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

D1.6
Final version of 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: 30 April 2023

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	UBI	Portugal
5	ELGOLINE DOO	ELGO	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	WP1
Deliverable number	D1.6
Deliverable title	Final version of fundamental rights, ethical and legal implications and assessment
Responsible beneficiary	VUB
Involved beneficiaries	All partners
Type[1]	R
Dissemination level[2]	PU
Contractual date of delivery	30 April 2023 (M42)
Last update	27 April 2023

[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
v 0.1	31/10/2022	Draft	Danaja Fabcic Povse (VUB)	ToC
V0.2	31/03/2023	Draft	Danaja Fabcic Povse (VUB)	Draft
V.0.3	11/03/2023	Draft	Martina Steinböck (SKBA)	Review
V.0.4	11/03/2023	Draft	Svenja Blömeke (SKA)	Review
V 0.5	13/04/2023	Draft	Jennifer Jiménez (APM)	Review
V0.6	24/04/2023	Draft	Danaja Fabcic Povse, Paul Quinn (VUB)	Internal consistency check & final editorial review
V1.0	30/04/2023	Draft	Danaja Fabcic Povse, Jorge Alfonso	Final version for submission

Acronyms and Abbreviations

Acronym/Abbreviation	Description
AI	Artificial intelligence
CDS	Clinical decision support software
CJEU	Court of Justice of the European Union
CNIL	Data Protection Authority in France
DPIA	Data protection impact assessment
DPO	Data protection officer
ECHR	European Court of Human Rights
EDPB/WP29	European Data Protection Board (ex Article 29 Working Party)
EDPS	European Data Protection Supervisor
EHDS	European Health Data Space
GDPR	General Data Protection Regulation
MDR	Medical Devices Regulation
NIS directive	Network and Information Systems Security directive
TeNDER	affecTive basEd iNtegrateD carE for betteR Quality of Life: TeNDER Project, funded under Grant Agreement no. 875325

Contents

List of Tables

Executive Summary

This deliverable presents the final evaluation and assessment of the TeNDER project from the legal and ethical perspective. It focuses on three main areas: data protection and privacy, medical devices, and socio-ethical aspects of integrated care systems. This deliverable is best read together with the *D1.5 Final version of legal and ethical monitoring*, which presents the legal and ethical aspects of the research carried out in the project and which also served as an information gathering tool for the assessments contained in this report.

In section *Legal and ethical work in the TeNDER project*, we discuss the relevance of legal and ethical work in TeNDER, **defining the scope of application** of the **General Data Protection Regulation (GDPR)** and the considerations **whether systems such as TeNDER should fall under the scope of the Medical Devices Regulation (MDR).**

Next, we discuss the *Recent legal developments on EU level*, such as the proposals for the **European Health Data Space and the Artificial Intelligence (AI) Act**, which are at the time of writing this deliverable, being debated in the Parliament, with likely impacts on similar integrated care systems. We also describe **three recent cases** from top European courts dealing with algorithmic decision-making and the treatment of health data.

The section *Main requirements for fundamental rights and socio-ethical acceptance* presents the bulk of this deliverable. It contains a comprehensive appraisal of TeNDER as an integrated care system under the applicable frameworks, such as **privacy, data protection, medical devices, bioethics, explainable AI, and usability/safety**.

This section also contains a table of essential requirements in the areas discussed.

Section *Recommendations* builds upon the findings in the previous section to discuss the wider implications of TeNDER. First, what advice can we give to future adopters of TeNDER, and second, suggestions to policy-makers on adapting the legal frameworks to correspond to the needs of digital health research projects.

Recommendations to future adopters include: responsible implementation of protection of patients' personal data, fundamental cybersecurity considerations under the GDPR and other frameworks, medical devices considerations of using TeNDER, and how to foster trust in the integrated care systems by going beyond the minimal legal requirements.

Recommendations to policy-makers address possible responses to legal gaps encountered by TeNDER; consent for older adults experiencing cognitive decline, legal basis for processing sensitive data of other persons in health and care settings (also referred to as incidental capture), and the need for clarification of the applicability of the MDR.

1 Introduction

1.1 Purpose and scope

This task will identify, adapt and define a complete overview of the main requirements with regard to fundamental rights to data protection and privacy, social and functional acceptance of technological solutions for integrated care in the European level, with special stress in the applications/solutions that can collect personalised information. The output of this task will be a set of recommendations to ensure that TeNDER heeds aforementioned requirements, reporting on the ethical and legal implication of data to be collected and its potential impact.

