics in AI, at 5.
[306] EP Briefing on EU guidelines on ethics in AI, at 5.

- **The constructive approach**: in contrast to the first two approaches, which assume that the ADS already exists, the constructive approach is to design ADS taking explainability requirements into account ('explainability by design')

The EU Ethics Guidelines on AI by AI HLEG provides, *inter alia*, check list on explainability:

- Did you assess to what extent the decisions and the outcome made by the AI system can be understood?
- Did you assess to what degree the system's decision influences the organisation's decision-making processes?
- Did you ensure an explanation as to why the system took a certain choice resulting in a certain outcome that all users can understand?
- Did you design the AI system with interpretability in mind from the start?
- Did you research and try to use the simplest and most interpretable model possible for the application in question?
- Did you assess whether you can analyse your training and testing data? Can you change and update this over time?
- Did you assess whether you can examine interpretability after the model's training and development, or whether you have access to the internal workflow of the model?

5.4.3 Proposal for a Regulation laying down harmonised rules on artificial intelligence ("Artificial Intelligence Act") by the EC

On 21st of April, 2021, the European Commission ("EC") published the first ever legal framework on AI, which addresses the risks of AI[307]. The rules are referred to as "Artificial Intelligence Act" ("AI Act") in the Proposed Regulation, and is also referred to as "The EU draft Regulation on AI" or "Drat AI Regulation" by many. This is a legislative proposal by the EC, and is not yet the law of the EU. It will go through the legislative process, and the text of the proposed law is likely to be modified and different when entering into force.

Most importantly, the Draft AI Regulation follows a risk-based approach, and AIs are categorized into three different risk: (1) unacceptable risk; (2) high-risk; (3) limited or minimal risk[308].

Unacceptable risk[309]**.** AI systems raise a clear threat to the safety, livelihoods and rights of people are considered "unacceptable risk." These will be banned. AI systems or applications

[307] See EC, Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://ec.europa.eu/newsroom/dae/items/709090. See also European Data Protection Supervisor, *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*, https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en.

[308] EC, *Europe fit for the Digital Age: Artificial Intelligence* [hereinafter *Europe fit for the Digital Age*], https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682.

[309] Title II of the Draft AI Regulation. See also Explanatory Memorandum, page 12.

that manipulate human behaviour to circumvent users' free will[310] and systems that allow 'social scoring' by governments are categorized as a group of unacceptable risk.

High-risk[311]**.** The Draft AI Regulation identifies two main categories of high-risk AI systems:

1. AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
2. Other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III[312].

Examples include:

- Critical infrastructures (e.g., transport), that could put the life and health of citizens at risk;
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g., scoring of exams);
- Safety components of products (e.g., AI application in robot-assisted surgery);
- Employment, workers management and access to self-employment (e.g., CV-sorting software for recruitment procedures);
- Essential private and public services (e.g., credit scoring denying citizens opportunity to obtain a loan);
- Law enforcement that may interfere with people's fundamental rights (e.g., evaluation of the reliability of evidence);
- Migration, asylum and border control management (e.g., verification of authenticity of travel documents);
- Administration of justice and democratic processes (e.g., applying the law to a concrete set of facts)[313].

These high-risk AI systems can only be placed on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment[314].

High-risk AI systems can be placed on the European market only if complies with the obligations:

- Adequate risk assessment and mitigation systems;
- High quality of the datasets feeding the system to minimise risks and discriminatory outcomes;
- Logging of activity to ensure traceability of results;
- Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;

[310] The Explanatory Memorandum raises "toys using voice assistance encouraging dangerous behaviour of minors" as an example.
[311] Title III of the Draft AI Regulation. See also Explanatory Memorandum, page 13.
[312] Explanatory Memorandum, page 13.
[313] Europe fit for the Digital Age, *supra*.
[314] Explanatory Memorandum, page 13.

- Clear and adequate information to the user;
- Appropriate human oversight measures to minimise risk;
- High level of robustness, security and accuracy.[315]

Limited risk. AI systems that pose limited risk are subject to specific transparency obligations. For example, when using chatbots, users should be aware that they are interacting with a machine so they can take an informed decision to continue or step back[316].

Minimal risk. The Draft AI Regulation does not intervene with minimal risk AI systems (e.g., AI-enabled video games or spam filters).

5.5 Relevance to HosmartAI and SELP

The HosmartAI Project will use AI and robotic technologies to achieve an effective and efficient health care system transformation. AI and robotic technologies will be applied in a wide range of functions and health care tasks, such as screening of high-risk patients, diagnosis systems, personalized rehabilitation and precise treatment, surgical support based on computer modelling and digital twins, assistive care, and the like. More specifically, it will involve AI and robotic technologies or mathematical/statistical techniques, such as deep learning, clustering, natural language processing and conversational robots, robotic and sensor-based devices, and the like.

Considering the fact that various cutting-edge AI/robotic technologies as well as mathematical/statistical techniques will be involved, it would be important and necessary for the Project to follow the principles and guidelines laid out by various instruments provided at the EU level. Specifically, the Ethics and trustworthy AI by AI HLEG would be most relevant to the Project.

5.5.1 Ethics and trustworthy AI by AI HLEG

As discussed in Section 5.4.1, the Expert Group identified a non-exhaustive list of requirements that are helpful in translating the identified principles into practical means of achieving trustworthy AI. To summarise, they are:

1. Human agency and oversight (including fundamental rights, human agency and human oversight);
2. Technical robustness and safety (including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility);
3. Privacy and data governance (including respect for privacy, quality and integrity of data, and access to data);
4. Transparency (including traceability, explainability and communication);
5. Diversity, non-discrimination and fairness (including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation);

[315] Europe fit for the Digital Age, *supra*.
[316] Europe fit for the Digital Age, *supra*.

