Co-funded by the Horizon 2020
Framework Programme of the European Union

D1.1 – Fundamental Rights, Ethical and Legal Implications, and Assessment

Work Package 1: Data Protection, Ethical Impact and Interoperability

affecTive basEd iNtegrateD carE for betteR Quality of Life: TeNDER Project

Grant Agreement ID: 875325

Start date: 1 November 2019

End date: 31 October 2022

Funded under programme(s): H2020-SC1-DTH-2018-2020/H2020-SC1-DTH-2019

Topic: SC1-DTH-11-2019 Large Scale pilots of personalised & outcome-based integrated care

Funding Scheme: IA - Innovation action

Disclaimer

The TeNDER consortium consists of the following Partners.

Table 1 - Consortium Partners List

No	Name	Short name	Country
1	UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
2	MAGGIOLI SPA	MAG	Italy
3	DATAWIZARD SRL	DW	Italy
4	UBIWHERE LDA	UBIWHERE	Portugal
5	ELGOLINE DOO	ELGOLINE	Slovenia
6	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
7	VRIJE UNIVERSITEIT BRUSSEL	VUB	Belgium
8	FEDERATION EUROPEENNE DES HOPITAUX ET DES SOINS DE SANTE	HOPE	Belgium
9	SERVICIO MADRILENO DE SALUD	SERMAS	Spain
10	SCHON KLINIK BAD AIBLING SE & CO KG	SKBA	Germany
11	UNIVERSITA DEGLI STUDI DI ROMA TOR VERGATA	UNITOV	Italy
12	SLOVENSKO ZDRUZENJE ZA POMOC PRI DEMENCI - SPOMINCICA ALZHEIMER SLOVENIJA	SPO	Slovenia
13	ASOCIACION PARKINSON MADRID	APM	Spain

Document Information

Project short name and Grant Agreement ID	TeNDER (875325)
Work package	WP.1
Deliverable number	D1.1
Deliverable title	Fundamental Rights, Ethical and Legal Implications and Assessment (First Version)
Responsible beneficiary	VUB
Involved beneficiaries	ALL
Type[1]	Report
Dissemination level[2]	PU
Contractual date of delivery	30 March 2020
Last update	25 March 2020

[1] **R:** Document, report; **DEM:** Demonstrator, pilot, prototype; **DEC:** Websites, patent fillings, videos, etc.; **OTHER**; **ETHICS**: Ethics requirement; **ORDP**: Open Research Data Pilot.
[2] **PU:** Public; **CO:** Confidential, only for members of the consortium (including the Commission Services).

Document History

Version	Date	Status	Authors, Reviewers	Description
v0.00	03/12/2019	Template	Paride Criscio	Project deliverable template
v0.01	21/01/2020	Draft	Lisa Feirabend (VUB)	Structure, table of contents
v0.02	29/01/2020	Draft	Lisa Feirabend (VUB)	First draft
v0.03	17/02/2020	Draft	Paul Quinn (VUB)	Internal Review
v0.04	21/02/2020	Draft	Lisa Feirabend, Paul Quinn (VUB)	Revised draft incorporating comments
v0.05	19/03/2020	Draft	Lisa Feirabend (VUB)	Sent draft to partners for internal review
v0.06	25/03/2020	Draft	Annelore Hermann (UPM)	Internal Review
v0.07	29/03/2020	Draft	Gustavo Hernández (UPM)	Final review and format for submission

Acronyms and Abbreviations

Acronym/Abbreviation	Description
AI	Artificial intelligence
EU	European Union
GDPR	General Data Protection Regulation
Mx	Month (where x defines a project month e.g. M8)
TeNDER	affecTive basEd iNtegrateD carE for betteR Quality of Life
Tx.x	Task
WPx	Work Package

Table of Contents

List of Figures

List of Tables

Executive Summary

The main aim of the TeNDER project is to develop an integrated care model to manage multi-morbidity in persons with neurodegenerative and cardiovascular diseases. The expectation is that by addressing the difficulties experienced by this group in independent living and other care arrangements, the TeNDER system will contribute to an increased quality of their life as well as that of their family and others in their care pathway. The TeNDER project intends to use a number of mobile, wearable and other sensorial technologies, including smart wristbands, sensors and scanners, home safety devices, microphones and mobile devices. The data collected by the use of these technologies is intended to feed into the TeNDER system which will process the information, including with the use of AI algorithms, and result in personalised models for each user to identify abnormalities, raise alerts for rapid intervention in case of need, and make personalised recommendations for the user's care plan.

The present report will summarise the main findings of T1.1, which focusses on identifying, adapting and defining a complete overview of the main requirements with regard to fundamental rights for data protection and privacy, as well as social and functional acceptance of ICT solutions for integrated care. The context of this analysis, unless explicitly stated, is mainly limited to the project's research activities. This report will serve as a basis to inform the subsequent development phases of the TeNDER project, especially in connection to the development of the TeNDER ecosystem and the implementation of the pilots.

The main findings of this report are related to the participation of humans in research and other ethical and societal concerns, the impact of the TeNDER project on fundamental rights, as well as the relevance of the medical devices framework.

As the TeNDER project intends to conduct large scale pilots with human participants, the principles of medical ethics are of great importance, including the principle of autonomy, beneficence and non-maleficence, and justice. These principles should guide TeNDER partners when conducting the pilots. Some key findings:

- *Of particular relevance is the notion of informed consent, a cornerstone of the principle of autonomy, which should be obtained from all research participants. Such consent should be given freely, specific, informed and a reflection of the participant's wishes.*
- *As the TeNDER project intends to engage potentially vulnerable groups (older persons, persons with chronic illness, including neurodegenerative diseases, and those unable to give informed consent), it is important to note that the TeNDER project is in line with international norms which specify that medical research with vulnerable groups should be responsive to the particular needs of that group and that it cannot be carried out in a non-vulnerable group.*
- *The TeNDER project will put in place specific safeguards and protections to minimise the risk for these particular vulnerable groups, as advised by the same international norms.*

In addition to the participation of vulnerable groups in scientific research, there are a number of other societal and ethical concerns that need to be considered in the context of the TeNDER project, including the use of new technologies, their acceptance by the society and trust in such technologies is something to assess and consider. Some key findings:

- *The main issue in the use of new technologies (including artificial intelligence, as well as mobile and wearable technologies) is to gain and preserve trust in using them. For that reason, TeNDER partners shall assess the technologies and develop ways to achieve this. In particular, understanding the technology and its use, as well as the implementation of technical and organisational means to ensure safety and the respect of fundamental rights, would enable society to trust technology and, in turn, the TeNDER project.*
- *It will be important for TeNDER partners to consider whether the technology proposed to be used during the pilots has a risk of infringing upon the rights of others, including family members sharing the home, visitors to the home, as well as other patients, staff or visitors in the hospital, day care centre or rehabilitation room (especially where those technologies could capture image/ movement/ sound). If it is determined that there is indeed a risk, the partners will have to consider measures to mitigate such risks to ensure that the rights of the persons involved in the pilots are balanced against fundamental rights and vital interests of other persons that might be affected by the implementation of the TeNDER system.*

As the TeNDER project will include large-scale pilots with human participants and the collection and processing of different types of data, it is important to consider how this may affect the fundamental rights of those involved, in particular the right to privacy and the right to data protection. Some key findings:

- *In terms of the right to privacy in the context of the TeNDER project, it will be important to find a right balance between the fundamental right to privacy of the participants in the pilots (and possibly people around them), and other interests, including the expected benefits of the proposed TeNDER system (i.e. an increased quality of life for users as well as that of their family and others in their care pathway).*
- *As for the right to protection of personal data, the types of data identified in this report that TeNDER partners intend to collect and process fall within the definition of either personal or sensitive data, thereby invoking the application of the GDPR.*
- *The legal basis for processing of personal and sensitive data in the TeNDER project is consent pursuant to Article 6(1)(a) of the GCPR and explicit consent pursuant to Article 9(2)(a) of the GDPR respectively.*
- *The TeNDER project intends to utilise various new technologies and it is recommended that a data protection impact assessment is conducted to an assess the impact of the envisaged processing operations on the protection of personal data.*
- *As some of the TeNDER partners are jointly involved in determining the purpose and means of processing personal data in the context of the TeNDER project, they will be considered joint data controllers.*

Finally, the relevance of the EU Medical Devices Regulation is considered in the context of the TeNDER project. Some key findings:

- *As some of the intended services of the TeNDER system might move beyond storage, archival, communication, 'simple search' or lossless compression, this might result in, at least these modules, to be considered a medical device, invoking the application of the EU Medical Devices Regulation.*
- *At this stage, it is possible to make a distinction between 'TeNDER the research project' and 'TeNDER the exploitable product' as it relates to the applicability of the EU Medical Devices Regulation. The selected approach will determine the extent to which the EU Medical Devices Regulation will apply to the TeNDER project.*

1. Introduction

Europe's growing population has faced significant demographic changes over the past years, including a rapidly growing ageing population. The increasing number of Europeans affected by cognitive impairments, such as Parkinson's disease ("PD"), Alzheimer's disease and other forms of dementia (together "AD"), as well cardiovascular diseases ("CVDs"), has become a major social and health issue.

While many elderly, including those with PD, AD and CVD, prefer to remain living at home, symptoms of PD, AD and CVD can cause significant difficulties in living independently and arranging their own care. To face these challenges, there is a need to develop new integrated care models for the management of co-morbidity, and to make them personalised and patient-centred. In light of this need, TeNDER, a multi-sectoral project funded by the EU Framework Programme for Research and Innovation, Horizon 2020, will develop an integrated care model to manage multi-morbidity in persons with neurodegenerative and cardiovascular diseases.

TeNDER will perform five large-scale pilots that will target persons who with AD, PD, and CVDs, alongside chronic illnesses. The aims of these pilots are to verify the technological acceptance of the TeNDER system, to demonstrate the feasibility of the implementation of the TeNDER system as an integrated care model, and to gather user feedback which will inform the product design.[3]

The researchers working in the TeNDER project will engage with human participants, including potentially vulnerable groups: older persons, persons with chronic illnesses, including neurodegenerative and cardiovascular diseases, and those unable to give informed consent. From these groups, the TeNDER partners will collect and process data, including potentially personal and sensitive data. In order to ensure that the TeNDER project runs in accordance with recognised legal rules and ethical norms, it is necessary to identify the relevant frameworks and normative conditions. Such is also required by Article 34 of the Grant Agreement ("GA"), which requires that "the beneficiaries must carry out the action in compliance with: (a) ethical principles (including the highest standard of research integrity) and (b) applicable international, EU and national law."[4]

The tasks under WP1 of the TeNDER project will ensure that the project and the TeNDER ecosystem are developed in line with the relevant rules and regulations in terms of data privacy, security, integrity and interoperability. As part of WP1, the present report will summarise the main findings of T1.1, which focusses on identifying, adapting and defining a complete overview of the main requirements with regard to fundamental rights to data protection and privacy, as well as social and functional acceptance of ICT solutions for integrated care. This report will serve as a basis to inform the subsequent development phases of the TeNDER project, including within WP1 (e.g. the development of a standard tool for integrated information gathering under T1.2 in line with the relevant rules on the processing of personal data) and for the other WPs, in connection to the development of the TeNDER ecosystem and the conduct of the pilots. Furthermore, this report will form the basis for the continuous review and monitoring of the TeNDER project, to ensure compliance with the relevant frameworks under T1.3.

[3] Grant Agreement ("GA"), Annex 1, Part A, p. 27.
[4] Article 34(1) (Ethics and Research Integrity), GA.

Section 2 of this report will present the conditions related to the engagement of human participants.[5] It will set out the relevant frameworks and ethical principles to consider when conducting research with human participants. In particular, it will set out the relevant considerations in relation to the principle of informed consent, including in relation to vulnerable groups and those adults unable to provide consent. Section 3 will explore the various ethical and societal concerns that might affect the activities and expected outputs of the TeNDER project, including concerns related to the use of AI and mobile and wearable technologies. Section 5 will consider the relevant fundamental rights, including the right to privacy and the right to protection of personal data. It will set out the relevant framework related to the collection and processing of personal data, including the European framework and relevant national laws. As the TeNDER project involves the use of various innovative technologies, this section provides an analysis of how these technologies might influence the protection of personal data and privacy, including the use of artificial intelligence capacities for automated decision-making. Finally, Section 5 will also consider the regulations related to medical devices and its potential implications for the TeNDER project.[6] It will define the term 'medical device', consider the TeNDER project in context of this definition, and set out the process under the relevant framework and its implications for the TeNDER project.

[5] This section relies on experience gained by the VUB through its involvement in the PROTEIN project, funded under Horizon 2020.

[6] Sections 3 to 5 will rely on experience gained by the VUB through its involvement in the PROTEIN, FASTER, Picasso and HR-Recycler projects, all funded under Horizon 2020.

2. Human Participants

2.1 Introduction

The pilots testing the TeNDER system are scheduled to commence in M13 of the project. During the pilots, partner organisations will test and evaluate the usability, performance and compliance of the TeNDER system against the requirements gathered in the phase of technology development.

In each TeNDER pilot setting (i.e. hospital, at home, and rehabilitation or day-care centres), research participants will be monitored using various different technologies, including sensors, microphones, 3D sensors that capture movement, affective recognition technology, and wristbands that record basic vitals.

There will be three groups of research participants. The first group will be patients under medical supervision in health care institutions such as hospitals, medically supervised rehabilitation or day-care centres. The second group consists of persons with PD, AD and CVDs in a home setting. The final group consists of those in the care pathway of people with AD, PD and/or CVDs: health professionals, social workers, caregivers (professional and informal) and others (administrative staff, hospital IT, day-care centre workers, etc.).

The following paragraphs will set out the conditions that should be taken into account when conducting pilots or tests with human participants.

2.2 Relevant legislative framework for TeNDER research

When considering the relevant legislative framework in connection to the TeNDER research, a distinction should be made between testing medicinal products on humans and other tests that observe humans or assess medical devices.[7] This distinction is relevant to the applicable law. Although research participants involved in the TENDER project may well be users of medicinal products, this will be in the course of their existing treatment and is not something the project itself will be covering, other than offering reminders for participants to take their medication and monitoring medication intake through the use of pill dispensers. As TeNDER will not test a medicinal product with human participants, EU legislation applicable to this type of trial, the EU Clinical Trial Directive[8] and its successor the EU Clinical Trials Regulation,[9] are therefore not directly applicable, though both documents may nevertheless provide useful guidance in certain areas.

[7] 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) ("PROTEIN"), pp. 11, 12.

[8] 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 Clinical Trials Directive"), see https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2001_20/dir_2001_20_en.pdf (last accessed on 11 February 2020).

[9] 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 Clinical Trials Regulation"), see https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf (last accessed on 11 February 2020). While this Regulation entered into force in 2014, the timing of its application depends on the development of a fully functional EU clinical trials portal and database. Accordingly, the entry into application is expected in 2020, although this date has been postponed several times. See

More importantly, guidance for conducting research with human participants in the context of the TeNDER research can be found in a number of different sources. Commonly used sources include ethical principles recognised at international and national levels, the rights of patients and the procedures and rules that govern the functioning of ethics committees at national and/or local levels. Furthermore, as the research participants are also data subjects in the context of the TeNDER research, European and national legislation on personal data protection also applies.[10] Finally, the EU Medical Devices Regulation[11] is of relevance to the TeNDER project and will be explored in Section 5.

2.3 Patients' rights in the European Union

One of the target groups of the TeNDER project comprises patients. Their patient status grants them certain rights at the EU level as set out in the EU Patients' Rights Directive.[12] Much of this Directive sees to the practical implications of cross-border healthcare, such as reimbursement of costs and the relevant administrative procedures. However, the Directive also requires that healthcare providers should provide relevant information to help patients make informed choices.[13] In turn, service providers, including ICT-based, should therefore ensure that they provide clear information regarding the availability, safety and quality of healthcare, the prices, insurance coverage and other protective measures regarding professional liability.[14]

The EU Patients' Rights Directive further recognises the obligation that Member States shall ensure protection of the fundamental right to privacy with respect to the processing of personal data in conformity with EU Directive 95/46/EC,[15] which has since been repealed and replaced by the General Data Protection Regulation ("GDPR").[16] This includes a 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.[17]

---

https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trial-regulation (last accessed on 11 February 2020).

[10] See *infra* Section 4.3 on the right to the protection of personal data.

[11] 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 Medical Devices Regulation"), see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745 (last accessed on 11 February 2020).

[12] 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"), see https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF (last accessed on 11 February 2020).

[13] Article 4(2)(d), EU Patients' Rights Directive.

[14] *Ibid*. See also PROTEIN, p. 12.

[15] Article 4(2)(e), EU Patients' Rights Directive. Also see 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 (last accessed on 6 February 2020).

[16] 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 (last accessed on 11 February 2020).

[17] Article 4(2)(f), EU Patients' Rights Directive.