1.2 Contribution to other deliverables

In the project, we have adopted a three-step methodology to address the legal and ethical frameworks governing the development and testing of integrated eHealth systems, and to provide good implementation practices. First, a benchmark report identified applicable laws and ethical principles *in abstracto*, and analysed the initial concerns of the nexus between technology and applicable frameworks (D1.1 – First version of fundamental rights, ethical and legal implications and assessment). Building upon its findings, the three follow-up impact assessments took into consideration privacy, data protection, ethical-societal aspects, and the regulation of medical devices (D1.4 and D1.5 – First and final versions of legal and ethical monitoring, respectively). This deliverable is the final legal report, containing the evaluation of the technologies developed during the project from legal and ethical perspective. The evaluation contained herein was based on answers from project partners to the three impact assessments, as well as general assembly and ad hoc bilateral conversations.

1.3 Structure of the document

This document consists of three main parts: a short summary of legal and ethical work in TeNDER, updates in the legal framework, the main human rights/legal and socio-ethical requirements, and a recommendations section.

2 Legal and ethical work in the TeNDER project

As a research project, TeNDER crosses a number of different legal frameworks. Concerning the development process, we have focussed on the requirements relevant to privacy and protection of patient data, such as legal basis for processing health data, privacy by design, and privacy-preserving measures; addressed the potential applicability of the Medical Devices Regulation, and a set of socio-ethical concerns. This report synthesises legal and ethical work throughout the project – it looks back to form an *evaluation*, as well as looks forward to *recommend* action to policy-makers and future adopters. Throughout the project, TeNDER development process went beyond the minimum set of legal requirements, since it also focused on fostering trust, safety, and a wider protection of privacy not limited only to patients.

The objective of legal and ethical work has been to ensure patient data could be shared and processed in a secure and efficient manner. Continuous ethical monitoring served to inform project development over the course of various activities, in order to guarantee access, privacy and security of data and experiment execution. The main objective has been to monitor the development of elements related to personal data management to make sure they are in harmony with relevant ethical principles and transparency.

The main legal framework applicable to TeNDER development process has without doubt been the General Data Protection Regulation (GDPR).[3]

GDPR applies when 1) personal data are 2) being processed.

> **Personal data** means any information relating to an identified or identifiable natural person (‘**data subject**’); an identifiable natural person is one who can be identified, directly or indirectly (Art. 4(1) of the GDPR).
>
> **Processing of personal data** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4(2) of the GDPR).
>
> The **data controller** is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4(7) of the GDPR).
>
> The **data processor** is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4(8) of the GDPR).

The data subjects in the project have been patients, as well as their caregivers when they interact with TeNDER, and other staff engaged in the project. Procedures to recruit patients

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

were described in the D10.1, and included factors such as age, location, language, sufficient level of decisional autonomy, etc. User partners acted as data controllers, and technical partners as data processors.

The six basic principles of data processing set out in art. 5(1) of the GDPR ***are lawfulness, fairness and transparency; purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality***. According to the **accountability principle**, the controller is responsible for showing compliance with these principles (art. 5(2) of the GDPR). Accountability in TeNDER was driven by all partners involved in development – legal, users, and technical partners. An in-depth assessment of the incorporation of data protection principles is provided in the sections immediately below.

Since development is by nature carried out in a controlled environment, with a limited amount of participants, and roles of different providers known in advance, legal requirements in a post-project setting may vary depending on their use-case. For example, the pilots in the project are based on small patient groups, where a data protection impact assessment (DPIA) is not always necessary as per the art. 35 of the GDPR, while in a larger organisational context it may well be obligatory. The findings of this report can nevertheless be useful in future settings, either for developers or organisations using similar solutions.

The second research angle concerned the potential application of the **Medical Devices Regulation**. As understood from its name, the regulation aims to provide a unified regime for placing **medical devices for human use and their accessories** on the market, making them available or putting them into service. The regulation also applies to **clinical investigations** concerning such medical devices and their accessories insofar they are conducted in the Union. Since the regulation has wide-ranging implications for developers of medical devices, we paid especial attention to its scope of application: does TeNDER constitute a medical device in the sense of the MDR? Given the development process carried out in the project, TeNDER does not fall under its scope. Full reasoning for this conclusion is given in section *4.3 Regulation of medical devices*.

While this report necessarily looks back upon the development process, we also consider the needs of future adopters and policy makers by providing guidelines in section *5 Recommendations*. They are based upon lessons learned in TeNDER both from the practical and academic points of view.