6. Accountability (including auditability, minimisation/reporting of negative impact, trade-offs and redress); and
7. Environmental and societal well-being (including sustainability and environmental friendliness, social impact, society and democracy).

Considering these requirements, the partners in the Project may wish to consider the following questions:

1. At what stage do humans control and operate AI? Can humans intervene the AI functioning or decision-making?
2. What decisions can AI make during the Project? What are the purposes of those decisions and how are they used?
3. What tools can be used to explain the decision made by AI? What is the most comprehensive way to do so?
4. What technical and organizational measures can be implemented to ensure resilience to attack and security of AI?
5. What level of accuracy does the AI have and how this level is guaranteed?
6. Are the algorithms of AI fair? Is the data fed to AI appropriate, accurate and up-to-date, and not biased?
7. How the mistakes in AI's functioning can be detected?
8. How the mistakes in AI's functioning can be deterred or corrected? How the mistakes can be prevented?
9. What are the roles and responsibilities of all the persons involved into the AI's development, training and operating[317]?

5.5.2 Proposal for a Regulation laying down harmonised rules on artificial intelligence ("Artificial Intelligence Act") by the EC

In addition, the Project should/will pay attention to developments and discussions surrounding the Proposal for a Regulation laying down harmonised rules on artificial intelligence ("Artificial Intelligence Act" or "AIA" for short) by the EC, touched in Section 5.4.3. First and foremost, while subject to changes, the proposed Artificial Intelligent Act may become a law and be legally binding on physical and digital services of the Project. Second, the proposed AIA specifically makes references to AI in health sector. Recital 28, in part, reads:

> AI systems could produce adverse outcomes to **health and safety of persons**, in particular when such systems operate as components of products… [i]n the **health sector** where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers'

[317] See also FASTER, p. 42.

> rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration (emphasis added)[318].

In pertinent part, Recital 45 reads:

> [I]n **health**, the European **health data space** will facilitate non-discriminatory access to **health data** and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance.[319]

Third, it is helpful for the Project to address and reduce various risks that may be raised. The proposed AIA is built upon Ethics and trustworthy AI by AI HLEG[320], and takes "proportionate risk-based approach." The proposed AIA and Annexes would be one of the helpful instruments to identify and evaluate risks of physical or digital services using AI and robotic technologies. Even if physical or digital services by the Project do not fall within the definition of "high-risk AI systems," the obligations provide clear guidance as to essential elements to address potential risks of AI systems, and voluntary compliance with the obligations may help the Project gain trust from the participants and more broadly from the public. Below reiterates the elements that need to be complied before placing high-risk AI systems:

- Adequate risk assessment and mitigation systems;
- High quality of the datasets feeding the system to minimise risks and discriminatory outcomes;
- Logging of activity to ensure traceability of results;
- Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;
- Clear and adequate information to the user;
- Appropriate human oversight measures to minimise risk;
- High level of robustness, security and accuracy

Further, the Annexes to the proposed AIA, can be a benchmark when complying with the elements mentioned above, including detailed documentation, providing clear and adequate information to the user, and conformity with the requirements (including quality

[318] European Commission, 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 (2021), page 24, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.
[319] *Id.*, page 29.
[320] *Id.*, page 8.

management system and control of technical documentation). With these regards, Annex IV[321], Annex V[322], Annex VI[323], Annex VII[324], or Annex VII[325] can be helpful references.

[321] ANNEX IV TECHNICAL DOCUMENTATION referred to in Article 11(1).
[322] ANNEX V EU DECLARATION OF CONFORMITY.
[323] ANNEX VI CONFORMITY ASSESSMENT PROCEDURE BASED ON INTERNAL CONTROL.
[324] ANNEX VII CONFORMITY BASED ON ASSESSMENT OF QUALITY MANAGEMENT SYSTEM AND ASSESSMENT OF TECHNICAL DOCUMENTATION.
[325] ANNEX VIII INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGHRISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 51.

6 Medical Device Regulation

6.1 Introduction

The HosmartAI project aims to integrate and offer two categories of services: (1) **physical** and (2) **digital** services[326], and these services can be subject to the rules and requirements set forth under the EU Medical Regulation. Formerly, the medical devices within the EU were regulated by the following three Directives[327]:

- Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD) (1990)[328]
- Council Directive 93/42/EEC on Medical Devices (MDD) (1993)[329]
- Directive 98/79/EC of the European Parliament and of the Council on in vitro Diagnostic Medical Devices (IVDMD)[330]

Currently, the following two new Regulations are replacing the three existing Directives[331].

- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on **medical devices**, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC[332]; and
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on **in vitro diagnostic medical devices** and repealing Directive 98/79/EC and Commission Decision 2010/227/EU[333] (emphasis added).

The Regulation (EU) 2017/745 ("Medical Devices Regulation" or "MDR" for short) is relevant for the purpose of HosmartAI Project. The MDR entered into force in 2017, but it was planned to begin to apply from 26 May 2020. Due to the coronavirus crisis, however, the Council and the Parliament adopted the Regulation 2020/561 amending Regulation (EU) 2017/745 on medical devices on 23 April 2020 in order to postpone the date of application for most

[326] HosmartAI, at 6 of 70.
[327] EC, Overview | Public Health, https://ec.europa.eu/health/md_sector/overview_en.
[328] Council Directive 90/385/EEC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01990L0385-20071011&locale=en.
[329] Council Directive 93/42/EEC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01993L0042-20071011&locale=en.
[330] Council Directive 93/42/EEC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01993L0042-20071011&locale=en.
[331] Until 2022. See EC, Overview | Public Health https://ec.europa.eu/health/md_sector/overview_en.
[332] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20170505.
[333] REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0746-20170505.

provisions by one year[334]. By virtue of this Regulation 2020/561, the provisions of the MDR will start to apply from 26 May 2021 onward.