Another noteworthy aspect of the EU Patients' Rights Directive is that it set up a voluntary network on eHealth.[18] This network aims to "connects national authorities responsible for eHealth"[19] 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".[20] The network has, for instance, under its Guideline on the electronic exchange of health data under cross-border Directive 2011/24/EU[21] and related Patient summary guideline,[22] developed "the minimum set of information needed to assure Health Care Coordination and the continuity of care". This is a useful notion for future users of the TeNDER system who travel, work or live in different Member States. It is also advisable that researchers take note of the efforts made by this network.

2.4 Sources for principles of ethics in research with humans

Of great importance for any research engaging directly with human participants are the principles of medical ethics. Many of these principles have a long tradition dating back centuries, some even back to Hippocrates of ancient Greece.[23] 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",[24] now 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".[25] This emphasis on autonomy is illustrated, for instance, by Principle 1, which makes voluntary consent absolutely essential to conducting of medical experiments, and Principle 9, which gives the human subject the power to end the experiment at any time.[26] The Code further requires that the risks of the experiment weigh against the expected benefits

[18] Article 14(1), EU Patients' Rights Directive. Also see PROTEIN, pp. 12, 13.
[19] See https://ec.europa.eu/health/ehealth/cooperation_en (last accessed on 6 February 2020).
[20] *Ibid*.
[21] 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 (last accessed on 6 February 2020).
[22] 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 (last accessed on 6 February 2020).
[23] Hippocrates, *The history of epidemics*, Samuel Farr (trans.), London: T. Cadell (1780).
[24] 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), see https://www.loc.gov/rr/frd/Military_Law/pdf/NT_war-criminals_Vol-II.pdf (accessed on 6 February 2020) ("Nuremberg Code").
[25] *Ibid*. Also see 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 (last accessed on 7 February 2020).
[26] Principles 1 and 9, Nuremberg Code.

(Principle 6)[27] and that the researcher should be prepared to terminate the experiment if its continuation would be dangerous (Principle 10).[28]

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".[29] While the Declaration of Helsinki is mainly aimed at physicians, it encourages others involved in medical research with human participants to adopt these principles.[30] 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.[31] 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".[32] The Guideline for Good Clinical Practice by the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use ("ICH" and "ICH GCP" respectively) can also provide useful guidance.[33] While TeNDER's project activities 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.[34] 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,[35] but is intended to generally be applicable to all research studies on human participants, "not just research involving pharmaceutical or other medical products".[36] Even if certain principles may not apply to all types of research on human participants, the WHO encourages

[27] 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").
[28] 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.").
[29] 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.
[30] Preamble, para. 2, Declaration of Helsinki.
[31] PROTEIN, p. 13.
[32] 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.
[33] 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").
[34] PROTEIN, pp. 13, 14.
[35] WHO, *Handbook for Good Clinical Research Practice*, 2005 ("WHO GCP"), see https://apps.who.int/iris/handle/10665/43392 (last accessed on 21 January 2020), p. 1.
[36] *Id.*, pp. 5, 6.

consideration of its principles wherever applicable "as a means of ensuring the ethical, methodologically sound and accurate conduct of human subjects' research."[37]

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,[38] the UNESCO's Universal Declaration on Bioethics and Human Rights,[39] 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")[40] and its Additional Protocol to the Convention on Human Rights and Biomedicine, Concerning Biomedical Research ("Oviedo Additional Protocol").[41] While not all TeNDER partner-countries have signed or ratified the Oviedo Convention or its Additional Protocol, both instruments nevertheless provide useful guidance on the conduct of scientific research on human participants and necessary safeguards and protections.

2.5 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.[42]

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.[43] In healthcare, the principle of autonomy requires that only upon an informed decision by the patient may any intervention to their body be made.[44] 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.[45] Informed consent plays an important role in the protection of patient (and research participant) autonomy. It constitutes a way in which patients and research

[37] *Id.*, p. 7.
[38] 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.").
[39] United Nations Educational, Scientific and Culture Organisation ("UNESCO"), *Universal Declaration on Bioethics and Human Rights,* 19 October 2005 ("UNESCO Declaration"), see http://portal.unesco.org/en/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html (last accessed on 7 February 2020).
[40] 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"), see https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98 (last accessed on 7 February 2020).
[41] 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"), see https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008371a (last accessed on 7 February 2020).
[42] T. L. Beauchamp, J. F. Childress, *Principles of biomedical ethics*, Oxford University Press, USA, 2001 (the book has been revised subsequently).
[43] Garrett *et. al.*, *Health Care Ethics*, Prentice Hall, 2nd Edition (1993), p. 28. Also see PROTEIN, p. 14.
[44] PROTEIN, p. 14.
[45] PROTEIN, p. 14.

participants can exercise their autonomy.[46] In general, informed consent can both be expressed and implied.[47] 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 to be implied.[48] Nevertheless, in research with human participants, it is generally considered that informed consent should be express and documented.[49]

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."[50]

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."[51]

The principle of justice must inform the physician's decisions about resource allocation and requires an equitable distribution of medical goods and services.[52] 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 treatment or considering an older person a burden rather than someone deserving of medical intervention.[53]

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,[54] thereby striking a balance between these, sometimes competing, interests.

2.6 Procedure and criteria for identifying and recruiting participants in TeNDER

The recruitment of participants for the TeNDER pilots will be without discrimination based on any forbidden grounds (e.g. sex, race, ethic or social origin, age, disability), nor on grounds of competence or proclivity towards technology. The recruitment procedure will further ensure gender balance.[55] Keeping these factors in mind will contribute to an inclusive recruitment of participants.

2.6.1 Criteria

[46] For instance, see Article 5, UNESCO Declaration; Guideline 9, CIOSM Guidelines, p. 34; Principle 7, WHO GCP, pp. 59, 60, 67.
[47] 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"), see https://doi.org/10.7326/M18-2160 (accessed on 7 February 2020), p. 6.
[48] *Ibid*.
[49] For instance, see 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.
[50] APC Ethics Manual, p. 3. Also see PROTEIN, p. 14.
[51] *Id*., p. 45.
[52] APC Ethics Manual, p. 2. Also see PROTEIN, p. 14.
[53] PROTEIN, p. 14.
[54] R. Gillon, *Beneficence: doing good for others*, British Medical Journal Vol. 291, 6 July 1985, p. 44.
[55] GA, Annex 1, Part B, pp. 97, 98.

In light of the purpose of the TeNDER project, namely to create an integrated care ecosystem for assisting people with chronic diseases, including AD, PD and CVDs, through the use of affect-based tools, the TeNDER partners have identified a number of inclusion and exclusion criteria to assist in the recruitment of research participants. The criteria depend on the group the participant belongs to, namely people with AD, PD and/or CVDs on the one hand, and those in the care pathway on the other.

The trial protocol sets out the recruitment of persons with AD, PD, CVDs, heterogeneously represented by gender, aged 60 years and older. For people with AD, PD and/or CVDs, the TeNDER partners have identified a number of general inclusion and exclusion criteria (also see D6.1). The general inclusion criteria, applicable to all persons with AD, PD and/or CVDs are:

- Age ≥ 60 years;
- Understand the local language;
- Have a caregiver or reference person;
- Able to move and walk in their homes;
- Enough autonomy to make decisions;
- Accept to participate themselves together with their caregivers, and have signed the informed consents;
- Comply with scenario setting: having internet at home, for home set scenarios.

Furthermore, TeNDER partners have identified the following common or general exclusion criteria (also see D6.1):

- Oncological history of primary and secondary tumours;
- Chronic therapy for immune diseases, chronic infectious diseases;
- Pyramidal and/or extrapyramidal signs on neurological exam;
- Patients whose caregiver is unwilling to participate / help;
- Patients / caregivers are unwilling to work with the technologies used in this project;
- Alcohol or drug abuse.

In addition, the partners have identified a number of general inclusion and exclusion criteria specific to each particular disease (also see D6.1):

Table 2 - Inclusion and exclusion criteria for Chronic conditions tackled by TeNDER

	Alzheimer's disease or Dementia	**Parkinson's disease**	**Cardiovascular diseases**
Inclusion criteria	- Persons expressing cognitive complaints and an MMSE score of 19 to 28 pts or having diagnosis of a disease-causing dementia with MMSE score of 19 to 28 pts or a diagnosis of Alzheimer's according to NINCDS-ADRDA criteria [5]).	- Confirmed diagnosis of Parkinson's disease. All patients will provide a report with an assessment from the neurologist.	- Suffering from Cardiovascular Disease (classification NYHA, stage II/IV) - Coronary heart disease; acute coronary syndrome; been a coronary catheterization for stent placement
Exclusion criteria	- Advanced stages of the disease (for example	-Parkinsonism's secondary to vascular	- Patients who have had a heart attack less than 4 weeks

	Alzheimer's disease: avoid GDS 6-7).	disease, treatment, etc.	ago, poor life expectancy (<6m) aortic stenosis.

In addition to these general inclusion and exclusion criteria specific to each disease, the pilot partners are currently also developing further disease and scenario-specific criteria as part of the co-designing process under WP2 (preparing the foundation for the technical and piloting phases as well as the overall architecture) and the development of the protocols for the pilots under WP6 (to verify the technological acceptance of the TeNDER system in controlled environments). As they are still under development at this stage, they will be included in later deliverables (including deliverables under WP6, as well as D1.4 (the first version of the legal/ethical monitoring and review) and/or D1.6 (the final version of the fundamental rights, ethical and legal implications and assessment)).

For those in the care pathway, the TeNDER partners also identified a number of inclusion and exclusion criteria (also see D6.1). The inclusion criteria are:

- For caregivers: to be able to consent and to comply with at least one of the following:
  - To be employed by a private company or directly by the person with AD, PD and/or CVDs to provide direct care and thus support daily activities.
  - To live with and/or take care of a relative (or other close relationship) affected by Parkinson's disease or Alzheimer's disease or/and other dementia or cardiovascular diseases.
  - To provide logistical support to a family member or a close friend affected by Parkinson's disease or Alzheimer's disease or/and other dementia or cardiovascular diseases.
- For health professionals (incl. general practitioners, nurses, social workers and others): to be able to consent and to be qualified and working in a medical area specialised in the care of PD, AD and/or CVDs.

The partners have identified the following exclusion criteria for those in the care pathway (also see D6.1):

- For caregivers:
  - Not being able to consent;
  - Not aware of the daily needs of patients.
- For health professionals:
  - Not being able to consent;
  - Not working as a health professional;
  - Working practice not connected to PD, AD, CVDs;
  - The existence of a conflict of interest.

As already mentioned above, as the co-designing process under WP2 and the development of the protocols for the pilots under WP6 continue, all of the criteria defined above are still subject to change. Such changes, if any, will be documented in deliverables under WP6, as well as D1.4 (the first version of the legal/ethical monitoring and review) and/or D1.6 (the final version of the fundamental rights, ethical and legal implications and assessment).

2.6.2 Procedure

The TeNDER partners have identified the following procedures for the recruitment of participants for the pilots, which will be conducted based on the above identified criteria. The procedure will differ, depending on the group the participant belongs to, namely people with AD, PD and/or CVDs on the one hand, and those in the care pathway on the other.

For people with AD, PD and/or CVDs in all four settings, the pilot-partners intend to implement a simple randomisation that will lead to the creation of two arms, namely the control group and the experimental group. After initial identification of potential participants in line with the general inclusion and exclusion criteria, pilot partners will conduct interviews with each potential participant and ensure that they undergo a medical investigation to determine that they fall within the specific criteria developed for each disease.

For those in the care pathway, including health professionals, social workers, caregivers (professional and informal) and others (administrative staff, hospital IT, day care centre workers etc) involved in the care of people with AD, PD and/or CVD co-morbidity, the partners will identify and recruit participants in the care pathway based on the inclusion and exclusion criteria. Compliance with these criteria will be tested by pilot partners through interviews of the potential participant.

As part of the recruitment phase, the potential participant will have to indicate their willingness to participate in the TeNDER pilots, and, if they so choose, provide their consent, or, where they are unable to provide such consent, the consent of their legal representative. The considerations that should be taken into account by the TeNDER partners when obtaining informed consent are set out below.

2.7 Informed consent

As explained in Section 2.5, informed consent is a cornerstone of the principle of autonomy and is relevant to conducting research with human participants. While the Nuremberg Code refers to "voluntary consent",[56] 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).[57] 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.[58] The Declaration requires that special attention be given "to the specific information needs of individual potential subjects as well as to the methods used to deliver the information".[59]

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

[56] Principle 1, Nuremberg Code.
[57] Para. 26, Declaration of Helsinki.
[58] *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.").
[59] Para. 26, Declaration of Helsinki.

consequences, the ability to weigh benefits, risks and alternatives, and the ability to make and communicate a decision.[60]

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,[61] CIOMS Guidelines,[62] the ICH GCP,[63] the WHO GCP,[64] and the UNESCO Declaration.[65]

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 expressly, specifically and is documented. Such consent may be freely withdrawn at any time".[66] 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 are 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.[67] 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."[68]

When considering these requirements related to informed consent in the context of the TeNDER project, it is important to consider that due to the nature of one of the groups of participants that the TeNDER project aims to attract, namely persons with PD, AD and/or CVDs, in all ranges of severity, it is likely that not all participants will be able to give consent for their participation in the pilots and the processing of their personal data themselves. Accordingly, the participants in the TeNDER pilots can be separated into two groups; those who are able to sign informed consent related to their participation and the processing of their personal data, and those who might not be in a position to give informed consent. The specific considerations that should be made for adults unable to give consent are set out below.

Furthermore, additional consideration will need to be given to the inclusion of vulnerable groups in the TeNDER pilots. TeNDER intends to provide a platform that will facilitate the application of integrated care, with a specific focus on elderly and/or chronically ill persons. These two groups are often considered particular vulnerable groups. While the CIOSM Guidelines recommend avoiding labelling an entire group of individuals as vulnerable, it does find it useful to consider the specific characteristics that may render an individual vulnerable. It finds that "this can aid in identifying the

[60] See for instance Guideline 19, CIOSM Guidelines, p. 62; Meulenbroek *et al*., *Informed Consent in Dementia research. Legislation, Theoretical Concepts and How to Assess Capacity to Consent*, European Geriatric Medicine 1 (2010) 58-63 ("Meulenbroek *et al.*"), p. 58.
[61] Article 7, ICCPR, *supra* note 38.
[62] Guideline 9, CIOMS Guidelines, p. 33.
[63] Principle 2.9, ICH GCP, pp. 9, 15 to 18.
[64] Principle 7, WHO GCP, p. 59 to 71.
[65] Article 6, UNESCO Declaration.
[66] 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."
[67] Article 13(1), (2), Oviedo Additional Protocol.
[68] Article 14(1), Oviedo Additional Protocol.

special protections needed for persons who may have an increased likelihood of being wronged or of incurring additional harm as participants in research."[69]

Accordingly, though many of these participants might still be able to give informed consent, special consideration should be given to their status as potentially vulnerable persons and the resulting implications thereof. These issues are set out in more detail below.

2.7.1 Inclusion of vulnerable categories: older persons, chronically ill and those unable to provide consent

Vulnerable persons are described as those who are relatively (or absolutely) incapable of protecting their own interests.[70] 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."[71] As mentioned above, 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,[72] 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.[73] 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."[74] It further provides that "[a]ll vulnerable groups and individuals should receive specifically considered protection."[75]

This principle of providing specific protections and safeguards to vulnerable persons is reiterated in the UNESCO Declaration, the WHO GCP and the CIOSM Guidelines.[76] Such 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."[77] 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."[78]

---

[69] Guideline 15, CIOSM Guidelines, p. 57.
[70] Principle 7, WHO GCP, p. 65.
[71] Guideline 15, CIOSM Guidelines, p. 57. Also see Principle 7, WHO GCP, 65.
[72] Guideline 15, CIOSM Guidelines, p. 57.
[73] See for instance, ICH GCP, p. 8; Principle 7, WHO GCP, pp. 65, 66; Guideline 15, CIOSM Guidelines, p. 58.
[74] Para. 20, Declaration of Helsinki.
[75] *Id*., para. 19.
[76] See for instance Article 8, UNESCO Declaration; Principle 1, WHO GCP, p. 22; Guideline 15, CIOSM Guidelines.
[77] See for instance Guideline 15, CIOSM Guidelines, p. 59; Principle 1, WHO GCP, p. 22.
[78] Guideline 15, CIOSM Guidelines, p. 59.

The TeNDER project falls squarely in the notion included in the Declaration of Helsinki, namely that medical research with vulnerable groups should be responsive to the particular needs of that group and it cannot be carried out in a non-vulnerable group. The TeNDER system is particularly aimed at relieving difficulties experienced by the intended group of research participants, creating an integrated care ecosystem that will contribute to an increased quality of their life as well as that of their family and others in their care pathway. Testing on a non-vulnerable group would not be beneficial to the development of the system, as it aims to create a system that is in tune with the needs of this particular group of persons with PD, AD and CVDs and those in the care pathway of such persons. Moreover, in the course of the TeNDER project, specific safeguards and protections will be put in place to minimise the risk for these particular vulnerable groups, including an informed consent procedure that is cognisant of these potential vulnerabilities and will involve legal representatives of those potential research participants unable to consent.