3 Recent legal developments on EU level

Since the previous version of this deliverable was published in 2020, we analyse relevant legal developments and legislative initiatives on European level broadly applicable to eHealth, that took place in the years between. Together with the legal and bioethical identified in D1.1, the recent developments present a comprehensive legal framework applicable to TeNDER.

3.1 Proposal for a European Health Data Space

As a part of the EU's Data Strategy, sectoral EU-wide data spaces will be created, with the EU health data space (EHDS) as the forerunner. The EHDS proposal from May 2022[4] has two broad aims:

1. Boost Europe's research competitiveness in a global economic context through liberalising the re-use (or secondary use) of data for research. Therefore a key part of the EHDS will establish infrastructure and procedures for research data sharing across the EU.
2. Improve the cross-border health care service for patients by inter alia enabling better access to electronic health records between different member states and allowing cross-border prescription issuance and fulfilment. This has long been a goal of the EU (see the e.g. Patients' rights directive, the eHealth network's Recommendation on the EHR format), replacing the latter's voluntary standards with mandatory ones.

The data protection implications of the EHDS were addressed by the joint opinion of the two privacy watchdogs (EDPB, EDPS)[5]. Inter alia, the opinion stresses the importance of the proposal to contributing to individuals' control over their own health data, and the potential benefits it will bring to policy, innovation and healthcare delivery. However, the watchdogs warn that the proposal may weaken the safeguards of the GDPR regarding re-use of health data. Instead, they suggest:

1. introducing a mandatory consultation of and a duty of cooperation with DPAs with regard to the assessment of complaints as well as the implementation of the Proposal whenever data protection aspects are involved (para. 24),
2. excluding the EHR and wellness applications from the scope of the Regulation, though third-party conformity assessment procedure could be introduced for EHR systems (paras. 75-81),
3. clarify the conditions for consent for reuse of data, which should be aligned with the Article 9(2) of the GDPR (para. 90),
4. as well as other actions, such as clarifying the scope of application of the proposed regulation, its definitions and its relationships with other recently adopted or proposed legislation (inter alia – the Data Act, the Data Governance Act, and the AI Act).

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space 2022 [COM/2022/197 final].

[5] European Data Protection Board and European Data Protection Supervisor, 'Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' (2022) <https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf> accessed 1 April 2022.

Since the EHDS still needs to pass Parliament and Council and is expected to undergo additional amendments, this is a piece of legislation that will be closely monitored by academics and practitioners in the years to come.

The aim is to have a large part of the EHDS in place by 2025, which will have a major impact on health research activities in the EU. Definition – EHR, data, etc. However, it is worth noting that the proposal will undoubtedly undergo more transformations in negotiations and later amendments, and thus will be a key piece of legislation to monitor in the coming years.

The relevance of the proposal for TeNDER is indirect since the regulation is not yet in force and the project has collected data directly from the patients. However, that may not be the case for adopters if healthcare organisations decide to use the medical information from the EHR together with TeNDER system. Since TeNDER development process has followed the EHR recommendations in building its technology (see WP5), this will in turn facilitate the adoption of EHDS-compliant systems insofar they are based on the Recommendation. As the EHDS proposal was released after the main technical works had been completed TeNDER is not based on the EHDS requirements but it is based on the Common EHR format recommendation.[6] This will also facilitate adoption for future users who perform cross-border healthcare since the EHR formats will be machine readable.

3.2 Proposal for an AI act

The other key legislative document relating to medical AI is the proposal for the Artificial Intelligence Act dated April 21 2021.[7] We do not deem the proposed AI Act directly relevant for TeNDER as the latter does not aim to be a prohibited or high-risk AI system in the sense of the proposal. However, since the Act targets the development of inter alia medical AI and medical systems more broadly, it may well be applicable to similar projects in the field.

The proposal does not seek to regulate AI in general; rather, it focuses on specific applications of the technology based on their risks to individuals' health, safety, and fundamental rights and freedoms. It relies on a four-tier system depending on the risk:

1. 'unacceptable risks' (explicitly prohibited),
2. 'high risks' (triggering a set of stringent additional requirements),
3. 'limited risks' (requiring transparency obligations),
4. 'minimal risks' (codes of conduct recommended but not mandatory).

The proposal contains the following sets of rules (art. 1):

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;
(b) prohibitions of certain artificial intelligence practices;
(c) specific requirements for high-risk AI systems and obligations for operators of such systems;

[6] See TeNDER deliverable D5.1, First Report on the Health Record and Pathway Repository

[7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS 2021 [COM/2021/206 final].