6.2 Scope of "Medical Device"

Whether or not MDR applies the device in question depends if the device falls within the definition set forth under the Medical Device Regulation. Article 2 defines "medical device" as:

> *. . . any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of 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.*
>
> - *The following products shall also be deemed to be medical devices:*
> - *devices for the control or support of conception;*
>
> *products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point*[335].

Note that software is explicitly included in the definition.

6.2.1 Intended Purpose

Another critical element is the intended purpose of the device. To qualify as a medical device, the manufacturer must have an intention that the device (including software) to be used for medical purposes. The Court of Justice of the European Union ("CJEU") ruled that a medical device must only satisfy the essential requirements of the directive and bear the CE marking, if its manufacturer expressly intended to market it for medical purposes[336]. Conversely, if a device that *de facto* performs an activity that squarely falls within the letter of the definition -- i.e., it monitors, for instance, blood pressure or heart activity -- but is not intended to be

[334] EC, Overview | Public Health https://ec.europa.eu/health/md_sector/overview_en.
[335] Article 2(1), EU Medical Devices Regulation.
[336] Brain Products GmbH v BioSemi VOF and Others, Case C-219/11, 22 November 2012, OJ C 26 from 26.01.2013, p.7. See also PROTEIN, p. 39.

used for medical purposes by its manufacturer, is not a medical device[337]. In such a case, safety certification as a medical device is not required.

The MDR provides that "software in its own right, *when specifically intended by the manufacturer* to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device" (emphasis added)[338]. Inversely, the MDR provides that "software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device" [339].

6.2.2 Guidance by the MDCG

The Medical Device Coordination Group ("MDCG"), established under Article 103 of the MDR, provides Guidance helpful to determine whether or not a device or software will be subject to the MDR:

- The Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019 ("MDCG 2019-11")[340]
- The Guidance document Medical Devices - Qualification and Classification of stand-alone software ("MEDDEV 2.1/6")[341]
- The Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices ("Manual Borderline Medical Devices")[342]
- Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software March 2020 ("MDCG 2020-1")

6.2.2.1 MDCG 2019-11

MDCG 2019-11 stipulates how "intended purpose" is determined. According to its Guidance, "the use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation" [343].

"Medical device software" is defined as software which is "intended to be used, alone or in combination, for a purpose as specified in the definition of a 'medical device' in the MDR",

[337] See also PROTEIN, p. 39.
[338] Recital 19, EU Medical Devices Regulation.
[339] Recital 19, EU Medical Devices Regulation. See also MDCG 2019-11, p. 6 ("It is important to clarify that not all software used within healthcare is qualified as a medical device. For example, "Simple search", which refers to the retrieval of records by matching record metadata against record search criteria or to the retrieval of information does not qualify as medical device software (e.g. library functions).")
[340] Medica Device Coordinating Group, MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019.
[341] European Commission, *Guidance document Medical Devices - Qualification and Classification of stand alone software*, July 2016 ("MEDDEV 2.1/6"), https://ec.europa.eu/docsroom/documents/17921/attachments/1/translations.
[342] Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (v.1.22), May 2019 ("Manual Borderline Medical Devices"), https://ec.europa.eu/docsroom/documents/35582.
[343] Medica Device Coordinating Group, MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019 ("MDCG" and "MDCG 2019-11" respectively), https://ec.europa.eu/docsroom/documents/37581, p. 3.

i.e., such software must have a medical purpose on its own as described by the manufacturer [344]. Generally, software constitutes "medical device" if it is "intended to process, analyse, create or modify medical information may be qualified as a medical device software if the creation or modification of that information is governed by a medical intended purpose" [345]. Some examples of such software, for instance software that "can directly control a (hardware) medical device (e.g. radiotherapy treatment software), can provide immediate decision-triggering information (e.g. blood glucose meter software), or can provide support for healthcare professionals (e.g. ECG interpretation software)" [346]. The Guidance clarifies that "software may be qualified as [medical device software] regardless of its location (e.g. operating in the cloud, on a computer, on a mobile phone, or as an additional functionality on a hardware medical device)" [347].

Medical device software may be separated into a number of applications or modules, whereby not all modules have a medical purpose. In such a case, only the modules which fall under the description of medical device must comply with the MDR and carry a 'CE' marking, whereas the non-medical device modules are not subject thereto [348]. The MDCG also recommends that such distinction should be clearly identified by the manufacturer based on the intended use and that where "modules which are subject to the medical device regulations are intended for use in combination with other modules of the whole software structure, other devices or equipment, the whole combination, including the connection system, must be safe and must not impair the specified performances of the modules which are subject to the medical device regulations" [349].

6.2.2.2 MEDDEV 2.1/6

MEDDEV 2.1/6 defines the term "stand alone software" as "software which is not incorporated in a medical device at the time of its placing on the market or its making available" [350]. Only if stand alone software has a medical purpose, as intended and described by the manufacturer, will it be qualified as a medical device[351]. It further stipulates that "if the software does not perform an action on data, or performs an action limited to storage, archival, communication, 'simple search' [352] or lossless compression (i.e. using a compression procedure that allows the exact reconstruction of the original data) it is not a medical device" [353].

[344] MDCG 2019-11, p. 6.
[345] MDCG 2019-11, p. 6.
[346] *Ibid*.
[347] MDCG 2019-11, p. 7.
[348] *Id*., pp. 17, 18.
[349] *Id*., p. 18.
[350] MEDDEV 2.1/6, p. 7.
[351] *Ibid.*
[352] Defined as "refers to the retrieval of records by matching record metadata against record search criteria". See MEDDEV 2.1/6, p. 11.
[353] *Ibid*.