2.7.1.1 Participation of older persons in research

It is generally considered that when it comes to the participation of older persons in scientific research, the consent requirements are the same that apply to people of younger age.[79] However, especially for those older persons living in nursing homes or similar institutions, there is an inherent risk of vulnerability due to the confined setting where they may feel less freedom to refuse participation or where it is assumed that giving consent will be rewarded.[80] Likewise, vulnerability may result from an existing dependent relationship with their caregiver.[81] In this regard, it is noted that Article 23 of the European Social Charter aims to ensure the effective exercise of the right of elderly persons to social protection, including appropriate support to elderly persons living in institutions.[82] These issues should be carefully considered and navigated by the TeNDER pilot-partners.

In practice, recruitment of older participants may require closer interaction with these participants, providing them with sufficient time to ask questions, as well as clear indications about the processing of personal information,[83] something that should be borne in mind by the TeNDER pilot-partners.

2.7.1.2 Participation of chronically ill persons in research

In principle, unless the illness results in a diminished mental capacity that affects their ability to sign consent,[84] it is generally considered that the existence of a chronic illness or disability does not alter the general consent requirements. Specifically, in relation to dementia, it has been noted that a diagnosis of dementia does not mean that a person is by definition incompetent to consent to

[79] GA, Annex 1, Part B, p. 102.
[80] See for instance Guideline 15, CIOSM Guidelines, p. 58. Also see GA, Annex 1, Part B, p. 103.
[81] See for instance Guideline 15, CIOSM Guidelines, p. 58.
[82] Council of Europe, *European Social Charter* (revised), 3 May 1996, ETS No. 163, see https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf93 (last accessed on 10 February 2020). Also see GA, Annex 1, Part B, p. 103.
[83] PROTEIN, p. 16.
[84] For the requirements of informed consent related to those persons who are unable to sign consent, see Section 2.7.1.3.

participate in any research.[85] Therefore it is important in dementia research to be able to judge the capacity to consent on an individual basis.[86]

Nevertheless, people living with disabilities, people with incurable/chronic diseases or people affected by physical frailty (including due to co-morbidity) are often considered a vulnerable category of research participants, requiring special consideration of their participation and potential protections and safeguards.[87]

In case persons with chronic illnesses are living in an institution, concerns related to the potential restrictions of such a confined setting, similar to those related to older persons living in an institution, should be borne in mind.[88] Furthermore, vulnerability due to a dependency relationship with their caregiver should be considered.[89] In this regard, the Declaration of Helsinki provides that when seeking informed consent, "the physician must be particularly cautious if the potential subject is in a dependent relationship with the physician or may consent under duress."[90] In that case, informed consent should be sought "by an appropriately qualified individual who is completely independent of this relationship".[91]

In particular, recruitment of persons in the early stages of dementia who still have the capacity to consent, additional efforts should be made to ensure that they have understood the information as they may have difficulty with "comprehension, attention span, memory and communication".[92] Close interaction with the potential participants seems to be the most effective way to improve their understanding.[93] Each person's pace should be respected and "printed information can be helpful as a support to memory and going back over what has been said can help the person remember what is involved."[94] It is recommended that TeNDER pilot partners give careful consideration to these issues.

2.7.1.3 Participation of persons in research who are unable to provide consent

Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults ("Recommendation"), 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."[95] While the

[85] Meulenbroek *et al.*, pp. 59, 61.
[86] Meulenbroek *et al.*, p. 59.
[87] See for instance Guideline 15, CIOSM Guidelines, p. 58; ICH GCP, p. 8.
[88] *Infra* Section 2.7.1.1.
[89] *Ibid*.
[90] Para. 27, Helsinki Declaration.
[91] *Ibid*.
[92] Alzheimer Europe, *Ethical issues – Participating in research* (website), see https://www.alzheimer-europe.org/Research/Understanding-dementia-research/Participating-in-research/Ethical-issues (last accessed on 10 February 2020).
[93] Meulenbroek *et al.*, p. 60.
[94] *Ibid*.
[95] 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"), see https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e303c (last accessed on 10 February 2020), Part I, para. 1.

Recommendation does not directly deal with the question of scientific research,[96] 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,[97] 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.[98] Central to these requirements are that, generally, the results of the research should have the potential to produce 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.[99]

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".[100] This last point is particularly relevant to the TeNDER project, where the condition that could prevent potential participants giving informed consent, dementia, is a necessary characteristic of (part of) the research group.

In fact, the CIOSM Guidelines 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.[101] This point is reiterated by the European Dementia Ethics Network in their report on dementia research and ethics[102] as well as by Alzheimer Europe in their 2019 report.[103] However, in this regard, 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.[104]

Some important legal protections for persons incapable of giving consent are set out in the Recommendation, which is governed by the principles of necessity, subsidiarity, maximum

[96] 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).
[97] Para. 28, Declaration of Helsinki.
[98] Article 17(1), Oviedo Convention; Article 15(1), Additional Protocol.
[99] *Ibid*. Also see paras. 28, 29, Helsinki Declaration; Guideline 16, CIOSM Guidelines, p. 61; Article 7(b), UNESCO Declaration.
[100] Para. 30, Declaration of Helsinki. Also see Principle 7, WHO GCP, p. 68.
[101] Guideline 16, CIOSM Guidelines.
[102] European Dementia Ethics Network, *Ethics of Dementia Research*, 2011, Section 3 (Involving people with dementia – background), see https://www.alzheimer-europe.org/Ethics/Ethical-issues-in-practice/2011-Ethics-of-dementia-research (last accessed on 6 March 2020), ("Involving people with dementia in all aspects of research is increasingly recognised as being essential to good dementia research. Their involvement as research participants is of paramount importance and recognised as a significant contribution to society. This also reflects their value within society and their equal right to participate in research".).
[103] Alzheimer Europe, *Overcoming Ethical Challenges Affecting the Involvement of People with Dementia in Research: Recognising Diversity and Promoting Inclusive Research*, 2019 ("2019 Dementia in Europe Ethics Report"), see https://www.alzheimer-europe.org/Publications/Alzheimer-Europe-Reports (last accessed on 2 March 2020), pp. 42, 43.
[104] Guideline 16, CIOSM Guidelines.

preservation of capacity and proportionality.[105] Especially the principle of maximum preservation of capacity is interesting to note here as this shows that the Recommendation favours the idea of 'actual capacity' versus 'legal capacity' where possible, especially in light of the fact that incapacity can be temporary or partial.[106] This is also echoed by the CIOSM Guidelines, which states that "a lack of decisional capacity is time-, task- and context-specific".[107]

But even in cases where the participant is indeed unable to consent, the Recommendation sets out the need for respect for 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.[108] 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.[109]

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 representative".[110] Furthermore, 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".[111] 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".[112] This is also echoed by the ICH GCP.[113] Similarly, in the event of research with participants with dementia who are unable to consent, Alzheimer Europe recommends their involvement in the decision-making process, to the greatest extent possible.[114]

---

[105] See Principles 1, 3, 5 and 6, Recommendation.

[106] 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"), see https://rm.coe.int/09000016805e302a (last accessed on 10 February 2020), paras. 35, 73. Also see 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.

[107] Guideline 16, CIOSM Guidelines, p. 62.

[108] Principle 9(1), Recommendation.

[109] 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").

[110] Para. 29, Declaration of Helsinki. Also see, for instance, Meulenbroek *et al.*, p. 62.

[111] Article 7(a), UNESCO Declaration.

[112] Guideline 16, CIOSM Guidelines, p. 62.

[113] Para. 4.8.12, ICH GCP, p. 17 ("When a clinical trial (therapeutic or non-therapeutic) includes subjects who can only be enrolled in the trial with the consent of the subject's legally acceptable representative (e.g., minors, or patients with severe dementia), the subject should be informed about the trial to the extent compatible with the subject's understanding and, if capable, the subject should sign and personally date the written informed consent").

[114] See Alzheimer Europe, *Ethical issues – Participating in research* (website), see https://www.alzheimer-europe.org/Research/Understanding-dementia-research/Participating-in-research/Ethical-issues (last accessed on 10 February 2020) ("However, the person with dementia should still be involved in the decision-making process as much as possible."). Also see 2019 Dementia in Europe Ethics Report, p. 69.

2.7.2 Procedures for obtaining consent in TeNDER

For TeNDER pilot-partners, one of the initial steps in the informed consent procedure will be to assess and determine whether the potential participant has the capacity to consent, or whether consent from their legal representative will need to be sought.

For those potential participants determined to be able to give consent, and taking into account those considerations set out in Section 2.7, the relevant pilot-partners will ensure that the following additional steps are taken in connection to the process of obtaining informed consent:

- Comprehensive information will be provided to the potential participants (see below for minimum requirements) to enable them to make an informed decision about their participation. This information is accompanied by a consent form, including relevant references to national and local legislation, which will document the confirmation of consent;
- The consent form will include the necessary information related to the processing of personal data of the participants in compliance with EU, national and local legislation;
- Partners will ensure that the information provided to each potential participant is adapted to their needs, especially in connection to vulnerable groups (see Sections 2.7.1, 2.7.1.1, and 2.7.1.2).

For those potential participants where it is determined that they are not in a position to provide consent, the relevant pilot partners will ensure that the following steps are taken in connection to the process of obtaining informed consent of their legal representative, bearing in mind the requirements and considerations set out in Sections 2.7.1 and 2.7.1.3:

- The partner will involve the potential participant's legal representative and provide them with comprehensive information (see below for minimum requirements) to enable them to make an informed decision about the potential participant's involvement in the project. This information is accompanied by a consent form, including relevant references to national and local legislation, which will document the confirmation of consent;
- The consent form will include the necessary information related to the processing of personal data of the participants in compliance with EU, national and local legislation;
- While it is determined that the potential participant is unable to provide consent, the partner will nevertheless involve the potential participant as much as possible in the process, provide information to the extent they can understand, obtain assent where possible, and respect their objection or dissent, even if the legal representative would consent to their participation.

While the precise requirements of information to be provided to the TeNDER research participants may differ based on the national and local requirements, certain minimum information should be provided to each participant during the process of obtaining informed consent in line with the information obligation set out in various instruments discussed in Section 2.7:

1. An overall description of the TeNDER system (including information about the financing of the project and possible conflict of interest) and the research scope of the pilot;
2. The pilot procedures, incl. approximate number of participants in the pilot;

3. The participant's role in the research project;
4. Foreseeable risks, inconveniences and benefits, if any;
5. A disclosure of appropriate alternative procedures for treatment/diagnosis, if any, that might be advantageous to the subject;
6. The free and voluntary nature of the participation;
7. The possibility to withdraw from the pilot at any time without consequences;
8. The responsibility of the participant and foreseeable circumstances and reasons where the participant's involvement may be terminated;
9. Type and extent of data collected and purpose of collection;
10. Confidentiality of information collected: how/where/for how long it will be stored; security measures in place, who will have access;
11. Confidentiality of participant identity;
12. Expected duration of the pilot and of the participant's specific participation;
13. The conditions of insurance;
14. The incidental and secondary findings policy;
15. Confirmation that this research project has been approved by an independent medical ethical organ;
16. Contact details of the researchers to enable the participant or legal representative to reach out to and questions.

Specifically, in relation to data processing and data protection, each potential participant and/or their legal representative, if applicable, will be informed about:

1. The type(s) of data to be collected;
2. The method(s) of collecting data;
3. Confidentiality and anonymity conditions associated with the data including any exceptions to confidentiality, for example, with respect to potential disclosures and details on possible sharing of personal information with authorised third parties on a strict need-to-know basis;
4. The opportunity to have any supplied personal data destroyed on request (unless such a request would render impossible or seriously impair the achievement of the objective of that processing – including the impairment or invalidation of the research);
5. The name and contact details of the person(s) responsible for the data collection and processing;
6. The regulatory authority for the specific pilot;
7. All other rights of the participant conferred by the GDPR (Articles 15 to 21 GDPR) as set out in the informed consent form;
8. How the data will be processed and disclosed.

Following these procedures will serve as an important safeguard during the pilot-phase of the TeNDER project to ensure that the consent provided by the research participants is freely given, specific, informed and a reflection of the participant's wishes.

2.8 Competent Ethics Committees

In addition to international ethical norms, medical research is also subject to the approval by an ethical committee. The Declaration of Helsinki provides that research protocols for studies with human participants must be submitted for "consideration, comment, guidance and approval" to the relevant ethics committee prior to the commencement of the study.[115] Such committees must be "transparent in its functioning, must be independent of the researcher, the sponsor and any other undue influence and must be duly qualified".[116]

The EU Clinical Trial Directive defines an ethics committee as "an independent body in a Member State, consisting of healthcare professionals and non-medical members, whose responsibility it is to protect the rights, safety and wellbeing of human subjects involved in a trial and to provide public assurance of that protection".[117] Its successor, the EU Clinical Trials Regulation, defines it as "an independent body established in a Member State in accordance with the law of that Member State and empowered to give opinions for the purposes of this Regulation, taking into account the views of laypersons, in particular patients or patients' organisations".[118]

In the context of the TeNDER project, the following ethical committees will be relevant:

Table 3 - Ethical committee for each of the TeNDER participant countries

Country	Ethics committee
Germany (SKBA)	Ethics Committee of the Faculty of Medicine of the Ludwig-Maximilians-University Munich Pettenkoferstraße 8a, 80336 München Tel: +49 (0)89/ 4400 55191 E-mail: ethikkommission@med.uni-muenchen.de
Italy (UNITOV)	Comitato Etico Email: Comitato.etico@ptvonline.it
Slovenia (SPO)	Ministry of Health, Republic of Slovenia, National Medical Ethics Committee Štefanova 5, 1000 Ljubljana Tel: +386 01 478 69 13 / Fax: +386 01 478 60 58 Email: kme.mz@gov.si
Spain (SERMAS)	Central Committee for Primary Care Research
Spain (APM)	San Carlos Clinical Hospital Ethics Committee Email: ceic.hcsc@salud.madrid.org

[115] Para. 23, Helsinki Declaration.
[116] *Ibid*.
[117] Article 2(k), EU Clinical Trials Directive.
[118] Article 2(11) of the EU Clinical Trials Regulation.

3. Ethical and societal concerns

3.1 Introduction

There are a number of different factors related to the TeNDER project that can give cause to ethical and/or societal concerns. One of these concerns, related to the participation of vulnerable groups in scientific research, has already been discussed in Section 2.7.1. Furthermore, the use of new technologies, their acceptance by the society and trust in such technologies is something to assess and consider. Furthermore, the balancing of various fundamental rights and vital interests of different groups of people is another.[119]

The following will address some of the existing ethical and societal concerns that may arise in connection with the TeNDER project.

3.2 New technologies: acceptance by the society and trust

It is intended that the TeNDER system will create an integrated care ecosystem to assist people with chronic illnesses (AD, PD, CVDs), through the use of affect-based micro tools, which will gather information about persons to adapt the system to the individual needs of the person. Various technologies, such as wearables, other sensorial devices and appliances and artificial intelligence algorithms, will be utilised for this purpose.

It is important for the TeNDER project to consider how it can achieve and maintain trust in relation to these new technologies.

3.2.1 Artificial intelligence (AI)

To process data, TeNDER partners intend to make use of various technologies, including artificial intelligence algorithms. It is intended that the collected data in the TeNDER project will be analysed using Deep Learning algorithms in order to allow the system to understand how the user's kinetic, health and emotional status evolves.[120] The TeNDER system will create personalised models for each user to identify abnormalities by detecting deviations from the expected behaviour and raise alerts for rapid intervention in case of need.[121] Making use of AI and health analytic techniques, it will also use the analysed data to make personalised recommendations for the user's care plan.[122]

AI algorithms are based on deep machine learning, which is a fast, automatic and not intuitively explanatory self-learning mechanism.[123] "Machine-learning algorithms are often described as transforming inputs to outputs through a black box. An analyst cannot look inside the black box to understand how that transformation occurs or describe the relationships with the same intuitive and causal language often applied to traditional statistical modelling".[124] "When AI constantly engages in self-learning, the possible output is difficult to predict and explain. The combination of these features

[119] See FASTER, p. 41.
[120] GA, Annex 1, Part B, p. 4.
[121] *Ibid*.
[122] GA, Annex 1, Part B, p. 25.
[123] See FASTER, p. 41, referring to C. Coglianese and D. Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, Penn Law: Faculty Scholarship Repository, 1734, (2017) ("Coglianese & Lehr"), see https://scholarship.law.upenn.edu/faculty_scholarship/1734/ (last accessed on 16 February 2020).
[124] Coglianese & Lehr, p. 1159.

means that humans have a minimal level of control and understanding at all the stages of AI decision-making".[125]

This 'black box' effect of AI contributes to a lack of transparency and thereby to the decline in trust.[126] Not only that, but it stands in contrast with the relevant rules surrounding automated decision-making, namely the requirement of transparency when it comes to processing of personal data based on automated decision-making as well as the data subject's right to information.[127]

It is worth considering here the Ethics Guidelines for Trustworthy Artificial Intelligence developed by the High Level Expert Group on AI.[128] The Expert Group 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".[129] In order to accomplish this, the Expert Group considers that AI needs to be human-centric, and rest on a commitment to its use in the service of common good and humanity, aiming to improve human welfare and freedom.[130] Acknowledging the risks associated with AI, the Expert Group 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 is:

- *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.*[131]

The Expert Group 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").[132]

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.[133] 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".[134]

---

[125] 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 ("Kiseleva"), see https://www.hiig.de/publication/the-futures-of-ehealth-social-ethical-and-legal-challenges/ (last accessed on 16 February 2020).
[126] See Kiseleva; FASTER, p. 41.
[127] See FASTER, p. 41.
[128] High Level Expert Group on AI, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 8 April 2019 ("Ethics Guidelines Trustworthy AI") see https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (last accessed on 17 February 2020). Also see FASTER, p. 42.
[129] Ethics Guidelines Trustworthy AI, p. 4.
[130] *Ibid*.
[131] Ethics Guidelines Trustworthy AI, p. 5.
[132] *Ibid*.
[133] Ethics Guidelines Trustworthy AI, pp. 11, 12.
[134] *Id*., p. 12.