(d) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;
(e) rules on market monitoring and surveillance.

The regulation will apply to (art. 2):

(a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
(b) users of AI systems located within the Union;
(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.

However, the regulation will not apply to military use AI, nor for AI used in law enforcement and judicial cooperation (art. 2). To high-risk AI systems that are safety components of products or systems, only art. 84 will apply, meaning that the Commission will periodically review their level of risk (art. 2(2)) – for example, this is the case for AI-powered machinery in the sense of the Machinery Directive.

While the regulation does not define AI as such, it does contain a definition of an '*artificial intelligence system'* (AI system) as 'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with' (art. 3(1)).

A '*provider*' (art. 3(2)) is defined as 'a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge'. The regulation will also apply to SMEs ('*small-scale provider*') (art. 3(3)).

A '*user*' is understood as 'any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity' (art. 3(4)).

The proposal contains **four explicit prohibitions (art. 5)**. It bans AI systems that cause or are likely to cause *"physical or psychological" harm through the use of "subliminal techniques"* or by *exploiting vulnerabilities of a "specific group of persons due to their age, physical or mental disability."* It prohibits AI systems from providing *social scoring for general purposes by public authorities*. It also precludes the use of *"real-time" remote biometric identification systems, such as facial recognition, in publicly accessible spaces for law enforcement purposes*.

Thus, it focuses on two aspects: practice and intent. In this context, practice stands for the placing on the market, putting into service or use of an AI system, and the intent means it is done in a manner that causes or is likely to cause that person or another person physical or psychological harm.

High-risk AI systems will be subject to a number of requirements, obligations and notification requirements, based on their classification, contained in art. 6-51. High-risk AI systems are classified as (art. 6):

(a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;
(b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

The areas of concern in Annex III refer to: biometric identification and categorisation of natural persons; management and operation of critical infrastructure; education and vocational training; employment, workers management and access to self-employment; access to and enjoyment of essential private services and public services and benefits; law enforcement; migration, asylum and border control management; and administration of justice and democratic processes. This list can be amended by the Commission according to art. 7 of the proposal.

Among the *requirements* there are provisions on high-risk AI systems' compliance with quality rules on data and data governance (i.e., those systems must be trained/validated/tested on data meeting the quality criteria from art. 10); documentation and record-keeping; transparency and provision of information to users; human oversight; and robustness, accuracy and security. At the end of April 2023, the European Parliament is set to vote on amendments to the proposal. One of those requires that all users of high-risk systems have to conduct an impact assessment to consider their potential impact on the fundamental rights of the affected person.[8]

Obligations differ based on whether address providers, users or third parties.

Obligations addressed to providers:

5. Compliance: Ensure compliance with the requirements for high-risk AI systems (outlined above);
6. Conformity assessment: Ensure the system undergoes the relevant conformity assessment procedure (prior to the placing the system on the market/putting the system into service);[9]
7. Corrective action and notification: Immediately take corrective action to address any suspected non-conformity and notify relevant authorities of such non-conformity;
8. Quality management system: Implement a quality management system, including a strategy for regulatory compliance, and procedures for design, testing, validation, data management, and recordkeeping;
9. Registration: Register the AI system in the AI database before placing a high-risk AI system on the market; and

[8] https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/

[9] Conformity Assessments will resemble the already existing data protection impact assessment to a certain degree, especially regarding the risks to fundamental rights and freedoms. See: Katerina Demetzou, 'Introduction to the Conformity Assessment under the Draft EU AI Act, and How It Compares to DPIAs - Future of Privacy Forum' (*Future of Privacy Forum*) <https://fpf.org/blog/introduction-to-the-conformity-assessment-under-the-draft-eu-ai-act-and-how-it-compares-to-dpias/> accessed 16 September 2022.

10. Post-market monitoring: Implement and maintain a post-market monitoring system, by collecting and analysing data about the performance of high-risk AI system throughout the system's lifetime. This includes obligations to report any serious incident or any malfunctioning of the AI system, which would constitute a breach of obligations under EU laws intended to protect fundamental rights.

Obligations addressed to users:

11. Use the systems in accordance with the instructions of the provider and implement all technical and organisational measures stipulated by the provider to address the risks of using the high-risk AI system;
12. Ensure all input data is relevant to the intended purpose;
13. Monitor operation of the system and notify the provider about serious incidents and malfunctioning; and
14. Maintain logs automatically generated by the high-risk AI system, where those logs are within the control of the user.