Software intended to create or modify medical information might qualify as a medical device "if such alterations are made to facilitate the perceptual and/or interpretative tasks performed by the healthcare professionals when reviewing medical information" [354].

Software might qualify as a medical device if it is "intended to be used for the evaluation of patient data to support or influence the medical care provided to that patient" [355]. For example, decision support software --- software which combines medical knowledge databases and algorithms with patient specific data -- is considered medical devices if it "intended to provide healthcare professionals and/or users with recommendations for diagnosis, prognosis, monitoring and treatment of individual patients" [356]. Conversely, if the information system is intended merely to store, archive and transfer data, it is unlikely to be considered as medical device. However, they may be coupled with additional modules which might be classified in their own right as medical device[357].

6.2.2.3 Manual Borderline Medical Devices

Manual Borderline Medical Devices provides guidance for cases where it is not clear whether or not a device may be classified as a medical device.

For example, a software-based system for information management and patient monitoring, may have a number of functionalities, such as viewing patient information, track changes in patient history, generate audible alerts and a patient-specific alarm filtering function based on severity and type of alarm. If a system has a number of functionalities, each functionality will be reviewed separately to determine if it will be classified as medical device. In the given example, only one function -- the alarm filtering function -- qualifies as a medical device. As the filtering made it possible to delay specific alarms, it was considered that this led to the generation of new or additional information which contributed to the monitoring and follow-up of the patient, thereby making the filter function move beyond a simple search[358].

Finally, it should be noted that, while MDCG-2019-11, MEDDEV 1.2/6 and the Manual Borderline Medical Devices provide useful guidance in determining whether or not a device or software in question will be considered as a medical device subject to the MDR, this guidance is not legally binding because the CJEU has the power to give an authoritative interpretation of the EU law.

6.3 Exception and essential requirements

6.3.1 Exception under Article 5(5)

Generally, when a device is considered a "medical device" under the MDR, it may only be placed on the EU internal market if it complies with the stringent requirements set forth in the MDR, including the general safety and performance requirements set out in Annex I[359].

[354] *Ibid*.
[355] MEDDEV 2.1/6, p. 12.
[356] *Id.*, p. 20.
[357] MEDDEV 2.1/6, p. 20.
[358] Example 9.6, Manual Borderline Medical Devices, p. 80.
[359] Article 5(1), (2), EU Medical Devices Regulation.

The MDR, however, stipulates an exception to its requirements. 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 MDR shall not apply, with the exception of Annex I. In other words, Application of Article 5(5) of the MDR would result in an exemption of the stringent requirements under the MDR, with the exception of Annex I and those set out in Article 5(5).

To benefit from the exception under Article 5(5), the following conditions should be met:

(a) *The devices are not transferred to another legal entity;*
(b) *manufacture and use of devices occur 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;*
    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 therefor.*
(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.*[360]

Again, if facts meet the conditions laid out under Article 5(5) of the MDR, development and use of a medical device within health institutions is permitted without requesting a 'CE' marking.

[360] Article 5(5), EU Medical Devices Regulation.

6.3.2 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[361]. It sets out some general safety and performance requirements[362], requirements regarding design and manufacture[363], as well as regarding necessary information supplied with the device[364].

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[365]. 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[366].

The requirements set out for electronic programmable systems (both devices that incorporate electronic programmable systems and software that are devices themselves)[367] is relevant to our HosmartAI Project. 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." Moreover, 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[368].

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[369]:

[361] Annex I, para. 2, EU Medical Devices Regulation.
[362] *Id*., Chapter I (paras. 1 to 9).
[363] *Id*., Chapter II (paras. 10 to 22).
[364] *Id*., Chapter III (para. 23).
[365] *Id*., paras. 3, 4, 8, 14.
[366] *Id*., para. 15.
[367] *Id*., para. 17.
[368] *Id.*, para. 17.4.
[369] MDCG, *MDCG 2019-16 Guidance on Cybersecurity for medical devices*, December 2019, https://ec.europa.eu/docsroom/documents/38941, p. 5.