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:

- *human agency and oversight (incl. fundamental rights, human agency and human oversight);*
- *technical robustness and safety (incl. resilience to attack and security, fallback plan and general safety, accuracy, reliability and reproducibility);*
- *privacy and data governance (incl. respect for privacy, quality and integrity of data, and access to data);*
- *transparency (incl. traceability, explainability and communication);*
- *diversity, non-discrimination and fairness (incl. the avoidance of unfair bias, accessibility and universal design, and stakeholder participation);*
- *environmental and societal well-being (incl. sustainability and environmental friendliness, social impact, society and democracy);*
- *accountability (incl. auditability, minimisation/reporting of negative impact, trade-offs and redress).*[135]

Considering the foregoing, with respect to AI technologies involved in the TeNDER project, the partners may wish to consider the following questions:

At what stage do the humans control and operate AI? Can humans intervene to the AI functioning?

What decisions can AI make during the project? What are the purposes of those decisions and how can they be used?

What tools can be used to explain a decision made by AI? What is the most comprehensive way to do so?

What technical measures can be implemented to ensure resilience to attack and security of AI?

What level of accuracy does the AI have and how is it guaranteed?

Are the algorithms of AI fair? Is the data fed to AI appropriate, accurate and up-to-date?

How can the mistakes in AI's functioning be discovered?

How can the mistakes in AI's functioning be corrected? How can the mistakes be prevented?

What are the roles and responsibilities of all the persons involved into the AI's development, training and operating?[136]

3.2.2 Mobile, wearable and other sensorial technologies

The TeNDER project also intends to use a number of mobile, wearable and other sensorial technologies, including smart wristbands, sensors and scanners, home safety devices, microphones and mobile devices. The data collected by the use of these technologies is intended to feed into the TeNDER system, resulting in personalised models for each user to identify abnormalities, raise alerts for rapid intervention in case of need, and make personalised recommendations for the user's care

[135] *Id.*, p. 14.
[136] See FASTER, p. 42.

plan.[137] In turn, the TeNDER system is intended to contribute to an increased quality of their life as well as that of their family and others in their care pathway.

While some of these technologies will mainly serve to provide input into the TeNDER system, it is nevertheless useful to consider some of the aspects of the use of such technologies. While subscribing to the benefits of assistive technology,[138] including promoting autonomy and safety,[139] Alzheimer Europe for instance, identifies a number of ethical issues related to their use for people with dementia. "In the case of dementia, the people using the technology are not necessarily able to fully understand the implications and may not have the capacity to give full consent, yet its use may be beneficial, enabling them to accomplish tasks that they would otherwise be unable to manage."[140] This can lead to certain ethical dilemmas that could affect society's trust in this technology.

For instance, installing devices and systems in people's homes could create a safer environment for people with dementia, but also carry the risk of making it feel "like a prison" for them. The system may also be a source of shame, stigma and embarrassment if the equipment is visible and/or invasive, or it may be a source of confusion if patients forget how the system and the devices work or that they were installed in the first place.[141] Similar concerns could apply to the use of such technology in hospitals, day care centres, or rehabilitation rooms. Another concern is that such technologies would replace human contact.[142] Furthermore, regardless of the settings, the use of movement, tracking or tagging sensors and electronic surveillance (adding a visual image of the person being monitored) can be perceived as an invasion of a person's privacy. Such intrusions can be limited by the type of equipment used, the duration of such use and limiting where such equipment is used and who has access to the footage captured by the sensor/surveillance equipment.[143]

To contribute to the acceptance and trust of such technology, it will be important to consider these ethical dilemmas and risks. For instance, Alzheimer Europe encourages that when considering the use of assistive technologies, proportionality is taken into account (i.e. the level of intervention should be restricted to what is really needed for a particular person in a particular situation),[144] to carefully weigh safety/security considerations against autonomy and liberty, whereby care should be taken not to resort to paternalistic tendencies (i.e. protecting people from themselves and assuming safety is more important than liberty), and to consider any potential dangers linked to the use of the device or system

[137] GA, Annex 1, Part B, pp. 4, 25.
[138] Alzheimer Europe, *The ethical issues linked to the use of assistive technology in dementia care* (developed within the framework of the European Dementia Ethics Network), 2010 ("AT in Dementia Care Report"), see https://www.alzheimer-europe.org/Ethics/Ethical-issues-in-practice/2010-The-ethical-issues-linked-to-the-use-of-assistive-technology-in-dementia-care (last accessed on 17 February 2020), Section 1 (Background information – Assistive technology). **Assistive technology** is described as "devices or systems which allow people to perform tasks which they would otherwise be unable to do, or to increase the ease and safety with which tasks can be performed".
[139] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Enhancing safety and wellbeing in the home & Surveillance, safety and monitoring).
[140] AT in Dementia Care Report, Section 2 (AT, ethical issues and legislation – Applying Ethics to AT).
[141] *Ibid*.
[142] *Ibid*.
[143] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Surveillance, safety and monitoring).
[144] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Enhancing safety and wellbeing in the home).

itself.[145] These principles can equally be applied to the use of assistive technology for people without dementia.

In connection to these technologies, TeNDER partners may consider the various ethical dilemmas their use may pose and answer certain questions similar to the questions posed in relation to the use of AI:

> *Is the technology in question safe? What measures can be taken to ensure its safety?*
>
> *Does the technology affect the fundamental rights of persons involved, including privacy and data protection rights?*
>
> *What are the roles and responsibilities of all the persons involved in the development and operation of the technology?*
>
> *What are the purposes, periods and conditions of the technology's use in the project?*[146]

Understanding the technology and its use as well as the implementation of technical and organisational means to ensure safety and the respect of fundamental rights would enable the society to trust that technology and, in turn, the TeNDER project. This would result in an increased efficacy and cost-effectiveness of the project.[147]

3.3 The necessity to balance between the fundamental rights and vital interests of different groups of people

During the pilots, data is intended to be collected in four settings, namely the home, hospital, day-care centre and rehabilitation room.[148] Various types of equipment is intended to be used, either wearable devices worn by the research participant or sensorial devices installed in the pilot sites. When equipment is installed in the pilot sites, there is an inherent risk that the sensor, depth sensors or microphone will pick up activity from others than those participating in the pilot, such as other family members living in the home or other patients, staff or visitors in the hospital, day-care centre or rehabilitation room. Although the general notion of picking up of activity from others by these technologies does not necessarily mean the processing of their personal data, it holds the possibility of affecting fundamental rights of others in some cases.

Alzheimer Europe also recognises this difficulty in their report on ethical issues related to the use of assistive technology in dementia care. In particular, they refer to the risk where one person's desire to use such assistive technology in a group setting, for instance, may infringe upon another's right to privacy or the other person may object to the use of a certain device or equipment (e.g. use of video

[145] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Surveillance, safety and monitoring). This same sentiment is reiterated by the European Committee for Standardization ("CEN"), as they state that "[t]he concrete balance point between care and surveillance needs and the need for guarding safety and dignity depends on a complex of contextual factors that include recognition that the health state of the care receivers, and hence their care needs, may change over time, typically with increasing age, greater frailty and affliction by several chronic diseases. Similarly, the advancement of technology allows for ever deeper sensing and pattern recognition", see 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, p. 10.
[146] See FASTER, p. 44.
[147] *Ibid*.
[148] GA, Annex 1, Part B, p. 15.

surveillance of a shared space/communal area).[149] Similarly, in a home environment, others living with the person for whom the technology has been installed, may not feel comfortable with such monitoring or surveillance and it may carry the risk of infringing on their right to privacy.

In light of the above, Alzheimer Europe advises that where consent is obtained for the instalment of assistive technologies, cohabitants are consulted as such installation may also represent an invasion of their privacy.[150]

Alzheimer Europe also addresses the right to privacy of staff where monitoring or surveillance-type equipment is used in areas where they work. While consent from such staff could be obtained, not all staff may feel comfortable with working in such an environment. Voicing their objection to their employer might not always be self-evident, especially if they feel inhibited to express their opinion due to a fear of losing their job.[151] While a potential solution to this would be the temporary transfer of the staff member to another unit, in case of prolonged use of such surveillance equipment this might not be feasible.[152]

In light of the above considerations, it will be important for TeNDER partners to consider these aspects and to determine whether the technology proposed to be used during the pilots has a risk of infringing upon the rights of others, including family members sharing the home, visitors to the home as well as other patients, staff or visitors in the hospital, day care centre or rehabilitation room. If it is determined that there is indeed a risk, the partners will have to consider measures to mitigate such risks to ensure that the rights of the persons involved in the pilots are balanced against fundamental rights and vital interests of other persons that might be affected by the implementation of the TeNDER system.

[149] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Respecting autonomy, the issue of consent & Enhancing safety and wellbeing in the home & Surveillance, safety and monitoring).
[150] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Enhancing safety and wellbeing in the home).
[151] AT in Dementia Care Report, Section 3 (Ethical issues linked to the use of specific forms of AT – Respecting autonomy, the issue of consent).
[152] *Ibid*.

4. Fundamental Rights

4.1 Introduction

The TeNDER project aims to develop an integrated care ecosystem to assist people with AD, PD and/or CVDs of diverse severity through the use of affect-based micro-tools.[153] These micro-tools would be able to recognise the mood of a person and adapt the system's probes to the person's needs through a multi-sensorial system and match with clinical and clerical patient information.[154]

The system intends to perform user analysis on three different axes: a) indoor daily activity analysis by employing, among others, depth sensors, visual sensors as well as binary sensors attached to doors, furniture; b) health status by using biosensing devices such as wearable devices measuring heart beat rate, body temperature, blood sugar level or blood pressure, and c) emotional status using multiple modalities from diverse devices (such as smartphones, RGB-D sensors and wearable devices).[155]

The utilisation of these various devices and technologies implies the collection of personal data, including information about a user's location, health condition and daily habits. The data that currently has been identified for collection during the pilots comes from both persons with AD, PD and/or CVDs as well as those in the care pathway. For that second group, including health professionals, social workers, caregivers (professional and informal) and others (administrative staff, hospital IT, day care centre workers etc), the following information is intended to be collected:

i. identifying data (incl. name, place and DoB, address, ID/social system number);
ii. contact data;
iii. professional status;
iv. information related to possible burn out.[156]

For persons with AD, PD and/or CVDs, the following data is intended to be collected:

i. identifying data (incl. name, place and DoB, address, sex, age);
ii. contact data;
iii. information regarding their living situation;
iv. data concerning their health status and treatment;
v. data gathered from sensorial components;
vi. geo-localisation data deriving from in/out-door tracking (to observe physical activities and to avoid consequences of erratic behaviour).[157]

It is intended that the collected data will be analysed using Deep Learning algorithms in order to allow the system to understand how the user's kinetic, health and emotional status evolve.[158] The system is intending to create personalised models for each person to identify abnormalities by detecting deviations from the expected behaviour and raising alerts for rapid intervention in case of need.[159]

[153] GA, Annex 1, Part B, p. 9.
[154] *Ibid*.
[155] GA, Annex 1, Part B, p. 4.
[156] See GA, Annex 1, Part B, p. 99, supplemented by further information obtained from pilot-partners.
[157] *Ibid*.
[158] GA, Annex 1, Part B, p. 4.
[159] *Ibid*.

Making use of AI and health analytic techniques, it will also use the analysed data to make personalised recommendations for the user's care plan.[160]

The collection and processing of these various types of data might have an effect on the fundamental rights of the research participants, including their right to privacy and their right to data protection. Therefore, the TeNDER partners should take note of the requirements of these fundamental rights and comply with the relevant rules and regulations relevant to the TeNDER project, including those related to the processing of personal data concerning health, a special category of personal data under the GDPR.[161]

In addition, as described above, with the installation of the various types of equipment at the pilot sites, there is a risk that the technology could pick up activity from others than those participating in the pilot, such as other family members living in or visitors to the home or other patients, staff or visitors in the hospital, day care centre or rehabilitation room. Although the general notion of picking up of activity from others by the devices does not necessarily mean the processing of their personal data, it holds the possibility of affecting fundamental rights in some cases.

In light of the above, the following sections will set out the relevant fundamental rights that might be impacted by the TeNDER project, mainly focusing on the right to privacy and the right to data protection. It will take into account the various types of technology that TeNDER intends to use, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, and artificial intelligence algorithms. It will further evaluate the types of data that will be collected and how they are processed in the course of the TeNDER project.

4.2 Right to Privacy and the right to respect for private life

The origins of the concept of privacy is traditionally attributed authors Samuel Warren and Louis Brandeis.[162] It developed in response to the technological developments of that time, such as instantaneous photographs and newspaper enterprises,[163] and "the state of American journalism"[164] 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".[165] In light of these developments, Warren and Brandeis called for privacy, or the right to be left alone.[166]

[160] GA, Annex 1, Part B, p. 25.
[161] Article 9, GDPR. Also see A. Kiseleva, P. Quinn (VUB), FASTER, D2.1 Benchmark Report on Social, Legal, Ethical and Policy Frameworks, 31 August 2019 ("FASTER"), p. 9.
[162] S. D. Warren & L. D. Brandeis, *The Right to Privacy*, Harvard Law Review Vol. 4, No. 5, 1890, p 193-220 ("Warren & Brandeis"). Also see 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.
[163] Warren & Brandeis, p. 195. Also see 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.
[164] De Hert & Gurwirth, p. 61.
[165] Warren & Brandeis, p. 195.
[166] *Ibid*.

While the concept of privacy has been in existence for more than a century, there is not one, universally accepted definition.[167] How the term is defined often depends greatly on the social, ethical and cultural context.[168]

After developing in academia, the concept of privacy found its way as a legal right into numerous national and international instruments. It emerged as a fundamental right in the Universal Declaration of Human Rights ("UDHR") of 1948.[169] The right has also been recognised in the European Convention on Human Rights ("ECHR") of 1950.[170] In 2000, the right was further included in the Charter for Fundamental Rights of the European Union ("CFR").[171]

4.2.1 Universal Declaration of Human Rights

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.

In the wake of World War II, recalling that "disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind", the United Nations General Assembly proclaimed the UDHR as "a common standard of achievement for all peoples and nations".[172] For the first time, it set out the fundamental human rights "to be universally protected".[173]

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".[174]

[167] See for instance 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 (last accessed on 12 February 20200).
[168] FASTER, p. 10; HR-RECYCLER, p. 10.
[169] United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948 ("UDHR"), see https://www.un.org/en/universal-declaration-human-rights/ (last accessed on 12 February 2020), Article 12.
[170] 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 (last accessed on 12 February 2020), Article 8.
[171] 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 (last accessed on 12 February 2020, Article 7.
[172] Preamble of the UDHR.
[173] United Nations, *The Universal Declaration of Human Rights* (website), see https://www.un.org/en/universal-declaration-human-rights/ (last accessed on 12 February 2020).
[174] 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 (last accessed on 12 February 2020), p. 21. Also see FASTER, p. 11.

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.[175]

4.2.2 European Convention on Human Rights

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

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

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

The Council of Europe was established in the aftermath of World War II "to bring together the states of Europe to promote the rule of law, democracy, human rights and social development".[176] It includes 47 members, 28 of which are members of the European Union.[177]

As part of its efforts, the Council adopted the ECHR in 1950. All Council member states have signed the ECHR.[178] 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".[179] Contracting Parties have the obligation to ensure the protection of the rights and freedoms set out in the ECHR.[180] All Member States of the Council of Europe have now "incorporated or given effect to the ECHR in their national law".[181] 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".[182]

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.[183] The "exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information".[184] When different rights are at stake, an attempt must be made to strike a balance between them.[185]

[175] Handbook on DP Law, p. 21.
[176] *Id*., p. 22.
[177] Council of Europe, *Who we are* (website), see https://www.coe.int/en/web/about-us/who-we-are (last accessed on 12 February 2020).
[178] *Ibid*.
[179] European Court of Human Rights, *European Convention on Human Rights* (website), see https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= (last accessed on 12 February 2020).
[180] Article 1, ECHR.
[181] Handbook on DP Law, p. 23.
[182] *Ibid*.
[183] Article 8(2), ECHR. See also HR-RECYCLER, p. 12; FASTER, p. 11.
[184] Handbook on DP Law, p. 24.
[185] *Ibid.* Also see HR-RECYCLER, p. 12.