Obligations addressed to third parties include:

15. art. 24 - obligations of product manufacturers,
16. art. 26 – obligations of importers,
17. art. 27 – distributors,
18. art. 28 – obligations of distributors, importers, users or any other third-party.

The proposal further provides for notification duties to supervisory authorities (art. 33), the composition and role of supervisory authorities, transparency requirements of AI systems intended to interact with natural persons (art. 52), with special rules for emotional detection high risk AI systems and deepfakes, measures in support of innovation such as regulatory sandboxes (art. 53-55), governance, including the European AI board (art. 56-59), EU database for standalone high-risk AI systems (art. 60), post-market monitoring information sharing, market surveillance (art. 61-68), including reporting serious incidents and malfunctioning, which is especially relevant for developers of medical devices. Further, art. 69 deals with codes of conduct, intended to foster the voluntary application of the requirements set out in Title III to AI systems other than high-risk AI systems. These are especially important for AI systems which do not pose a high risk.

It is worth noting that algorithmic bias is not explicitly addressed, though data quality requirements provide some mitigation, nor does it mention gender bias which is often a problem in algorithmic systems.

If the proposal is accepted, it will apply 24 months from the moment it enters into force. Its adoption will contribute to other policy developments in the Digital Single Market, such as the Data Governance Act, Digital Services Act, and the Data Act.

3.3 Recent jurisprudence

3.3.1 CJEU case on automated decision-making (OQ v Land Hesse, C-634/21)

This case concerns the scope of art. 22 – the right not to be subject to automated decision-making. The German court referred two questions to the CJEU, namely:

1. Is Article 22(1) of Regulation (EU) 2016/679 to be interpreted as meaning that the automated establishment of a probability value concerning the ability of a data subject to service a loan in the future already constitutes a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her, where that value, determined by means of personal data of the data subject, is transmitted by the controller to a third-party controller and the latter draws strongly on that value for its decision on the establishment, implementation or termination of a contractual relationship with the data subject?
2. If Question 1 is answered in the negative, are Articles 6(1) and 22 of Regulation (EU) 2016/679 to be interpreted as precluding national legislation under which the use of a probability value – specifically, in relation to a natural person's ability and willingness to pay, in the case where information about claims against that person is taken into account – regarding specific future behaviour of a natural person for the purpose of deciding on the establishment, implementation or termination of a contractual relationship with that person (scoring) is permissible only if certain further conditions, which are set out in more detail in the grounds of the request for a preliminary ruling, are met?[10]

The Advocate General's opinion, delivered on March 16 2023, explicitly advocated against a formalistic and narrow interpretation of Article 22 GDPR. In the Advocate General's opinion, this would lead to a legal vacuum in protecting the rights of data subjects if the profiling in question would not be classified as a decision falling within the scope of Article 22 GDPR. In that regard, he proposed that the controller should be responsible for answering data subject access (and rectification) requests, even if it formally does not take the final decision on granting or refusing a loan. More specifically, the controller should provide more than general information about the profiling applied to the applicant under Article 15(1)(h) GDPR. It should rather inform data subjects how the criteria were applied to them, including the respective weight given to the individual criteria.

This is likely to be a landmark case, settling questions of what constitutes automated decision-making as opposed to pure profiling, or other types of automated processing. According to a report from the court's hearing[11] the final ruling can be expected in late 2023 and may focus on two points: interpreting art. 22 as a prohibition, not a right; and interpreting the notion of a decision in a broad manner.

3.3.2 CJEU case on processing of sensitive data (OT v Vyriausioji tarnybinės etikos komisija, C-184/20)

This judgment, delivered on August 1 2022,[12] concerns the publication of data online, including sensitive data. OT, one of the parties in the case, was a CEO in a company receiving

[10] *Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) – OQ v Land Hesse* [2021] Court of Justice of the European Union C-634/21.

[11] Andreas Häuselmann, 'The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber' (*European Law Blog*, 20 February 2023) <https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/> accessed 1 March 2023.

[12] *OT v Vyriausioji tarnybinės etikos komisija* [2022] Court of Justice of the European Union C-184/20.

public funding and was thus required to submit a declaration of private interests with the Chief Ethics Commission of Lithuania. In turn, this declaration is posted online. The applicant refused to comply, arguing that the publication could trigger revealing sensitive information about their and their relatives' private lives.

The referring Lithuanian court sent two preliminary ruling questions concerning the interpretation of art. 6(1)(c), 6(1)(e), and art. 9 of the GDPR (on the legal basis for the publication and on the protection of sensitive data, respectively) in light of the fundamental rights to privacy and data protection.