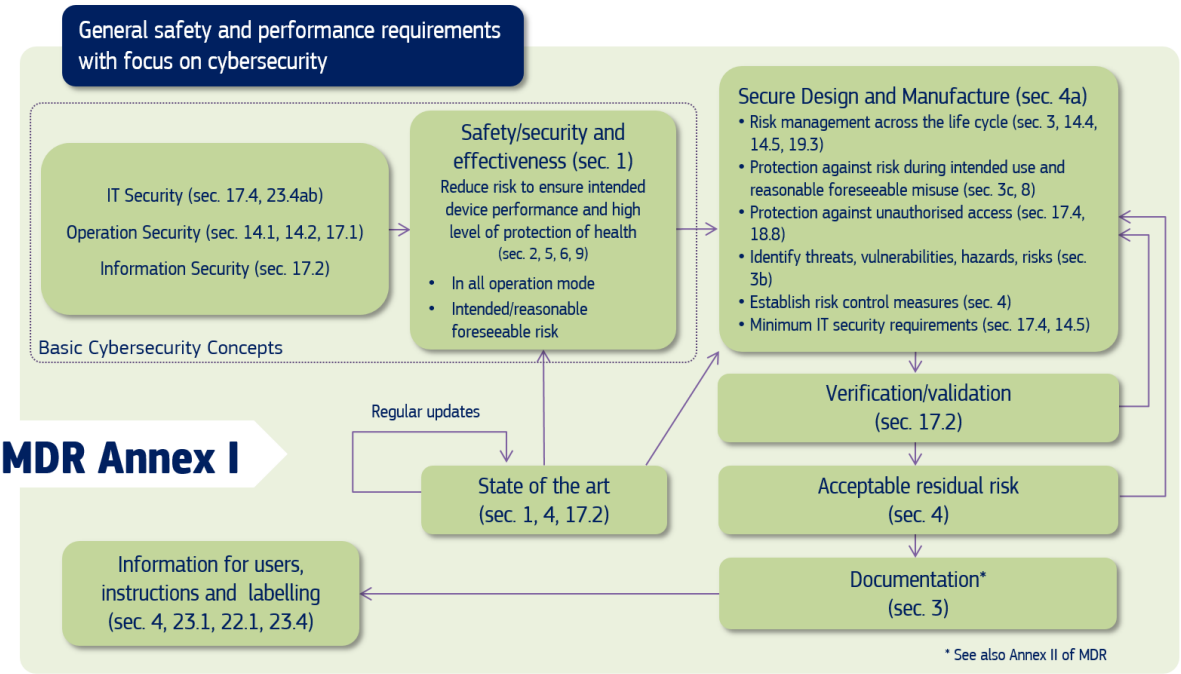


Figure 1: Cybersecurity requirements contained in MDR Annex I

Further requirements related to "active devices" (i.e., the operation of which depends on a source of energy other than that generated by the human body for that purpose)[370] 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[371].

Devices must also be developed in such a way that they protect, as much as possible, users against mechanical and thermal risks[372]. Also, Annex I requires that "devices for use by lay persons" to 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" [373].

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" [374]. If the

[370] Article 2(4), EU Medical Devices Regulation.
[371] Annex I, para. 18, EU Medical Devices Regulation.
[372] *Id.*, para. 20.
[373] *Id.*, para. 22.1.
[374] *Id.*, para. 23.1.

manufacturer has a website, such information should also be included there and kept up to date[375].

For class I and class IIa devices, no instructions for use are necessary in case such devices can be used safely without such instructions[376]. 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[377].

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' [378].

6.4 Classifications

The specific rules and procedures applicable to placing a particular device on the market will depend on the classification of the device. Article 51(1) of the MDR provides that all devices "shall be divided into classes I, IIa, IIb and III, taking into account the intended purpose of the devices and their inherent risks". Classification rules are based on the vulnerability of the human body and need to take into consideration "potential risks associated with the technical design and manufacture of the devices" [379] and are set out in Annex VIII of the MDR. Of the different classes, class I is generally considered the least invasive type of device. Classes increase as the risk associated with the device increases[380]. The higher the class, the stricter the rules that apply to them.

With regard to the classification of software, Annex VIII of the MDR provides:

- ***Class I****: all other software not covered below;*
- ***Class IIa****: software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes, or software to monitor physiological processes;*
- ***Class IIb****: software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes when such decisions have an impact that may cause a serious deterioration of a person's state of health or a surgical intervention, or software to monitor physiological processes intended for monitoring vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient;*

[375] *Ibid*.
[376] Annex I, para. 23.1(d), EU Medical Devices Regulation.
[377] *Id*., para 23(4)(q).
[378] *Id*., para. 23(20(q).
[379] Recital 58, EU Medical Devices Regulation.
[380] See Annex VIII, EU Medical Devices Regulation.

- ***Class III**: software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes when such decisions have an impact that may cause death or an irreversible deterioration of a person's state of health.*[381]

In the event of a dispute between the manufacturer and the relevant notified body[382], regarding the application of Annex VIII, the competent authority of the Member State in which the manufacturer has its registered place of business will decide[383].

The class of the medical device will determine the subsequent procedures that will apply, including the conformity assessment[384].

6.5 Conformity assessment

Article 52(1) of the MDR requires that, before placing a device on the internal market, the manufacturer shall undertake an assessment of conformity in accordance with the procedures set out in Annexes IX and X to the Regulation. Article 2(40) of the MDR describes the conformity assessment as "the process demonstrating whether the requirements of this Regulation relating to a device have been fulfilled."

Annex IX sets out the rules of the conformity assessment based on a quality management system implemented by the manufacturer and on the assessment of technical documentation. Annex X covers conformity assessments based on type-examination, which is the procedure whereby the notified body determines whether a device fulfils the requirements under the MDR.

The scope of obligations in terms of the conformity assessment depends on the classification of the device. For class I devices, conformity assessments are generally conducted under the sole responsibility of the manufacturer in light of the low level of vulnerability associated with such devices. In contrast, for class IIa, IIb and III devices, a certain level of involvement from the notified body is compulsory[385].

Upon completion of the conformity procedure, medical devices can be 'CE' marked and put into circulation[386].

6.6 Clinical evaluation and investigation

6.6.1 Clinical evaluation

Article 5(3) of the MDR requires that a demonstration of conformity of a device with the general safety and performance requirements under Annex I shall include a clinical evaluation in accordance with Article 61 and Part A of Annex XIV of the MDR, performed by the

[381] Rule 11, para. 6.3, Annex VIII, EU Medical Devices Regulation.
[382] See Section 4.7.
[383] Article 51(2), EU Medical Devices Regulation.
[384] See FASTER, p. 37.
[385] Recital 60, EU Medical Devices Regulation.
[386] See PROTEIN, p. 41; FASTER, p. 38.

manufacturer [387]. A clinical evaluation means "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" [388].

The type and amount of clinical data needed to demonstrate conformity with the general safety and performance requirements will depend on the characteristics of the device as well as its intended use[389]. According to Article 2(48) of the MDR, clinical data "means information concerning safety or performance that is generated from the use of a device." Conducting a clinical evaluation will reveal: (1) which clinical data is necessary; (2) "which clinical data can be adequately supplemented by other methods, such as literature search, prior clinical investigations, clinical experience or by using suitable clinical data from equivalent devices; and (3) which clinical data remain to be delivered by clinical investigations" [390].

The clinical evaluation and its documentation are required to be conducted throughout the life cycle of a device[391]. "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" [392].