4.2.3 Charter of Fundamental Rights of the European Union

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.

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.

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.[186] Accordingly, the EU adopted the CFR on 9 December 2000, though the document only became legally binding with the entry into force of the Lisbon Treaty in 2009.[187]

The language of Article 7 of the CFR is almost identical to that of Article 8 of the ECHR. One difference, whereby 'correspondence' has been replaced by 'communications', was introduced to take stock of technological developments.[188] 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 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.

4.2.4 Balancing between fundamental rights

From the above, it becomes clear that the right to respect for private and family life under both the ECHR and the CFR, is not an absolute one and that often a balancing exercise between different fundamental rights will be required. With regard to the CFR, 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

[186] European Commission, *Why do we need the Charter* (website), see https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_nl (last accessed on 12 February 2020).
[187] *Ibid*.
[188] See HR-RECYCLER, pp. 12, 13.

the principle of subsidiarity and to the Member States only when they are implementing Union law".[189] Therefore, the CFR provides a basis for EU legislation, including the GDPR.[190]

In terms of the TeNDER project, there is, on the one hand, the fundamental right to privacy of the participants in the pilots (and possibly people around them). On the other hand, the monitoring conducted as part of the TeNDER system is aimed to create an integrated care ecosystem for people with chronic illness such as AD, PD and CVDs, that will contribute to an increased quality of their life as well as that of their family and others in their care pathway. Accordingly, with regard to the TeNDER project, different legal, legitimate and democratic limitations to the right to privacy could be applicable.

4.3 Right to the protection of personal data

4.3.1 Introduction

The right to the protection of personal data is, like the right to privacy, a fundamental right enshrined in a number of instruments.[191] The concept of data protection stems from the right to privacy. Both are "instrumental in preserving and promoting fundamental values and rights; and to exercise other rights and freedoms – such as freedom of speech or the right to assembly".[192] 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".[193]

During its development, the TeNDER system will process personal and/or sensitive data of research participants. The following will set out the applicable framework related to the collecting and processing of personal data.

4.3.2 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").[194]

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.[195] The principles contained

[189] Article 51(1), CFR.
[190] FASTER, p. 12.
[191] 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* (website), see https://edps.europa.eu/data-protection/data-protection_en (last accessed on 12 February 2020).
[192] European Data Protection Supervisor, *Data Protection* (website), see https://edps.europa.eu/data-protection/data-protection_en (last accessed on 12 February 2020). Also see FASTER, p. 13.
[193] Handbook on DP Law, p. 19. Also see FASTER, p. 13; HR-RECYCLER, p. 13.
[194] 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"), see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (last accessed on 12 February 2020). Also see FASTER, p. 13.
[195] Handbook on DP Law, p. 26.

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.[196] 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.[197]

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").[198]

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.

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

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[199] or the need to protect the rights and freedoms of others.

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

[196] Council of Europe, *Convention 108 and its Protocols - Background* (website), see https://www.coe.int/en/web/data-protection/convention108/background (last accessed on 12 February 2020).
[197] Council of Europe, *Data protection leaflet*, see https://rm.coe.int/leaflet-data-protection-final-26-april-2019/1680943556 (last accessed 12 February 2020).
[198] 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 (last accessed on 12 February 2020).
[199] Article 3 of the TFEU and Article 23(1) of the GDPR list a series of objectives of general interest.

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.

4.3.3 The General Data Protection Regulation

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[200] and repeals the Directive 95/46/EC.

While the GDPR is intended to harmonise the rules related to data protection across Europe, it is important to note that the Regulation leaves room for derogations by Member States in certain areas, including the processing of special categories of personal data, which can be subject to stricter rules in national law.[201]

Important in GDPR compliance and the provision of recommendations and guidance in GDPR implementation are the European Data Protection Supervisor ("EDPS") and the European Data Protection Board ("EDPB").[202] 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.[203]

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".[204] The EDPB replaces the Article 29 Data Protection Working Party.[205]

4.3.3.1 Definitions in the GDPR

In the context of the TeNDER project, it will be important to consider a number of terms that have been defined by the GDPR, because their application will often determine which data protection provisions apply and how. The main definitions that are of relevance for the TeNDER project are the following (see Articles 4, 9, 22 and recitals 26 and 52):

[200] Preamble of the GDPR ("Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof").
[201] See PROTEIN, p. 19.
[202] See FASTER, p. 13; HR-RECYCLER, p. 16; PROTEIN, p. 19.
[203] EDPS, *About* (website), see https://edps.europa.eu/about-edps_en (last accessed on 12 February 2020).
[204] EDPB, *About EDPB* (website), see https://edpb.europa.eu/about-edpb/about-edpb_en (last accessed on 12 February 2020).
[205] Also see PROTEIN, p. 20.

Table 4 - GDPR definitions of interest fo TeNDER

"Anonymous data"	Information which does not relate to an identified or identifiable natural person or personal data which is rendered anonymous in such a manner that the data subject is not or no longer identifiable.
"Automated individual decision-making"	Decision based solely on automated processing, including profiling, which produces legal effects concerning data subject or similarly significantly affects them.
"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 (fingerprint identification).
"Consent of the data subject"	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.
"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 their health status.
"Data controller"	A natural or legal person who, alone or jointly, determines the purposes and means of processing.
"Data processor"	A natural or legal person who processes personal data on behalf of the controller.
"Data subject"	Any natural person whose personal data is being processed.
"Identifiable natural person"	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
"Personal data breach"	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
"Personal data"	Any information relating to an identified or identifiable natural person (data subject).
"Processing"	Any operation or set of operations 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"	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"	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to

	technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
"Sensitive data"	Personal data which are, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms. It may include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
"Supervisory authority"	An independent public authority established in each Member State which 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.

Relevance for TeNDER project

A key step for the TeNDER partners is to understand and determine whether the data processed by the project falls under the definition of 'personal data'. This will determine whether or not the requirements set by the GDPR apply and adhered to by the TeNDER partners. It is important to note here that the definitions of personal data and processing prescribed by the GDPR are wide and encompass any activity with data about an identified or identifiable person. Accordingly, all such activities might be recognised as processing of personal data and fall within the scope of the GDPR.

The aim of the TeNDER project is to develop the TeNDER system as an integrated care ecosystem to assist people with chronic illnesses (AD, PD, CVDs) through the use of affect-based micro tools which will gather information about persons to adapt the system to the individual needs of the person. Various technologies, such as wearables and other sensorial devices and appliances, will be utilised for this purpose. The type of data that is currently intended to be collected includes identifying data (e.g. name, sex, age, place and DoB, address, ID/social system number), geo-localisation data and data concerning health status.[206] It is therefore safe to conclude that the data processed by the TeNDER project falls under the definition of personal data, and some under the definition of sensitive data, and thereby will fall within the scope of the GDPR.

It is important here to briefly consider the concept of anonymous data. From a legal perspective, this is an attractive concept because the processing of anonymous information, including for statistical or research purposes, does not fall under the scope of the GDPR.[207] However, this option is not always easily achievable in research contexts because data that is truly anonymous may often offer little or no potential in terms of research or practical value.[208] 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

[206] See Section 4.1 above. Also see GA, Annex 1, Part B, p. 99.
[207] Recital 26, GDPR. Also see 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.
[208] Quinn, pp. 2, 15, 16.

contexts".[209] Nevertheless, the concept shall be taken into consideration depending on the nature of the data and the conditions of its processing within the project.

4.3.3.2 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. These are the overarching principles that should always be taken into consideration in the application of the GDPR.

In addition, the GDPR sets out a number of other principles that also need to be adhered to when processing personal data. Insofar the TeNDER partners will process personal data, the following principles should be taken into account:[210]

Table 5 - GDPR protection principles of relevance for TeNDER

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.[211] Fair processing governs primarily the relationship between the controller and the data subject.[212] 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.[213] 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.[214]
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 incompatible with those purposes. The purpose of processing data must be defined before processing is started.[215] 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 TeNDER project would infringe the data minimisation principle.

[209] Quin, p. 15.
[210] Also see FASTER, pp. 16-18; HR-RECYCLER, pp. 18, 19.
[211] The legal ground that is most likely applicable to TeNDER is prior and informed consent of the data subject (for more detail, see Section 3.3.3.3).
[212] Handbook on DP Law, p. 118
[213] *Ibid.*
[214] Article 12(1), GDPR. Also see Handbook on DP Law, p. 120.
[215] Handbook on DP law, p. 122.

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 which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[216] 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.[217]
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.[218]
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 mechanisms; 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.[219]

4.3.3.3 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:

(a) the data subject has given free, voluntary and specific **consent**;
(b) **performance of a contract** to which the data subject is a party;
(c) **compliance** with a **legal obligation** of the controller;
(d) **protection of the vital interests** of the data subject or of another natural person;
(e) activity carried out **in the public interest** or in the **exercise of official authority**;
(f) **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,[220] the GDPR sets more stringent requirements for their processing. In fact, the GDPR prohibits processing of such data, unless one of the grounds set out in Article 9(2) applies, including:

[216] *Ibid.*
[217] *Ibid*.
[218] *Ibid*.
[219] See FASTER, p. 18; HR-RECYCLER, p. 19.
[220] 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".

- **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;[221]
- **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;
- **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.

To define the appropriate legal basis for processing personal data in the TeNDER project, an assessment should be made to determine the purposes of processing, types of processed personal data and the nature, circumstances, other features of processing.[222] For the TeNDER project, it is likely that consent (and explicit consent in case of sensitive data) of the research participant will be one of the most essential legal bases. Another interesting option insofar it processes sensitive data is to consider 'scientific research purposes' under Article 9(2)(j). In this regard, it is noteworthy that the GDPR provides that this "should be interpreted in a broad manner, including for example technological development and demonstration".[223]

As the TeNDER project intends to collect and process personal data directly from data subjects, it is expected that (explicit) consent shall serve as the legal basis where the TeNDER partners collect and process any personal and/or sensitive data. In defining consent, the GDPR sets out its four elements,[224] namely that it is:

[221] 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."
[222] See FASTER, p. 19.
[223] Recital 159, GDPR.
[224] Article 4(11), GDPR. Also see 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"), see https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 (last accessed on 13 February 2020), p. 5.

- **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".[225]
- **Specific**: the GDPR requires that (explicit) consent is given "for one or more specific purposes".[226] 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".[227]
- **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".[228]
- **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".[229]

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.[230] While consent may be given in writing as well as digitally and orally,[231] there rests a duty on the controller to be able to demonstrate that consent for the processing of data has been obtained.[232] 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".[233] Explicit consent may be obtained in writing as well as digitally[234] and orally.[235] 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 TeNDER 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

[225] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011 ("Art. 29 Working Group Opinion 15/2011"), see https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (last accessed on 13 February 2020).
[226] See Articles 6(1)(a) and 9(2)(a), GDPR.
[227] Art. 29 Working Group Opinion 15/2011, p. 17.
[228] Art. 29 Working Party Guidelines, p. 13.
[229] Art. 29 Working Party Guidelines, p. 15.
[230] Art. 29 Working Party Guidelines, p. 17.
[231] Art. 29 Working Group Opinion 15/2011, pp. 21, 22.
[232] Recital 42, GDPR.
[233] Art. 29 Working Party Guidelines, p. 18.
[234] 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.
[235] Art. 29 Working Party Guidelines, p. 18.

authorisation has been given by their legal representative or by an authority, person or body provided for by law.[236]

4.3.3.4 The rights of the data subject

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

Table 6 - GDPR aspects concerning data subject rights for TeNDER

Right to be informed (Art. 12, 13 14 GDPR)	The controller shall take appropriate measures to provide to data subject information about data controller (identity, contact detail, contacts of DPO), the purposes of the processing, the recipients of data and other information. It should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
Right of access (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: a) the purpose of processing; b) the categories of personal data concerned; c) the recipients of personal data; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e) the existence of the right to request from the controller rectification or erasure of personal data; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) the existence of automated decision-making, including profiling. The controller shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
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: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

[236] Also see PROTEIN, p. 25.

	b) the data subject withdraws consent on which the processing is based and where there is no legal grounds for processing; c) the data subject objects to the processing and there is no other legitimate ground of processing; d) the personal data have been unlawfully processed; e) the personal data have to be erased in compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services.
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: (a)the accuracy of the personal data is contested by the data subject; (b)the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing when the processing is based on public interest or legitimate interest of data controller by pending the verification whether the legitimate grounds of the controller override those of the data subject.
Right to data portability (Art. 20 GDPR)	The data subject shall have the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on a consent of data subject or performance of the contract and the data processed by automated means.
Right to object (Art. 21 GDPR)	The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data concerning them which is based on public interest or the legitimate interest of the data controller, including profiling based on those provisions and marketing purposes. The controller shall no longer process the personal data unless some exceptions are applied.
Right to lodge a complaint with a supervisory authority (Art. 77 GDPR)	Every data subject shall have 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	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.[237]

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

receive compensation (Art. 78, 82 GDPR)	

4.3.3.5 Role and obligations of the data controller

The data controller is responsible for ensuring and demonstrating compliance with the GDPR when processing personal data (accountability principle), and for that purpose "implement appropriate technical and organisational measures".[238]

As TeNDER partners intend to process personal data under the GDPR, and noting that the TeNDER pilots will be conducted at multiple sites, by multiple partners, it is important to note that the GDPR recognises the concept of joint controllers, where two or more controllers "jointly determine the purposes and means of processing".[239] Noting that the some of the partners in TeNDER are jointly involved in determining the purpose and means of processing personal data in the context of the TeNDER project, it is likely that they will be considered joint controllers. In the event of such joint controllers, it is important that they make arrangements that clearly identify and allocate responsibilities under the GDPR,[240] which is a step the relevant TeNDER partners will have to undertake.

The GDPR sets out a number of obligations for data controllers which they should adhere to when processing personal data. The following obligations will be relevant for the data controllers in the context of the TeNDER project.

Record of processing activities (Article 30 GDPR)

All data controllers shall maintain a record of processing activities under their responsibility, including information about the data controller, the data processor, if any, and the processing 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,[241] such a register can nevertheless be beneficial to better assess risks and serve as a demonstration of compliance.

Data security (Article 32 GDPR)

The GDPR further requires data controllers (and processors) to put in place 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 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.[242]

Technical measures

[238] Articles 24(1) and 5(2), GDPR.
[239] Article 26, GDPR.
[240] Article 26(1), GDPR. Also see Recital 79, GDPR.
[241] Article 30(5), GDPR.
[242] Article 32(1), GDPR.

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.[243]

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 numbers.[244] 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 identification of a person should be taken into account.[245] 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".[246] 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".[247]

Accordingly, there is a considerably high standard for anonymisation.[248] Pseudonymisation is not a method of anonymisation, but rather only "reduces the linkability of a dataset with the original identity of a data subject".[249] As pseudonymisation therefore continues to allow for identifiability of the data subject, it stays inside the scope of the GDPR,[250] unlike truly anonymised data which falls outside of the scope of the GDPR.[251]

TeNDER partners have expressed the intention to implement the following technical measures in the course of the project that will ensure the security of the personal data that is being processed.

It is generally intended that personal data collected from the research participants will be collected at each of the pilot sites, locally stored and, in some instances, undergo initial processing locally at the pilot sites after which only selected data is sent for further processing (for example only if an anomaly is detected). At this stage, TeNDER partners have indicated that they intend to make use of pseudonymisation of personal and sensitive data to the highest extent possible. This would include assigning codes to each research participant. Where this is possible, TeNDER partners will anonymise data. These measures will be described in more detail in D10.7.

Organisational measures

[243] See Article 32(1), GDPR.
[244] See P. Quinn, P. de Hert (VUB), PICASSO, D3.5 Privacy Compliance Laws Associated with Surveillance, 22 December 2017 ("Picasso"), p. 26.
[245] Recital 26, GDPR.
[246] Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014 ("Opinion 05/2014 on Anonymisation") see https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (last accessed on 26 February 2020), p. 8.
[247] Recital 26, GDPR.
[248] PICASSO, p. 26.
[249] Opinion 05/2014 on Anonymisation, p. 3.
[250] *Id*., p. 10.
[251] Recital 26, GDPR.