The Court ruled that the publication of declarations could fall under art. 6(1)(c) of the GDPR as it is a legal obligation laid upon the Ethics Commission. However, since it constitutes an interference with fundamental rights, in addition to a legitimate legal basis, the publication obligation must also meet the other criteria of art. 52(1) of the Charter, namely necessity and proportionality. The proportionality criterion was not fulfilled in this case, since while the aim of the publication obligation was legitimate (to fight corruption), the publication of all the information was not strictly necessary to achieve that aim. Nor was the blanket publication of all the data proportionate, as it could lead to deriving (sensitive) information about the applicant and their relatives, and because it was available to an unlimited number of recipients.

Regarding the second question on sensitive data under art. 9 of the GDPR, the Court decided that the publication could be deemed to constitute of processing of sensitive data in the meaning of Article 9 (1) GDPR, because it could reveal information about the individual's sexual orientation, even where the sensitivity of the data may be only indirectly inferred. This means a broad interpretation of sensitive data as understood by art. 9 of the GDPR is now legal precedent.

3.3.3 ECHR case on the sale of health data (Y.G. v. Russia, 8647/12)

This case, decided by the European Court of Human Rights on August 30 2022[13], concerns the selling of a database, which contains sensitive health data.

The applicant who lives with HIV and hepatitis learned that as a result of a purchase his data, amongst the data of thousands of others, were available on that database in an identifiable form, including his names, address, criminal conviction and information that he has AIDS and hepatitis. He requested the government inform him why it possessed health information concerning him, to rectify the information on AIDS as he did not have AIDS and to remove the information on his hepatitis status as he had not consented to the disclosure of this information. His request to the Information Centre was denied as the agency claimed it did not have the applicant's health data, and further law suits were unsuccessful.

The applicant filed a request with the ECHR under art. 8, complaining that "the law-enforcement authorities had unlawfully collected, stored and entered his health data in a database, and that they had failed to ensure the confidentiality of his data and to carry out an effective investigation into their disclosure".

[13] *Y.g v Russia* [2022] European Court of Human Rights 8647/12.

The Court found that the government had not taken the necessary measures to ensure the confidentiality of the applicant's health data regardless of who compiled the database. Moreover, the authorities failed to investigate the complaint, even though the legal framework allowed for investigations of privacy breaches. Hence, the Russian government had failed to meet its positive obligations under art. 8 of the Convention.

4 Main requirements for fundamental rights and socio-ethical acceptance

4.1 Methodology

Information used in this deliverable has been gathered through three impact assessments by means of dedicated questionnaires (coordinating partners/technical partners/user partners) that reflect the development process through three successive waves of pilots as well as the initial questionnaire on the intended final use of the product. Since interdisciplinary projects are by definition going to run into the problem of field-specific terminology, our questionnaires were developed in collaboration with all partners, who were able to review and comment on those questionnaires before they were sent out for data gathering. We describe the process in the ***D1.5 Final version of legal and ethical monitoring***, which also contains the second and third impact assessments together with the relevant questionnaires.

The evaluation is based on two negative, and one positive assumptions:

1. TeNDER is a recommendation system **outside the notion of "automated decision-making"** as understood by art. 22 of the GDPR. The main deciding factor is who makes the decision – the system, or the human. In the case of TeNDER, the system gives general recommendations on every day health and wellness (e.g., to call a family member, to take a nap, to go for a walk…), but the final decision will always rest with the user – the patient, physician or caregiver. This is further elaborated in section 4.2.5 TeNDER as a recommendation system outside the scope of art. 22 GDPR.
2. TeNDER is a health and wellness device **and not a medical device** as understood by the MDR. It was not developed with the aim of being used for a medical purpose, such as diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, or any other goals mentioned in art. 2 of the MDR. Nor does the system present a clinical decision support. We explain the reasoning for this conclusion in the section 4.3 Regulation of medical devices.
3. TeNDER is a **health information system and a means of connecting** the patients and their caregivers **through a dedicated set of services**, as defined in deliverable *D2.2 – Report on TeNDER Service Provision*. It is a system that processes personal data of patients and caregivers in order to improve the patients' quality of life. The legal work is thus consistent with technical work and patient requirements as identified in the first year of the project.

4.2 Privacy and data protection

This section focuses on requirements under the GDPR, associated case-law and expert opinions.