A number of stages are identified in the performance of a clinical evaluation:

Table 10: Steps to perform in a clinical evaluation

Stage 0	Define the scope, 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 on rare complications, long term performance, safety under wide-spread use), whether these are acceptable for CE-marking, and whether they are required to be addressed during post-market surveillance.

[387] Article 10(3), EU Medical Devices Regulation.
[388] *Id*., Article 2(44).
[389] *Id*., Article 61(1). See also European Commission, Guidelines on Clinical Investigation: A Guide for Manufacturers and Notified Bodies, MEDDEV, 2.7/4, December 2010 ("MEDDEV 2.7/4"), see https://ec.europa.eu/docsroom/documents/10336/attachments/1/translations/en/renditions/native (accessed on 16 February 2020), p. 6.
[390] MEDDEV 2.7/4, p. 7. For more on clinical investigations, see Section 5.6.2.
[391] See Article 61(11), EU Medical Devices Regulation; MEDDEV 2.7/1, p. 10.
[392] See MEDDEV 2.7/1, p. 10. See also FASTER, p. 39.

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[393].

6.6.2 Clinical Investigation

Article 61(4) of the MDR requires, in general, a clinical investigation to be performed for implantable devices and class III devices. Furthermore, "[d]epending on clinical claims, risk management outcome and on the results of the clinical evaluation, clinical investigations may also have to be performed for non-implantable medical devices of classes I, IIa and IIb" [394].

A clinical investigation is "any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device" [395]. The requirements for the conduct of a clinical investigation are set out in Article 62 to 81 and Annex XV of the EU MDR. In general, a clinical investigation must:

- be part of the clinical evaluation process;
- follow a proper risk management procedure to avoid undue risks;
- be compliant with all relevant legal and regulatory requirements;
- be appropriately designed;
- follow appropriate ethical principles.[396]

Clinical investigations, where carried out as part of a clinical evaluation for conformity assessment purposes, shall be carried out for a specific purpose, including "to establish and verify the clinical benefits of a device as specified by its manufacturer" or "to establish and verify the clinical safety of the device and to determine any undesirable side-effects, under normal conditions of use of the device, and assess whether they constitute acceptable risks when weighed against the benefits to be achieved by the device" [397].

"The design of the clinical investigation . . . should provide the clinical data necessary to address relevant aspects of clinical performance, safety, including undesirable side-effects as well as the residual risks identified in the risk management process" [398]. They 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" [399].

[393] MEDDEV 2.7/1, p. 13. See also FASTER, p. 40.
[394] MEDDEV 2.7/4, p. 7.
[395] *Id*., Article 2(45).
[396] MEDDEV 2.7/4, p. 7.
[397] Article 62(1)(b) & (c), Medical Devices Regulation.
[398] MEDDEV 2.7/4, p. 8.
[399] Article 62(3), Medical Devices Regulation.

Importantly, clinical investigations are subject to scientific and ethical review. The latter must be performed by an ethics committee in accordance with national law[400].

A sponsor means "any individual, company, institution or organisation which takes responsibility for the initiation, for the management and setting up of the financing of the clinical investigation" [401]. The sponsor of the clinical investigation should be established in the EU or ensure that they have a legal representative established in the EU[402].

The sponsor of a clinical investigation is required to submit an application for assessment to the relevant Member State where the clinical investigation will be conducted[403]. If the application is validated by the Member State, unless otherwise stated in national law and provided that no negative opinion from an ethical committee is received, the sponsor may start the clinical investigation for investigational class I devices or in the case of non-invasive class IIa and class IIb devices[404]. In case of other investigational devices, the sponsor may only commence the clinical investigation once an authorisation from the Member State is received and provided that no negative opinion from the relevant ethical committee is received[405]. In their assessment, Member States shall consider "whether the clinical investigation is designed in such a way that potential remaining risks to subjects or third persons, after risk minimisation, are justified, when weighed against the clinical benefits to be expected" [406]. In the event of a clinical investigation that is to be conducted in multiple Member States, the sponsor may submit a single application for assessment. Via the electronic system used for applications for assessment of clinical investigations, such an application is transmitted electronically to all Member States in which the clinical investigation is to be conducted[407]. In such an application, the sponsor will propose which Member State acts as Coordinating Member State, under whose direction the concerned Member States will then coordinate their assessment of the application[408].

6.7 The 'CE' ('Conformité Européenne') marking

Article 2(43) of the MDR defines CE ('Conformité Européenne') marking as "a marking by which a manufacturer indicates that a device is in conformity with the applicable requirements set out in this Regulation and other applicable Union harmonisation legislation providing for its affixing." All devices, other than custom-made or investigational devices, that are in conformity with the requirements set out by the MDR shall bear the CE marking[409].

[400] *Ibid.*
[401] *Id.*, Article 2(49).
[402] Article 62(4)(c) & (2), EU Medical Devices Regulation.
[403] Article 70(1), EU Medical Devices Regulation.
[404] *Id.*, Article 70(7)(a). An investigational device is a "device that is assessed in a clinical investigation" (see Article 2(46), EU Medical Devices Regulation).
[405] *Id.*, Article 70(7)(b).
[406] *Id.*, Article 71(3).
[407] *Id.*, Article 78(1).
[408] *Id.*, Article 78(2) & (3).
[409] Article 20(1), EU Medical Devices Regulation.

Article 20(3) and (4) of the MDR requires that, before the device is placed on the market, the CE marking be affixed to the device (or its sterile packaging) "visibly, legibly and indelibly" and that it will appear in instructions as well as on sales packaging. Where a notified body has been involved in the conformity assessment, the CE marking must be followed by the identification number of the notified body[410].