Organisational measures that a data controller could implement include regular information provisions to employees about data security rules, clear distribution of responsibilities in matters of data processing, protection of access to locations and to hard- and software of the controller/processor.[252]

In the context of the TeNDER project, a number of such organisational measures will be implemented. First, the TeNDER partners will, among them, ensure a clear distribution of responsibilities in the processing of data under the TeNDER project. How the TeNDER project manages data throughout its life cycle, in order to be compliant to the regulatory framework, will be set out in the Data Management plan (D9.2). In the event that data will be processed by others outside of the TeNDER consortium, it is recommended that a Data Processing Agreement is signed with such data processor which will clearly set out the mandate of the data processor.[253]

Furthermore, TeNDER partners will ensure that access to personal data stored will be restricted to the TeNDER consortium and those who need such access for processing activities. In particular, during the work in WP5, the relevant TeNDER partners will develop a pilot platform that adheres to the relevant data security requirements set out in WP1 (including the present deliverable) and will implement measures to ensure secure access to data from users of the platform. Moreover, personal data will only be processed upon the signing of an informed consent form by the research participant (or their legal representative in the event they are unable to give consent) which details how the personal data will be used and processed and the rights of the data subject.

Finally, a data protection impact assessment ("DPIA") will be undertaken in line with Article 35 of the GDPR (see below) as part of T1.3 which will map, in more detail, the possible risks associated with the processing of personal data in the context of the TeNDER project and identify any additional technical and organisational measures to be taken in addition to those already identified here.

Privacy by design and default (Article 25 GDPR)

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.[254]

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".[255]

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

[252] Handbook on DP Law, p. 167.
[253] See Annex A for a template Data Processing Agreement, see https://gdpr.eu/data-processing-agreement/ (last accessed on 25 February 2020).
[254] Article 25 and recital 78, GDPR.
[255] Article 25(1), GDPR.

necessary for each specific purpose of the processing are processed".[256] This specifically applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility.

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

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

Data breach notification (Articles 33 and 34 GDPR)

If a data breach occurs, the data controller is required, without undue delay and preferably not later than 72 hours after having become aware of the breach, to notify the relevant supervisory authority thereof. If 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 rights and freedoms of natural persons. The controller must document such personal data breaches, including the relevant facts, its 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.

Data protection impact assessment (Article 35 GDPR)

The present deliverable is to include an opinion on whether a DPIA should be conducted in line with Article 35 of the GDPR. Carrying out a DPIA is not mandatory for every processing operation, but rather dependent upon the risk connected to the processing.[257] 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".[258] (emphasis added)

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

(a) 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;
(b) processing on a large scale of sensitive data or of personal data relating to criminal convictions;
(c) a systematic monitoring of a publicly accessible area on a large scale.

The TeNDER project intends to utilise various technologies, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, and artificial intelligence algorithms, resulting

[256] Article 25(2), GDPR.
[257] 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"), see https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (last accessed on 14 February 2020), p. 8.
[258] Article 35(1), GDPR.

in personalised models for each user to identify abnormalities, raising alerts for a rapid intervention in case of need, and making personalised recommendations for the user's care plan.[259] The use of new technology can result in the need to carry out a DPIA because the use of such new technologies can include new forms of data collection and processing and "the personal and social consequences of the deployment of a new technology may be unknown".[260] For example, certain 'Internet of Things' applications will require a DPIA because they may have a substantial impact on privacy and individuals' lives. Therefore, a DPIA would assist a controller in better understanding and responding to risks of new technology.[261]

In light of this, the first two categories under Article 35(3) could potentially apply to the TeNDER project. The use of artificial intelligence algorithms and technologies has the potential to affect the rights of the data subject substantially. Furthermore, the TeNDER project intends to process sensitive data, including data concerning health. Depending on the scale of this processing, it could fall under the second category, thereby requiring a DPIA to be conducted.

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, including:

- where personal data are processed which reveal data concerning health;
- 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;[262]
- where processing operations include new technologies.[263]

All of these elements are relevant to the TeNDER project and in that regard, it is important to note that 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.[264] 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".[265]

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.[266] This might be relevant in light of the multi-centred nature of the TeNDER pilots.

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

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

[259] GA, Annex 1, Part B, pp. 4, 25.
[260] Art. 29 Working Party Guidelines on DPIA, p. 10.
[261] *Ibid*.
[262] Recital 75, GDPR. Also see 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)").
[263] Recitals 89, 91, GDPR.
[264] Art. 29 Working Party Guidelines on DPIA, p. 11.
[265] Art. 29 Working Party Guidelines on DPIA, p. 8.
[266] Article 35(1), GDPR.

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects;
(d) 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.

In light of the considerations set out above, especially noting the type of data to be collected and processed, and the type of data subjects, it is recommended that a DPIA is conducted in the context of the TeNDER project. Accordingly, such a DPIA will be conducted as part of T1.3 (continuous legal/ethical monitoring and review) and specifically under D1.4 (first version legal/ethical monitoring and review).

Stakeholder consultations (Article 35(9) GDPR)

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".

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

Data controllers involved in processing 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.[267]

4.3.3.6 The role and obligations of data processors

In addition to the notion of joint controllers in light of the fact that the TeNDER pilots will be conducted at multiple sites, by multiple partners, it will be important to discern between the roles of the data controller and the data processor, and allocate responsibilities to each.[268] 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.[269]

While a data controller is responsible for compliance with the GDPR and determines the purpose and means of processing, a data processor carries out processing on behalf of the controller and under their instruction.[270] While they act under the supervision of a controller, the GDPR imposes many of

[267] Article 83(4), (5), GDPR.
[268] See PROTEIN, p. 22.
[269] 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"), see https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (last accessed on 14 February 2020), p. 28.
[270] Article 28(1), 29 GDPR. Also see Handbook on DP Law, p. 101.

the obligations placed on controllers also on data processors.[271] The lawfulness of the data processor's processing activity is solely determined by the mandate set by the controller.[272] Article 82(2) of the GDPR 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".[273] 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 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.[274]

Prior to the processing of any personal data, it will be important to define the respective roles of the various TeNDER partners. In the collection and processing of the data about the users utilising the TeNDER system, different partners will be involved, including the pilot-partners conducting the pilots, and the providers of technologies and algorithms to analyse the collected data and others.

As set out above, noting that some of the partners in TeNDER are jointly involved in determining the purpose and means of processing personal data in the context of the TeNDER project, it is likely that they will be considered joint data controllers. With joint controllers, it is important that arrangements are made that clearly identify and allocate responsibilities under the GDPR.[275] In the event that any processing activities, including IT solutions and cloud storage, are conducted by parties external to the TeNDER consortium, it is recommended that a data processing agreement is signed.[276]

4.3.3.7 Transfer of personal data within and outside the European Union

The GDPR makes a distinction between the transfer of data within the EU where, on principle, the principle of free flow of personal data applies,[277] 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 i) an adequacy decision by the European Commission,[278] ii) in the absence thereof, the controller or processor provides appropriate safeguards,

[271] Handbook on DP Law, p. 101. Including Articles 30, 31, 32, 33.
[272] Art. 29 Working Party Opinion 1/2010, p. 25. See also FASTER, p. 27.
[273] Article 28(1), GDPR.
[274] Article 28(3), GDPR.
[275] Article 26(1), GDPR. Also see Recital 79, GDPR.
[276] Recital 81, GDPR. See Annex A, template Data Processing Agreement, see https://gdpr.eu/data-processing-agreement/ (last accessed on 25 February 2020).
[277] Article 1(3), GDPR.
[278] 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.

enforceable rights and legal remedies for the data subject,[279] or iii) in the absence of both an adequacy decision and appropriate safeguards, a number of specific derogations are possible.[280]

All TeNDER partners are located in an EU Member State and there is no intention to send, store or process data outside the EU.[281] Therefore the starting point for the TeNDER project will be free flow of personal data in line with the GDPR requirements.

4.3.3.8 Processing of personal data with the use of artificial intelligence capacities

To collect and process data, TeNDER partners intend to make use of various technologies, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, and artificial intelligence algorithms.

As far as the AI algorithms, it is intended that the collected data in the TeNDER project will be analysed using Deep Learning algorithms in order to allow the system to understand how the user's kinetic, health and emotional status evolve.[282] It is intended that the TeNDER system will create personalised models for each user to identify abnormalities by detecting deviations from the expected behaviour and raise alerts for rapid intervention in case of need.[283] Making use of AI and health analytic techniques, it will also use the analysed data to make personalised recommendations for the user's care plan.[284]

The term "artificial intelligence" is not defined under the law. The European Parliament identified that "there is a need to create a generally accepted definition of robot and AI that is flexible and is not hindering innovation".[285]

Nevertheless, AI algorithms may underlie automated decision-making and profiling[286] and therefore may invoke the application of the GDPR. "Automated decisions are decisions taken using personal data processed solely by automatic means without any human intervention".[287] 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".[288] Accordingly, 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

[279] Article 46, GDPR.
[280] Article 49, GDPR. Also see HR-RECYCLER, p. 28.
[281] GA, Annex I, Part B, p. 101.
[282] GA, Annex 1, Part B, p. 4.
[283] *Ibid*.
[284] GA, Annex 1, Part B, p. 25.
[285] European Parliament, *Report with Recommendations on Civil Law Rules on Robotics*, 27 January 2017 ("EP Recommendations on Civil Law Rules on Robotics"), see http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN (last accessed 12 July 2018), Recital C. Also see FASTER, p. 30.
[286] 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"), see https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (last accessed on 14 February 2020), p. 5.
[287] Handbook on DP Law, p. 233.
[288] Article 4(4), GDPR.

profiling must be to evaluate certain personal aspects of the natural person.[289] In the context of TeNDER, it is important if the intended functionalities of the TeNDER system will result in the evaluation of personal aspects (health) of the pilot participants and eventual users.

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".[290] They 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.[291] However further restrictions and safeguards exist with regard 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 that concern them or 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.[292] 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.[293]

In case of automated decision-making, including profiling, the data subject is entitled "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".[294]

4.3.3.9 Processing of personal data in the TeNDER Project

The TeNDER project intends to develop an integrated care ecosystem for people with chronic illness such as AD, PD and CVDs, and is expected to collect and process different types of data, including information about a user's location, health condition and daily habits. This might have an impact on the fundamental rights of the people involved.

In terms of the TeNDER project, there is the risk that the fundamental right to privacy of the participants in the pilots would be affected. As has been explained, the right is not absolute and in case of competing interests, a balance should be struck. The monitoring conducted as part of the TeNDER system, as an integrated care ecosystem, might be able to contribute to an increased quality of life of its users as well as that of their family and others in their care pathway. Accordingly, with regard to the TeNDER project, different legal, legitimate and democratic limitations to the right to privacy could be applicable.

[289] See Guidelines on Automated Decision-Making and Profiling, pp. 6, 7. Also see FASTER, p. 30.
[290] Guidelines on Automated Decision-Making and Profiling, p. 8. Also see FASTER, p. 30.
[291] Guidelines on Automated Decision-Making and Profiling, p. 9.
[292] Article 22(4) GDPR, referring to Article 9(2)(a) and (g).
[293] Article 22(4) GDPR.
[294] Article 13(2)(f), GDPR.

Furthermore, the collection and processing of various types of data in the course of the TeNDER project will have an effect on the right to data protection of the research participants. The data currently intended to be collected and processed in the context of the TeNDER project is set out in Section 4.1. In the course of the development and testing of the TeNDER system, TeNDER partners will continue to review the type of data to be collected and processed, the means and purpose of processing, as well as the arrangements setting out the partner's responsibilities as joint data controller. This information will form the basis on which the application of the GDPR will be determined and the initial determination and continuous assessment will be vital to TeNDER's legal compliance.

The TeNDER project intends to utilise various technologies, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, bringing the data collected by these technologies together in the new TeNDER system using artificial intelligence algorithms. The use of new technology can result in the need to carry out a DPIA. The GDPR allows DPIAs to address multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. In light of the multi-centred nature of the intended TeNDER pilots, cooperation between the partners with respect to data protection regulations, including DPIA, would be effective in terms of time and costs. In light of these considerations, it is recommended that such DPIA is performed as part of T1.3 and related D1.4.

4.3.4 Member state derogations from the GDPR for processing personal data relating to health status

The GDPR clearly sets out a number of instances where Member States may derogate from the principles laid out therein. For instance, 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 on the basis of public interest.[295] Member States may further incorporate derogations from the GDPR in connection to the processing of sensitive data, including prohibiting the processing of sensitive data on the basis of the data subject's consent, processing necessary for the purposes of occupational or preventive medicine and for public interest in the area of public health.[296] 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".[297]

It is therefore important to consider national law of the various TeNDER pilot sites that include such derogations to the GDPR. These should then be taken into consideration in addition to the rules set out above. Below is an overview of relevant derogations in connection to national legislation of TeNDER pilot partners.

4.3.4.1 Germany

[295] Also see FASTER, p. 46.
[296] Article 9(2), GDPR. Also see FASTER, p. 46.
[297] Article 9(4), GDPR. Also see FASTER, p. 46.

The German Bundesdatenschutzgesetz (or Data Protection Amendment Act), which implements the new German Federal Data Protection Act ("BDSG"), was passed on 5 July 2017 and entered into force on 25 May 2018.[298]

The BDSG sets out a general framework for the processing of sensitive data, including rules on health data.[299] Such processing is only possible if "suitable and specific" safeguards are applied to protect such data. The safeguards may include technical and organisational measures, pseudonymisation, encryption, or the appointment of a Data Protection Officer.[300]

It further provides derogations in relation to the processing of sensitive data without consent. This 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.[301] However, 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.[302] In line with Article 23 of the GDPR, paragraphs 32 to 37 of the BDSG include other restrictions of data subjects' rights.[303]

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 GDPR requirements.[304] Similar amendments are taking place at the regional German Federal States ('Bundesländer').[305]

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 instance, 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 interest and the processing is absolutely necessary).[306] Furthermore, 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.

---

[298] GA, Annex I, Part B, p. 100. Also see Bird&Bird, GDPR Tracker (Germany) ("GDPR Tracker Germany") https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/germany (last accessed on 16 February 2020).
[299] GDPR Tracker Germany.
[300] GDPR Tracker Germany.
[301] GDPR Tracker Germany.
[302] GDPR Tracker Germany.
[303] GDPR Tracker Germany.
[304] PWC, *Reform of German data protection legislation: Second EU Data Protection Amendment and Implementation Act passed*, 23 September 2019 ("PWC"), see 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 (last accessed on 16 February 2020). Also see GDPR Tracker Germany.
[305] GDPR Tracker Germany.
[306] PWC.

The relevant data protection authority in Germany is Bayerisches Landesamt für Datenschutzaufzicht (BayLDA).[307]

4.3.4.2 Italy

The Legislative Decree no. 101 of 10 August 2018 ("Decree") implementing the GDPR has been published in the Official Journal on 4 September 2018. The Decree did not repeal the Italian Data Protection Act but rather amended any provisions of the act conflicting with the GDPR.[308]

There are a number of derogations from the GDPR included in the relevant Italian law, including with respect to processing special categories of data. For example, a "substantial public interest" is a viable lawful basis for the processing of special categories of personal data.[309] For the processing of genetic, biometric and health data the Italian Data Protection Authority ("IDPA") issues guidelines every 2 years and defines the applicable safeguards for processing these categories of data. Moreover, the act specifies that when a high risk of 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.[310] So far, the IDPA has published several guidelines and opinions on the processing of data concerning health, biometric and genetic data.[311]

The Italian law further 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. 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.[312]

The data protection authority in Italy is the Garante per la protezione dei dati personali.[313]

4.3.4.3 Slovenia

---

[307] GA, Annex I, Part B, p. 100.
[308] GA, Annex I, Part B, p. 100. Also see Bird&Bird, GDPR Tracker (Italy) ("GDPR Tracker Italy") https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/italy (last accessed on 16 February 2020).
[309] GDPR Tracker Italy.
[310] GDPR Tracker Italy.
[311] IDPA, General Application Order Concerning Biometrics as of November, 2014, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3590114 (last accessed on 16 February 2020); IDPA, Guidelines on Processing Personal Data to Perform Customer Satisfaction Surveys in Healthcare Sector as of May 5, 2011, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3853781 (last accessed on 16 February 2020); IDPA, Authorization №2/2014 Concerning Processing of Data Suitable for Disclosing Health or Sex Life as of December 30, 2014, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3800455 (last accessed on 16 February 2020); IDPA, Guidelines on the Electronic Health Record and the Health File as of July 16, 2009, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821 (last accessed on 16 February 2020); IDPA, General Authorization №8/2012 for the Processing of Genetic Data as of December 13, 2012, see https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2474250 (last accessed on 16 February 2020).
[312] GDPR Tracker Italy.
[313] GA, Annex I, Part B, p. 100.