4.2.1 Data processing principles

According to art. 5(1) of the GDPR, personal data shall be:

1. The principle of lawfulness, fairness and transparency; art. 5(1)a

… processed lawfully, fairly and in a transparent manner in relation to the data subject …

TeNDER involves a wide range of technologies developed and operated by different partners. The technologies are connected to each other and operated both separately and commonly as part of the TeNDER ecosystem. Additionally, the project involves different data subjects and different pilots. The variety of all these elements as well as the complexity of technologies might create difficulties for a data subject to understand the flows of their personal data and subjects involved in the processing. This affects both lawfulness and transparency of data processing.

The same mitigation measures as in the prior two waves apply, namely the prior informed consent procedures for patients (D10.3), accompanied by information sheets in the patients' own languages, as well as simplified informed consent forms.

2. The principle of purpose limitation; art. 5(1)b

… collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; […] …

TeNDER is a research project, and the purpose of personal data processing is conducting the research activities, including development, testing and piloting the technologies. Purpose limitation principle is inextricably linked to the knowledge the data subject has on the data processing. Therefore, the information sheets published in WP10 were created with layered purpose, clear description of the project and its goals in mind. The conditions of project-specific data processing (including purpose, legal basis, processing activities) have been defined separately from the existing processing activities in partners' internal organisation in order to ensure the data collected in the project context is not accidentally processed. Moreover, research projects like TeNDER can refer to the research exemption for re-use of personal data (art. 5(1)(b) and art. 89(1) of the GDPR).

3. The principle of data minimisation; art. 5(1)c

… adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed …

This principle consists of three building blocks; adequacy, relevance and necessity of personal data. Adequacy and relevance are addressed in the data management plan (WP9), which inter alia addresses the quality, interoperability and data formats, ensuring the data can be used as planned. Necessity was addressed in the three impact assessments in the context of developing functionalities without using personal data. Data that are not adequate or relevant to achieve the purposes of processing are deleted by the involved partners.

4. The principle of accuracy; art. 5(1)d

… 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 …

Accuracy of personal data, especially health and lifestyle data, is extremely important in projects like TeNDER. The system needs accurate information to perform its functions and deliver the TeNDER services.

This means that in order to ensure a more comprehensive overview of a patient's medical history, the development phase includes integrating electronic health records (EHR) into the system. This information is then matched with data from other devices in order to ensure an integrated care service. In data protection terms, this contributes to the data accuracy principle; this principle requires that personal data must be accurate and, where necessary, kept up to date, and that inaccurate personal data must be erased or rectified without delay (art. 5(1)(d) of the GDPR). When patient data is concerned, this principle is very important to ensure appropriate treatment of the patient, especially if data are going to be fed into AI systems.[14]

5. The principle of storage limitation; art. 5(1)e

… 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; […] …

This principle requires that personal data must not be kept any longer than needed to achieve a specific purpose. In research projects involving many different partners from various countries, such as TeNDER, this is a challenging principle. Due to national legislation requirements and internal policies, it is often not possible to define a consortium policy on data deletion. The general data retention policy is specified in the data management plan (D9.2), stating that "[personal] data are stored after passing pseudo-anonymization. It will not be possible to map the generated data with the original data, during a data transfer, even if one knows how the algorithm works." Detailed further answers from partners are reported in the impact assessments (T1.3). Research data that is not considered personal data may be kept for longer, depending on national and EU legal frameworks, e.g. in the context of the Open Research Data pilot.

6. The principle of integrity and confidentiality; art. 5(1)f

… 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 …

As documented in WP10 (especially D10.6 on security measures and D10.7 on pseudonymisation measures), the consortium has taken due care to ensure the security and confidentiality of the personal data processed. In the cloud storage, security, pseudonymisation and anonymization techniques have been used. Data access is protected by Keycloak authentication and authorisation mechanisms and only logged-in users with specific permissions can access it. TeNDER partners have taken high-level measures to ensure access controls and other organisational and technical measures to ensure data is not access by unauthorised parties. High-level measures are described in D10.6 and was further determined in the D2.4 (delivered M19).

7. The principle of accountability; art. 5(2)

[14] Stefanelli & Stefanelli, 'Artificial Intelligence, Medical Devices and GDPR in Healthcare: Everything You Need to Know about the Current Legal Frame' (*Lexology*, 20 March 2022) <https://www.lexology.com/library/detail.aspx?g=8cba1347-0323-4951-b9b5-69015f6e169f> accessed 7 April 2022.