6.8 National notified bodies

Authorities responsible for the conformity assessment and related procedures are established at the Member State level[411]. There are two types of relevant authorities with regard to conformity assessments: (1) authorities responsible for notified bodies; and (2) the notified bodies themselves. The former oversees the notified bodies as is provided for in Article 35(1) of the MDR, which provides that "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 under this Regulation shall appoint an authority ('authority responsible for notified bodies')". The latter, defined as "a conformity assessment body designated in accordance with this Regulation" [412] is a body that "performs third-party conformity assessment activities including calibration, testing, certification and inspection and designated in accordance with the Regulation on medical devices" [413].

6.9 Relevance to HosmartAI and SELP

6.9.1 Exception under Article 5(5) of the MDR

The first question that the HosmartAI Project, or each partner, can ask is whether it aims to make sure the facts will meet the conditions laid out under Article 5(5). This is especially useful if HosmartAI partners wish to avoid, at this stage, the full application of the strict requirements under the MDR. Alternatively, it can opt for the full conformity assessment process from an early stage of the Project, following a decision that a particular device is a "medical device" under the MDR.

As a practical matter, this Report assumes that the HosmartAI Project does not have an immediate intention to bring the devices into the market; rather, exploitation is considered at the later stage or at the end of the project. If so, it is likely that the Project would fit under the exception 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, provided that facts indeed meet the conditions set forth (see Section 6.3.1).

6.9.2 Exploitable products

The second question relevant to HosmartAI Project is, when it will bring its products into the market (intended as a "medical device"), and what needs to be done in order to place them

[410] Article 20(5), EU Medical Devices Regulation.
[411] See FASTER, p. 38.
[412] Article 2(42), EU Medical Devices Regulation.
[413] FASTER, p. 39.

into the market. While the first part of the question is a decision-making issue, the answer to the second part of the question is a compliance issue.

Under the MDR, any medical devices of HosmartAI will 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 post-market surveillance; and market surveillance), as discussed above[414].

The obligations under the Medical Devices Regulation 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 [415]. Obligations are also foreseen for importers, distributors and, in some instances, other persons[416].

[414] See also FASTER, p. 36.
[415] Article 11, EU Medical Devices Regulation.
[416] See Articles 13, 14, 16.

7 References

7.1 Primary sources

7.1.1 International treaties

- United Nations General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
- United Nations Educational, Scientific and Culture Organisation ("UNESCO"), Universal Declaration on Bioethics and Human Rights, 19 October 2005.
- United Nations General Assembly, Universal Declaration of Human Rights, 10 December 1948.

7.1.2 EU treaties and other instruments

- EU 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.
- EU Regulation No. 536/2014 of the European Parliament and of the Council of 14 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.
- EU Regulation No. 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) 1223/2000 and repealing Council Directives 90/385/EEC and 93/42/EEC.
- EU Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.
- EU Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- EU Regulation 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).
- Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, 4 April 1997, ETS No. 164.
- Council of Europe, Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, 25 January 2005, CETS No. 195.
- Council of Europe, European Social Charter (revised), 3 May 1996, ETS No. 163.
- Council of Europe, Recommendation No. R(99)4 of the Committee of Ministers of the Member States on Principles Concerning the Legal Protection of Incapable Adults, 23 February 1999.
- Council of Europe, Explanatory Memorandum – Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults, 23 February 1999.
- Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.

- European Parliament, Council and Commission, Charter on Fundamental Rights of the European Union, 7 December 2000.
- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 28 January 1981.
- EU, Treaty on the Functioning of the European Union, 25 March 1957.

7.1.3 National legislation

- Bundesdatenschutzgesetz (or Data Protection Amendment Act), which implements the new German Federal Data Protection Act, was passed on 5 July 2017 and entered into force on 25 May 2018.
- Legislative Decree no. 101 of 10 August 2018, published in the Official Journal on 4 September 2018.
- Italian Data Protection Authority, General Application Order Concerning Biometrics as of November, 2014.
- Italian Data Protection Authority, Guidelines on Processing Personal Data to Perform Customer Satisfaction Surveys in Healthcare Sector as of May 5, 2011.
- Italian Data Protection Authority, Authorization №2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life as of December 30, 2014.
- Italian Data Protection Authority, Guidelines on the Electronic Health Record and the Health File as of July 16, 2009.
- Italian Data Protection Authority, General Authorization №8/2012 for the Processing of Genetic Data as of December 13, 2012.
- Personal Data Protection Act (Official Gazette of the Republic of Slovenia, no. 86/04, 113/05, 51/07, 67/07 and 94/07; Zakon o varstvu osebnih podatkov), originally adopted in 2004, and subsequently amended a number of times, entered into force in 2007.
- Patient Rights Act (Official Gazette of the Republic of Slovenia, no. 15/08 and 55/17; Zakon o pacientovih pravicah).
- Health Services Act (Official Gazette of the Republic of Slovenia, no. 23/05, 15/08, 23/08, 58/08, 77/08, 40/12, 14/13, 88/16 and 64/17; Zakon o zdravstveni dejavnosti).
- Rules on the Composition, Tasks, Competencies and Manner of Work of the Medical Ethics Commission of the Republic of Slovenia (Official Gazette RS, Nos. 30/95, 69/09, 47/17, 64/17 - ZZDej-K and 21/18), 1995 (last updated 23 March 2018).
- Healthcare Databases Act (Official Gazette of the Republic of Slovenia, no. 65/00 and 47/15).
- Law No. 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) and Transposing into National Law Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) and Other Provisions (“Greek Law 4624/2019”)
- The Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data (“the GDPR Implementing Law”)
- The Act of 3 December 2017 Establishing the Data Protection Authority ('the DPA Law')

7.1.4 Case law

- CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015.
- Brain Products GmbH v BioSemi VOF and Others, Case C-219/11, 22 November 2012, OJ C 26 from 26.01.2013.