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").[314] 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.[315] 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".[316]

Processing may generally only take place if such processing is provided for by statute or if personal consent has been obtained.[317] 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.[318]

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.[319] It indicates that while the processing of a patient's health data and other personal data outside procedures of medical treatment always requires 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.[320] Similarly, the Health Services Act provides that when personal health data is used for scientific research purposes, the relevant patient must be unidentifiable.[321] The Health Services Act further provides that testing of

[314] GA, Annex I, Part B, p. 100. Also see http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906 (last accessed on 16 February 2020).
[315] See https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208 (last accessed on 18 February 2020). Also see an Analytics Framework for Integrated and Personalised Healthcare Services in Europe (AEGLE), *AEGLE in Your Country – Slovenia*, 30 March 2018 ("AEGLE Report"), see http://www.aegle-uhealth.eu/imagem/AEGLEinyourcountry_Slovenia.pdf, p. 6.
[316] Information Commissioner of the Republic of Slovenia, *Personal Data Protection Act* (website), see https://www.ip-rs.si/en/legislation/personal-data-protection-act/ (last accessed on 5 March 2020). Also see DLA Piper, *Data Protection Laws of the World – 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 (last accessed 18 February 2020), p. 2.
[317] See for instance, Articles 8, ZVOP.
[318] Article 17(1), (2), ZVOP. Also see AEGLE Report, p. 8.
[319] AEGLE Report, p. 4.
[320] Article 44(4) & (6), Patient Rights Act (Official Gazette of the Republic of Slovenia, no. 15/08 and 55/17; Zakon o pacientovih pravicah), see http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4281 (last accessed on 5 March 2020). Also see AEGLE Report, p. 8.
[321] 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), see http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO214 (last accessed on 5 March 2020). Also see AEGLE Report, pp. 5, 8.

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.[322] Such testing will generally be subject to consent of the Medical Ethics Commission of the Republic of Slovenia under its relevant Regulation.[323] "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 appear remote, and the study is expected to provide important new scientific information, the NMEC may exempt the research proposer from the duty to seek consent".[324]

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".[325]

Following some concerns expressed by 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".[326] 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,[327] or derogations on the rights of data subjects.[328] 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).[329]

[322] Article 57, Health Services Act.
[323] 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 (last updated 23 March 2018), see https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-0896?sop=2018-01-0896 (last accessed on 6 March 2020). Also see AEGLE Report, p. 9.
[324] AEGLE Report, p. 10.
[325] Official Gazette of the Republic of Slovenia, no. 65/00 and 47/15, see AEGLE Report, p. 5.
[326] DLA Piper Slovenia Report, p. 2.
[327] 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, see https://www.jadek-pensa.si/en/the-slovenian-personal-data-protection-act-zvop-2-proposal-overstepping-the-gdpr-boundaries/ (last accessed on 18 February 2020).
[328] AEGLE Report, p. 17.
[329] 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, seehttps://www.rppp.si/wp-content/uploads/2019/05/20190506_GDPR-National-implementation.pdf (accessed on 18 February 2020), p. 2.

The Slovenian data protection authority is the Information Commissioner of the Republic of Slovenia.[330] It is expected that this will not change with the proposed ZVOP-2.[331]

4.3.4.4 Spain

The official Gazette of Spain published the Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights (Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales) which has been in force since 7 December 2018.[332] This law implements the GDPR into the Spanish legislation.

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).[333] Moreover, the law establishes that the processing of special categories of personal data based on the public interest, for the purposes of 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.[334] 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.[335]

The data protection national authority in Spain is Agencia Española de Protección de Datos (AEPD).[336]

[330] GA, Annex I, Part B, p. 100.
[331] AEGLE Report, p. 7.
[332] GA, Annex I, Part B, p. 100. Also see https://delajusticia.com/wp-content/uploads/2018/12/Ley-proteccion-datos.pdf (last accessed on 16 February 2020). Also see Bird&Bird, GDPR Tracker (Spain) ("GDPR Tracker Spain"), see https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/spain (last accessed on 16 February 2020).
[333] GDPR Tracker Spain. Also see FASTER, p. 46.
[334] *Ibid*.
[335] *Ibid*.
[336] GA, Annex I, Part B, p. 100.

5. Medical devices regulations

5.1 Introduction

The main instrument of the EU framework regarding medical devices, the EU Medical Devices Regulation, aims to harmonise the rules and procedures related to medical devices. The EU Medical Devices Regulation entered into force in 2017, though it will only apply as of 26 May 2020. In light of its imminent application, it will be considered in the context of the TeNDER project.

As described above, the TeNDER project intends bring data collected by various technologies, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, and artificial intelligence algorithms, together in the new TeNDER system, with the aim of producing personalised models for each user to identify abnormalities, raise alerts for rapid intervention in case of need, and make personalised recommendations for the user's care plan. Considering the TeNDER project's utilisation of various existing technologies as well as the development of a new technology, the TeNDER system itself, it is important to consider the relevance of the EU Medical Devices Regulation.

5.2 Scope of 'Medical Device'

Whether the TeNDER system will be defined as a medical device will determine if the provisions of the EU Medical Devices Regulation will apply. A medical device is defined 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.*[337]

As software is explicitly mentioned in this definition, consideration of the TeNDER system as a potential medical device should be considered carefully.

It is intended that the TeNDER system will have the integrated technology and alignment of interests to support a user through their entire clinical journey, including through the integration of all actors in the care pathway to decrease fragmentation of support for people with co-morbidities. The system intends to support the user in their daily activities, treatment adherence, and improve overall treatment efficiency by facilitating information sharing and coordination among those in the care pathway.[338] As one of the expected services, the system will monitor of the user's biological and

[337] Article 2(1), EU Medical Devices Regulation.
[338] GA, Annex 1, Part B, p. 34.

behavioural variables based on which abnormal situations can be detected and reported.[339] Moreover, the system intends to analyse the user's data to generate personal recommendations. Depending on the exact nature of both services, they could potentially fall under the scope of "diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation", thereby attracting the application of the Medical Devices Regulation.

However, to qualify as a medical device, it is important that the manufacturer intended the software (or device) to be used for medical purposes. In a case before the Court of Justice of the European Union ("CJEU"), it was noted 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.[340] Instead, a device that *de facto* performs an activity that squarely falls within the letter of the definition – because it monitors, for instance, blood pressure or heart activity – but is not intended to be used for medical purposes by its manufacturer, is not a medical device.[341] In such a case, the safety certification as a medical device cannot be required.

Likewise, the EU Medical Devices Regulation 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).[342] The Medical Device Coordination Group ("MDCG"), established by Article 103 of the EU Medical Devices Regulation, advises that 'intended purpose' means "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] It is therefore important for TeNDER partners to declare from the outset whether they intend to manufacture the TeNDER system as a device with an intended medical purpose. If so, this could result in stricter safety controls to be applicable than in the event of it being deemed a non-medical device.[344]

The EU Medical Devices Regulation 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".[345] To further assist in the determination of whether the TeNDER system would be considered a medical device, there are a number of guiding documents. For instance, in guidance from the MDCG, '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 medical devices regulation", i. e. such software must have a medical purpose on its own as described by the

[339] *Ibid*.
[340] Brain Products GmbH v BioSemi VOF and Others, Case C-219/11, 22 November 2012, OJ C 26 from 26.01.2013, p.7. Also see PROTEIN, p. 39.
[341] PROTEIN, p. 39.
[342] Recital 19, EU Medical Devices Regulation.
[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), see https://ec.europa.eu/docsroom/documents/37581 (last accessed on 18 March 2020), p. 3.
[344] Also see PROTEIN, p. 39.
[345] Recital 19, EU Medical Devices Regulation. Also see 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).")

manufacturer.[346] The MDCG further provides 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)".[347] It further 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)".[348]

However, the MDCG also reiterates that not all software used in health care is necessarily considered a medical device. Rather, what is generally considered a medical device is "software which 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".[349] Furthermore, the MDCG clarifies that medical device software may be separated into a number of applications or modules, whereby not all modules have a medical purpose. In such an instance, only the modules which fall under the description of medical device must comply with the EU Medical Devices Regulation and carry a 'CE' marking, whereas the non-medical device modules are not subject thereto.[350] Moreover, the MDCG 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".[351]

The Guidance document Medical Devices - Qualification and Classification of stand-alone software ("MEDDEV 2.1/6")[352] provides similar guidance. Useful in connection to the eventual TeNDER system, MEDDEV 2.1/6 provides that "if the software does not perform an action on data, or performs an action limited to storage, archival, communication, 'simple search'[353] or lossless compression (i.e. using a compression procedure that allows the exact reconstruction of the original data) it is not a medical device".[354] It further 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".[355] Only if stand-alone software has a medical purpose, as intended and described by the manufacturer, will it be qualified as a medical device.[356]

---

[346] MDCG 2019-11, p. 6.
[347] *Ibid*.
[348] MDCG 2019-11, p. 7.
[349] MDCG 2019-11, p. 6.
[350] *Id*., pp. 17, 18.
[351] *Id*., p. 18.
[352] European Commission, *Guidance document Medical Devices - Qualification and Classification of stand alone software*, July 2016 ("MEDDEV 2.1/6"), see https://ec.europa.eu/docsroom/documents/17921/attachments/1/translations (last accessed on 14 February 2020).
[353] Defined as "refers to the retrieval of records by matching record metadata against record search criteria". See MEDDEV 2.1/6, p. 11.
[354] *Ibid*.
[355] MEDDEV 2.1/6, p. 7.
[356] *Ibid.*

Furthermore, MEDDEV 2.1/6 provides that software intended to create or modify medical information might qualify as a medical device, especially "if such alterations are made to facilitate the perceptual and/or interpretative tasks performed by the healthcare professionals when reviewing medical information".[357] Another indicator that the software might qualify as a medical device if the software is meant for the benefit of individual patients, namely "intended to be used for the evaluation of patient data to support or influence the medical care provided to that patient".[358]

For example, decision support software, software which combines medical knowledge databases and algorithms with patient specific data, which are "intended to provide healthcare professionals and/or users with recommendations for diagnosis, prognosis, monitoring and treatment of individual patients, are considered medical devices".[359] In case of an information system that is intended to store, archive and transfer data, it might not be classified as a medical device. However, they may be coupled with additional modules which might be classified in their own right as medical device.[360]

Another useful guide is the Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices ("Manual Borderline Medical Devices").[361] The Manual Borderline Medical Devices provides guidance for cases where it is not directly clear whether a device may be classified as a medical device or not. For instance, a software-based system for information management and patient monitoring, including a number of functionalities such as viewing patient information, tracking changes in patient history, generating audible alerts and a patient-specific alarm filtering function based on severity and type of alarm. Noting that the system had a number of functionalities, each functionality needed to be reviewed separately to determine their correct classification. Only one function, the alarm filtering function, subsequently qualified 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.[362]

Important to note here is that, while MDCG-2019-11, MEDDEV 1.2/6 and the Manual Borderline Medical Devices provide useful guidance in the process of determining whether something is a medical device, they are not legally binding. Only the CJEU has the power to give an authoritative interpretation of EU law.

Noting that the TeNDER system could offer monitoring of the user's biological and behavioural variables based on which abnormal situations can be detected and reported as well as analysis of the user's data to generate personal recommendations, this data might be considered to move beyond storage, archival, communication, 'simple search' or lossless compression, and rather constitute processing, analysis, creation or modification of medical information for a medical purposes. If this were indeed the case, this would result, at least these modules, to be considered a medical device.

5.3 Essential requirements

[357] *Ibid*.
[358] MEDDEV 2.1/6, p. 12.
[359] *Id.*, p. 20.
[360] MEDDEV 2.1/6, p. 20.
[361] Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (v.1.22), May 2019 ("Manual Borderline Medical Devices"), see https://ec.europa.eu/docsroom/documents/35582 (last accessed on 14 February 2020).
[362] Example 9.6, Manual Borderline Medical Devices, p. 80.

As it is quite likely that the TeNDER system, or at least modules thereof, will be considered a medical device, it would result in application of the EU Medical Devices Regulation. Such a device may only be placed on the EU internal market if it complies with the stringent requirements under the EU Medical Devices Regulation, including the general safety and performance requirements set out in Annex I.[363] However, it is possible here to make a distinction between 'TeNDER the research project' and 'TeNDER the exploitable product' as it relates to the applicability of the EU Medical Devices Regulation. Such a distinction is useful if TeNDER partners would like to avoid, at this stage, the full application of the strict requirements under the EU Medical Devices Regulation, though it will be for the partner's consideration whether they wish to pursue this path, or rather opt for the full conformity assessment process at this point, following a determination of the TeNDER system, or parts thereof, as a medical device. Requirements and considerations related to both paths are set out below.

5.3.1 TeNDER as research project – Article 5(5) of the EU Medical Devices Regulation

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

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

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

(a) The devices are not transferred to another legal entity;
(b) manufacture and use of devices occurs under appropriate quality management systems;
(c) the health institution justifies in its documentation that the target patient group's specific needs cannot be met, or cannot be met at the appropriate level of performance by an equivalent device available on the market;
(d) the health institution provides information upon request on the use of such devices to its competent authority which shall include a justification of their manufacturing, modification and use;
(e) the health institution draws up a declaration which it shall make publicly available, including:
  i) the name and address of the manufacturing institution;
  ii) the details necessary to identify the device;
  iii) a declaration that the device meets the general safety and performance requirements set out in Annex I to this Regulation and, where applicable, information on which requirements are not fully met with a reasoned justification therefore.
(f) the health institution draws up documentation that makes it possible to have an understanding of the manufacturing facility, the manufacturing process, the design and performance data of the devices, including the intended purpose, and that is sufficiently

[363] Article 5(1), (2), EU Medical Devices Regulation.

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.[364]

The application of Article 5(5) of the EU Medical Devices Regulation would result in an exemption of the stringent requirements under the EU Medical Devices Regulation, with the exception of Annex I and those set out in Article 5(5).

5.3.1.1 Safety and performance requirements under Annex I

Annex I sets out the general safety and performance requirements that a medical device should adhere to. The requirements in the Annex aim to reduce the risks of the use of a medical device as far as possible without adversely affecting the benefit-risk ratio.[365] It sets out some general safety and performance requirements,[366] requirements regarding design and manufacture,[367] as well as regarding necessary information supplied with the device.[368]

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.[369] 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.[370]

Highly relevant for TeNDER are the requirements set out for electronic programmable systems (both devices that incorporate electronic programmable systems and software that are devices themselves).[371] Paragraph 17.2 requires that "software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation". Furthermore, paragraph 17.3 sets out that such software intended to be used in combination with mobile computing platforms "shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise)". Manufacturers shall also set out the minimum requirements in terms of "hardware, IT network characteristics and IT security measures, including protection against unauthorised access" that are necessary to run the software as intended.[372]

[364] Article 5(5), EU Medical Devices Regulation.
[365] Annex I, para. 2, EU Medical Devices Regulation.
[366] *Id*., Chapter I (paras. 1 to 9).
[367] *Id*., Chapter II (paras. 10 to 22).
[368] *Id*., Chapter III (para. 23).
[369] *Id*., paras. 3, 4, 8, 14.
[370] *Id*., para. 15.
[371] *Id*., para. 17.
[372] *Id.*, para. 17.4.

In their guidance, the MDCG helpfully sets out the cybersecurity requirements contained in Annex I in relation to both pre-market and post-market aspects, which are illustrated in the following figure:[373]

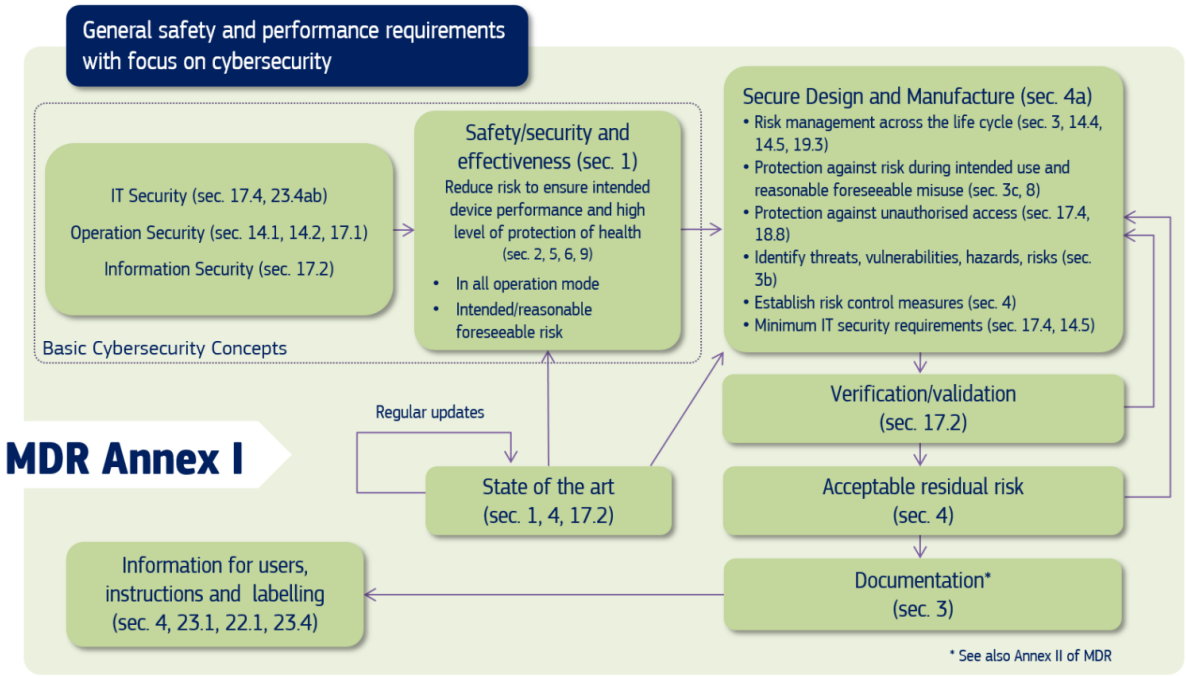

Figure 1 - Cybersecurity requirements contained in MDR Annex I

Further requirements related to 'active devices' (the operation of which depends on a source of energy other than that generated by the human body for that purpose)[374] 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.[375]

Devices must also be developed in such a way that they protect, as much as possible, users against mechanical and thermal risks.[376] As the TeNDER system is also intended to be used by lay persons, Annex I requires that it be developed and manufactured in such a way that "they perform appropriately for their intended purpose taking into account the skills and means available to laypersons and the influence resulting from variation that can be reasonably anticipated in the layperson's environment".[377]

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,

[373] MDCG, *MDCG 2019-16 Guidance on Cybersecurity for medical devices*, December 2019, see https://ec.europa.eu/docsroom/documents/38941 (last accessed on 18 March 2020), p. 5.
[374] Article 2(4), EU Medical Devices Regulation.
[375] Annex I, para. 18, EU Medical Devices Regulation.
[376] *Id*., para. 20.
[377] *Id*., para. 22.1.

on the packaging or in the instructions for use".[378] If the manufacturer has a website, such information should also be included there and kept up to date.[379]

For class I and class IIa devices, no instructions for use are necessary in case such devices can be used safely without such instructions.[380] 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.[381]

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'.[382]

5.3.1.2 Devices used in connection with the TeNDER system

In terms of the technologies that will be used to collect data to input in the TeNDER system, including wearables, sensors and scanners, home safety devices, microphones and mobile devices, some might already bear the 'CE'-marking of a medical device, however, some of these will not be considered a medical device at all as their manufacturer did not intend them for medical purposes, even if they are used as such. In case of the latter technologies, it is important to note that the relevant national ethical boards may take particular note of any tests with the use of non-'CE'-marked medical devices.