7.2 Secondary sources

7.2.1 Codes & guidelines

- World Medical Association, Declaration of Helsinki – Ethical principles for medical research involving human subjects (June 1964, and most recently amended October 2013).
- Trials of War Criminals before the Nuremberg Military Tribunals, under Control Council Law No. 10, Vol. 2, pp. 181-182, Washington, D.C.: U.S. Government Printing Office (1949) (Nuremberg Code).
- Council for International Organizations of Medical Sciences in collaboration with the World Health Organisation, International ethical guidelines for health-related research involving humans, (1982, and most recently amended in 2016).
- International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Guideline for Good Clinical Practice, 10 June 2996.
- World Health Organisation, Handbook for Good Clinical Research Practice, 2005.
- L. S. Sulmasy, T. A. Bledsoe, for the ACP Ethics, Professionalism and Human Rights Committee, American College of Physicians Ethics Manual: Seventh Edition, Ann Intern Med., (2019).

7.2.2 Books and articles

- Hippocrates, The history of epidemics, Samuel Farr (trans.), London: T. Cadell (1780).
- A.M. Lachapelle-Henry, P. D. Jethwani, M. A. Grodin, The complicated legacy of the Nuremberg Code in the United States, in: Medical Ethics in the 70 Years after the Nuremberg Code, 1947 to the Present, Czech, H., Druml, C. & Weindling, P (eds.), Wien Klin Wochenschr 130, 180 (2018).
- T. L. Beauchamp, J. F. Childress, Principles of biomedical ethics, Oxford University Press, USA, 2001.
- Garrett et. al., Health Care Ethics, Prentice Hall, 2nd Edition (1993).
- R. Gillon, Beneficence: doing good for others, British Medical Journal Vol. 291, 6 July 1985.
- S. Jansen, Recommendation No. R(99)4 of the Committee of Ministers to Member States on Principles concerning the Legal Protection of Incapable Adults, and Introduction in Particular to Part V Interventions in the Health Field, 7 Eur. J. Health L. 333 (2000).
- C. Coglianese and D. Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, Penn Law: Faculty Scholarship Repository, 1734, (2017).

- A. Kiseleva, 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, July 2019.
- S. D. Warren & L. D. Brandeis, The Right to Privacy, Harvard Law Review Vol. 4, No. 5, 1890.
- P. de Hert & S. Gutwirth, Privacy data protection and law enforcement. Opacity of the individual and transparency of power, in Privacy and the Criminal Law, E. Claes et al. (eds), 2006.
- D. J. Solove, Understanding Privacy, Cambridge Massachusetts: Harvard University Press, 2008.
- R. C. Post, Three Concepts of Privacy, Faculty Scholarship Series (Paper 185), 2001.
- European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018 edition.
- P. Quinn, The Anonymization of Research Data – A Pyric Victory for Privacy that Should not be Pushed Too Hard by the EU Data Protection Framework?, European Journal of Health Law (2017).
- Jadek & Pensa Law Firm (Slovenia), The Slovenian Personal Data Protection Act (ZVOP-2) proposal – overstepping the GDPR boundaries?, 20 March 2018.
- Rojos Peljhan Prelesnik & Partners Law Firm (Slovenia), Analysis of the Slovenian GDPR Implementation Law in Light of its Main Deviations from, or Supplements to, Default Rules Set out in the GDPR, 6 May 2019.

7.2.3 Reports and other sources

- P. Quinn, E. Mantovani, A. van Scharen (VUB), PROTEIN, D10.1 Report on security, data protection, privacy, consumer protection, ethics and social acceptance (TARESS Framework) (2019).
- eHealth Network, Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU (General Guidelines), 21 November 2016.
- eHealth Network, Patient Summary Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU (Patient Summary for unscheduled care), 21 November 2016.
- High Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence, 8 April 2019.
- European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence (“Artificial Intelligence Act”)
- A. Kiseleva, P. Quinn (VUB), FASTER, D2.1 Benchmark Report on Social, Legal, Ethical and Policy Frameworks, 31 August 2019.
- S. Roda, I. Böröcz, Ioulia Konstantinou (VUB), HR-RECYCLER, D2.1 Report on Security, data protection, privacy, ethics and societal acceptance, 7 June 2019.
- Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017 (last revised on 1 April 2018).
- Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011.

- P. Quinn, P. de Hert (VUB), PICASSO, D3.5 Privacy Compliance Laws Associated with Surveillance, 22 December 2017.
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.
- Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017.
- Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010.
- European Parliament, Report with Recommendations on Civil Law Rules on Robotics, 27 January 2017.
- Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2018 (last revised 6 February 2018).
- PWC, Reform of German data protection legislation: Second EU Data Protection Amendment and Implementation Act passed, 23 September 2019.
- Analytics Framework for Integrated and Personalised Healthcare Services in Europe (AEGLE), AEGLE in Your Country – Slovenia, 30 March 2018.
- DLA Piper, Data Protection Laws of the World – Slovenia, 14 January 2020.
- European Committee for Standardization (“CEN”), CEN Workshop Agreement 17502, Privacy of monitoring technology— Guidelines for introducing ambient and wearable monitoring technologies balancing privacy protection against the need for oversight and care, February 2020.
- Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software March 2020 (“MDCG 2020-1”)
- Medica Device Coordinating Group, MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, October 2019.
- Medica Device Coordinating Group, MDCG 2019-16 Guidance on Cybersecurity for medical devices, December 2019.
- European Commission, Guidance document Medical Devices - Qualification and Classification of stand alone software, July 2016 (MEDDEV 2.1/6).
- Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (v.1.22), May 2019.
- European Commission, Guidelines on Clinical Investigation: A Guide for Manufacturers and Notified Bodies, MEDDEV, 2.7/4, December 2010 (MEDDEV 2.7/4).