In Germany for instance, it is generally understood that the review process by ethical boards of research studies involving the use of non-'CE'-marked medical devices on human participants might take considerably longer than research studies involving the use of only 'CE'-marked medical devices. While the use of such non-'CE'-marked devices is not prohibited *per se* and could be approved by the relevant ethical board, it is important for the TeNDER members to bear in mind that the use of such devices might result in a delay in the review process. There are no indications at this stage that other pilot-countries have similar concerns.

5.3.1.3 TeNDER Research project pilots

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

The TeNDER research project does intend to conduct large scale testing of the TeNDER system on human participants. According to the EU Medical Devices Regulation, "any systematic investigation involving one or more human subjects undertaken to assess the safety or performance of a device" constitutes a clinical investigation. While by definition the TeNDER pilots may constitute a clinical investigation, they do not fall under Article 62(1) of the EU Medical Devices Regulation as they are not "carried out as part of a clinical evaluation for conformity assessment purposes" as TeNDER would not, at this stage, seek to obtain a 'CE' marking. Article 82(1) provides that such 'other' clinical

[378] *Id*., para. 23.1.
[379] *Ibid*.
[380] Annex I, para. 23.1(d), EU Medical Devices Regulation.
[381] *Id*., para 23(4)(q).
[382] *Id*., para. 23(20(q).

investigations only have to observe a number of minimal requirements set out in Article 62(2), (3), (4)(b), (c), (d), (f), (h), (l) and (6):

- *Where the sponsor of a clinical investigation is not established in the Union, that sponsor shall ensure that a natural or legal person is established in the Union as its legal representative.*
- *Clinical investigations shall be designed and conducted in such a way that the rights, safety, dignity and well-being of the subjects participating in a clinical investigation are protected and prevail over all other interests and the clinical data generated are scientifically valid, reliable and robust.*
- *Clinical investigations shall be subject to scientific and ethical review. The ethical review shall be performed by an ethics committee in accordance with national law.*
- *A clinical investigation may only be performed when:*
  - *an ethics committee, set up in accordance with national law, has not issued a negative opinion in relation to the investigation, which is valid for that entire Member State under its national law;*
  - *the sponsor, or its legal representative or a contact person is established in the Union;*
  - *vulnerable populations and subjects are appropriately protected;*
  - *the subject or, where the subject is not able to give informed consent, their legally designated representative has given informed consent;*
  - *the rights of the subject to physical and mental integrity, to privacy and to the protection of the data concerning them in accordance with the GDPR are safeguarded;*
  - *the investigational device(s) in question conform(s) to the applicable general safety and performance requirements set out in Annex I apart from the aspects covered by the clinical investigation and that, with regard to those aspects, every precaution has been taken to protect the health and safety of the subjects. This includes, where appropriate, technical and biological safety testing and pre-clinical evaluation, as well as provisions in the field of occupational safety and accident prevention, taking into consideration the state of the art.*
- *The investigator shall be a person exercising a profession which is recognised in the Member State concerned as qualifying for the role of investigator on account of having the necessary scientific knowledge and experience in patient care. Other personnel involved in conducting a clinical investigation shall be suitably qualified, by education, training or experience in the relevant medical field and in clinical research methodology, to perform their tasks.*

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

While application of Article 82 (and relevant parts of Article 62) of the EU Medical Devices Regulation is not strictly required in connection to the development and use of devices under Article 5(5) (as this provides that with the exception of Annex I, the Regulation does not apply), it is advisable to nevertheless take guidance from the requirements under Article 82, as they mainly sets out basic principles of good clinical practice for conducting research with medical devices involving human participants. Moreover, taking into consideration the requirements of Article 82 during the TeNDER

pilots would facilitate the use of any clinical data gathered during these pilots in any future conformity assessment process under the EU Medical Devices Regulation should the TeNDER partners wish to place the system on the market during its exploitation stage.

Moreover, in terms of retaining the clinical data gathered during the TeNDER project pilots, it is recommended to keep these on file for a period of 25 years. This is based on a reading of the EU Medical Devices Regulation in conjunction with the EU Clinical Trials Regulation.[383] As mentioned above, while the EU Clinical Trials Regulation will only be directly applicable in cases of clinical trials that test medicinal products, there are a number of provisions in the EU Medical Devices Regulation that require harmonisation of certain parts of the medical device trial procedures with the Clinical Trials Regulation.[384] This may be interpreted to mean that it shows the underlying intention that the EU Medical Devices Regulation strives for compatibility and synergy with the EU Clinical Trials Regulation, where possible. Accordingly, as a measure of good clinical practice, and especially since the TeNDER pilots will use human participants, it is advised to strive for this 25-year retention period to ensure the validity of the research.

5.3.2 TeNDER as exploitable product

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

Under the Medical Devices Regulation, the TeNDER system would have to "go through the procedures of clinical evaluation, conformity assessment, assessing the risks of the device, 'CE' marking of the device, control during marketing of the device" as well as registration in a number of electronic systems (of medical devices; Unique Device Identification System ("UDI system"); devices' economic operators; clinical investigations; vigilance and most-market surveillance; and market surveillance).[385]

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.[386] Obligations are also foreseen for importers, distributers and, in some instances, other persons.[387]

The main implications of the application of the EU Medical Devices Regulation to the TeNDER system as medical device upon exploitation are set out below.

[383] As already mentioned earlier, both Regulations have not yet entered into application. The EU Medical Devices Regulation only officially enters into application on 26 May 2020. The EU Clinical Trials Regulation currently does not have a set date for when it will enter into application, though it is expected in 2020. Nevertheless, because they are both expected to enter into application in the course of the TeNDER project, they are relied upon in this report.
[384] For instance, see Recital 67 and Articles 73(2) and 78(7), EU Medical Devices Regulation.
[385] See FASTER, p. 36.
[386] Article 11, EU Medical Devices Regulation.
[387] See Articles 13, 14, 16.

5.4 Classification

The specific procedures and rules relevant to placing a particular device on the market will depend on the classification of the device. Article 51(1) of the EU Medical Devices Regulation 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"[388] and are set out in Annex VIII of the EU Medical Devices Regulation. 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.[389] The higher the class, the stricter the rules that apply to them.

In the context of the eventual exploitation of the TeNDER system, the partners would first need to determine whether the TeNDER system, or modules of it, would fall under the EU Medical Devices Regulation in light of their potential intended medical purpose. If one or more elements of the system are indeed considered a medical device, the classification thereof should be determined. According to paragraph 3.3 of Annex VIII, software independent of any other device shall be classified in its own right, whereas software which drives a device or influences the use of a device will fall within the same class as the device. Paragraph 3.2. of the Annex adds that "[i]f the device in question is intended to be used in combination with another device, the classification rules shall apply separately to each of the devices". For TeNDER it will be important to determine (for any of those modules that may fall under this Regulation) how the interaction between the TeNDER system with the associated technologies (e.g. mobile devices, wearables and other sensors) affects the potential classification.

In relation to the classification of software, Annex VIII of the EU Medical Devices Regulation 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;*
- ***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.*[390]

[388] Recital 58, EU Medical Devices Regulation.
[389] See Annex VIII, EU Medical Devices Regulation.
[390] Rule 11, para. 6.3, Annex VIII, EU Medical Devices Regulation.

In the event of a dispute between the manufacturer and the relevant notified body[391] regarding the application of Annex VIII, the competent authority of the Member State in which the manufacturer has its registered place of business will intervene.[392]

The class of the medical device will determine the subsequent procedures that will apply, including the conformity assessment.[393]

5.5 Conformity assessment

Before placing a device on the internal market, Article 52(1) of the Medical Devices Regulation requires that manufacturers 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 Medical Devices Regulation 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 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 Medical Devices Regulation.

The scope of obligations in terms of the conformity assessment depend 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 to such devices. In contrast, for class IIa, IIb and III devices, a certain level of involvement from the notified body is compulsory.[394]

Upon completion of the conformity procedure, medical devices can be 'CE' marked and put into circulation.[395]

5.6 Clinical evaluation and investigation

5.6.1 Clinical evaluations

Article 5(3) of the Medical Devices Regulation provides 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 EU Medical Devices Regulation, performed by the manufacturer.[396] 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".[397]

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

[391] See Section 4.7.
[392] Article 51(2), EU Medical Devices Regulation.
[393] See FASTER, p. 37.
[394] Recital 60, EU Medical Devices Regulation.
[395] See PROTEIN, p. 41; FASTER, p. 38.
[396] Article 10(3), EU Medical Devices Regulation.
[397] *Id*., Article 2(44).

use.[398] According to Article 2(48) of the EU Medical Devices Regulation, clinical data "means information concerning safety or performance that is generated from the use of a device". Conducting a clinical evaluation will reveal which clinical data are necessary and "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 which clinical data remain to be delivered by clinical investigations".[399]

The clinical evaluation and its documentation are conducted throughout the life cycle of a device.[400] "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".[401]

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

Table 7 - 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.
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.[402]

In the context of the eventual exploitation of the TeNDER system, if the TeNDER system, or modules thereof, are indeed identified as a medical device, the partners will have to ensure that a clinical evaluation is conducted in line with Part B of Annex XIV to ensure conformity of the system/modules with the general safety and performance requirements under Annex I of the EU Medical Devices

[398] *Id*., Article 61(1). Also see 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.
[399] MEDDEV 2.7/4, p. 7. For more on clinical investigations, see Section 5.6.2.
[400] See Article 61(11), EU Medical Devices Regulation; MEDDEV 2.7/1, p. 10.
[401] See MEDDEV 2.7/1, p. 10. Also see FASTER, p. 39.
[402] MEDDEV 2.7/1, p. 13. Also see FASTER, p. 40.

Regulation. As mentioned above, if the TeNDER system is developed under Article 5(5) of the EU Medical Devices Regulation (and thereby compliant with the requirements under Annex I) and if the TeNDER pilots are conducted in line with the requirements set by Article 82 of the EU Medical Devices Regulation and any relevant national law, this will likely satisfy many of the requirements under the clinical evaluation and form an important source of information.

In addition to a clinical evaluation, it should further be considered whether an additional clinical investigation is also warranted. Considerations related to this determination are set out below. In the case of TeNDER, the need for further clinical investigation will partly depend on already available usable clinical data from the pilots should they have been conducted in line with Article 82 of the EU Medical Devices Regulation as set out above.

5.6.2 Clinical investigations

For implantable devices and class III devices, Article 61(4) of the EU Medical Devices Regulation requires, in general, that a clinical investigation be performed. In addition to this, and "depending 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".[403] Accordingly, while the TeNDER system is not an implantable device, and most likely would be classified lower than class III (if at all), there still might be the need to conduct a clinical investigation to collect sufficient clinical data to satisfy the requirements for the clinical evaluation.

As explained above, a **clinical investigation** is "any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device".[404] The requirements for the conduct of a clinical investigation are set out in Article 62 to 81 and Annex XV of the EU Medical Devices Regulation. 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.[405]

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".[406]

"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".[407] 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

[403] MEDDEV 2.7/4, p. 7.
[404] *Id*., Article 2(45).
[405] MEDDEV 2.7/4, p. 7.
[406] Article 62(1)(b) & (c), Medical Devices Regulation.
[407] MEDDEV 2.7/4, p. 8.

investigation are protected and prevail over all other interests and the clinical data generated are scientifically valid, reliable and robust".[408]

Importantly, clinical investigations are subject to scientific and ethical review. The latter must be performed by an ethics committee in accordance with national law.[409] The sponsor of the clinical investigation should be established in the EU or ensure that they have a legal representative established in the EU.[410] 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".[411]

Specific requirements are set out for the protection of vulnerable populations as well as for obtaining informed consent under Article 63 and 64 (related to incapacitated subjects).

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.[412] 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.[413] 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.[414]

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".[415]

In the event of a clinical investigation that is to be conducted in multiple Member States, as could be the case with the exploitation of the TeNDER system, 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.[416] 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.[417]

5.7 The 'CE' marking

Article 2(43) of the Medical Devices Regulation describes 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

[408] Article 62(3), Medical Devices Regulation.
[409] *Ibid.*
[410] Article 62(4)(c) & (2), EU Medical Devices Regulation.
[411] *Id.*, Article 2(49).
[412] Article 70(1), EU Medical Devices Regulation.
[413] *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).
[414] *Id.*, Article 70(7)(b).
[415] *Id.*, Article 71(3).
[416] *Id.*, Article 78(1).
[417] *Id.*, Article 78(2) & (3).

for its affixing". All devices, other than custom-made or investigational devices, that are in conformity with the requirements set out by the Medical Devices Regulation shall bear the CE marking.[418]

Article 20(3) and (4) of the Medical Devices Regulation 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.[419]

5.8 National notified bodies

Authorities that are responsible for the conformity assessment and related procedures are established on the level of each Member State.[420] There are two types of relevant authorities in connection to conformity assessments, authorities responsible for notified bodies and the notified bodies themselves. The former oversees the notified bodies as is provided for in Article 35(1) of the Medical Devices Regulation, which states 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"[421] 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."[422]

[418] Article 20(1), EU Medical Devices Regulation.
[419] Article 20(5), EU Medical Devices Regulation.
[420] See FASTER, p. 38.
[421] Article 2(42), EU Medical Devices Regulation.
[422] FASTER, p. 39.

References

Primary sources

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.

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.

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).

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.

Secondary sources

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).

Books & 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.
- Meulenbroek *et al*., *Informed Consent in Dementia research. Legislation, Theoretical Concepts and How to Assess Capacity to Consent*, European Geriatric Medicine 1 (2010) 58-63.
- 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.

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.
- European Dementia Ethics Network, *Ethics of Dementia Research*, 2011.
- Alzheimer Europe, *Overcoming Ethical Challenges Affecting the Involvement of People with Dementia in Research: Recognising Diversity and Promoting Inclusive Research*, 2019.
- High Level Expert Group on AI, *Ethics Guidelines for Trustworthy Artificial Intelligence*, 8 April 2019.
- 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.
- 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).

Websites

- https://ec.europa.eu/health/ehealth/cooperation_en
- https://www.alzheimer-europe.org
- https://www.un.org/en/universal-declaration-human-rights/
- https://www.coe.int
- https://www.echr.coe.int
- https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_nl
- https://edps.europa.eu/
- https://edpb.europa.eu/
- https://gdpr.eu/data-processing-agreement/

- https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker
- https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208
- https://www.ip-rs.si/en
- https://delajusticia.com/wp-content/uploads/2018/12/Ley-proteccion-datos.pdf

Annex A – Data Processing Agreement Template[423]

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

_____

(the "Company") and

_____

(the "Data Processor")

(together as the "Parties")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

[423] From https://gdpr.eu/data-processing-agreement/ (last accessed on 25 February 2020).

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the _____ services the Company provides.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and

organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those Company Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of _____.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company

Signature _____

Name: _____

Title: _____

Date Signed: _____

Processor Company

Signature _____

Name _____

Title _____

Date Signed _____