According to art. 5(2) of the GDPR, the controller is responsible for and must be able to demonstrate compliance with paragraph 1 ('accountability').

Principle of accountability, foreseen by Art. 5(2) GDPR and further detailed by Art. 24 GDPR –requires the controller to put in place "appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing meets the requirements" of the law[15]. These provisions not only formalise an already existing principle of data protection law[16] (i.e., the responsibility of the controller in complying with data protection law) but also they have to be regarded as a fundamental shift in the approach to data protection. In fact, it demands the controller i) to adopt a **proactive role** in ensuring the protection of personal data through **appropriate technical and organisational measures** and ii) to be able to **demonstrate compliance** with data protection law requirements.

This shift implies a wider autonomy of the controller in deciding the means and purposes of the processing and at the same time the controller will need to further **document its choices** in order to prove its compliance with law. To this regard, controllers are recommended to **adopt**, where appropriate, **internal data protection policies** to ensure compliance with data protection rules[17].

In TeNDER, users acted as controllers, and technical partners as processors. To this end, data processing agreements were concluded prior to the pilots kick-off (early 2021). Partners further ensured their commitment to accountability principle through the impact assessments which monitored legal and socio-ethical risks during three waves of pilots.

4.2.2 Legal basis for TeNDER patients' data processing

Following the lawfulness principle of art. 5(1)(a) of the GDPR, personal data processing can only be lawful to the extent it can be connected to valid legal grounds. While art. 6(1) provides for six different legal bases, only one can be used at a time.[18]

Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; […]

In the TeNDER project, we identified legal grounds as consent from art. 6 (a), with the explicit consent from art. 9(b) as an exemption from the art. 9(a) prohibition of processing.[19] However, as many patients with Alzheimer's and Parkinson's diseases experience decrease of cognitive function, ensuring the informedness of the consent can be a challenge. While the GDPR contains special rules for *children's consent* (art. 8 of the GDPR), there is no similar rule for obtaining *informed consent from incapable adults*, nor is this addressed in the relevant

[15] Art. 24 GDPR.
[16] For a wider overview of the accountability principle in the previous framework: C. Kuner, L. Bygrave, C. Docksey, Draft commentaries on 10 GDPR articles, in Commentary on EU General Data Protection Regulation, OUP, 2019, pp. 82-98.
[17] Art. 24(2) GDPR.
[18] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (2020) 05/2020 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.
[19] Described in D10.3, which also contains informed consent forms and information sheets,.

guidelines of the EDPB[20]. To resolve this legal gap and ensure the patients were fully briefed, they were provided with both original and simplified information sheets, following bioethical recommendations contained in several (non-binding) international documents, such as the Helsinki declaration and the Council of Europe Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults. While these are not requirements for consent under binding law, they contribute to better involvement of patients with Alzheimer's in research projects.[21]

4.2.3 Processing personal data of data subjects who are not patients

Some of the devices used in the TeNDER (cameras, personal assistant etc.) can accidentally capture other people aside from the patient.

Regarding cameras, our approach was based on the GDPR and the opinion of the EDPB.[22] A video system used to process special categories of data must be based on valid legal grounds as well as a derogation under art. 9; since TeNDER is a research project, informed explicit consent from the patients was collected prior to the data processing. Adopters outside the research setting could rely on the derogation of 'scientific research purposes' under art. 9(2)(j) where obtaining explicit consent could not be feasibly done. 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". However, since accidental capture can happen to an undefined audience, relying on their consent is not realistic. In the cited guidelines, legitimate interests of the controller is suggested as an alternative legal basis; however, it cannot be relied on if the data subject's rights and interests outweigh the legitimate interest. Considering that remote care technology involves health data, it is difficult to see how that would meet the legitimate interests balancing test.[23]

Due to the lack of legal clarity, the consortium instead opted for technical and organisational measures, including:

- Consulting patients to determine their preferences about use of devices and the placement of devices (WP2). There are no hidden or surprise cameras or microphones that third parties could not be aware of.
- Using infra-red cameras instead of "regular" cameras in physiotherapy. Infra-red cameras process only skeleton outlines, without biometric data or identifying facial characteristics. They were used in physiotherapy session as part of the rehabilitation room pilot and not in other settings e.g. patients' homes or rooms.
- Several technologies developed in the project can be turned off by the patient or their caregiver/family member, without loss of functionality.

[20] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (n 18).
[21] Documented in TeNDER D1.1.
[22] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2019).
[23] Article 29 Working Party, 'Opinion 06/2014 on the "Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC"' (2014) WP217 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.

- Third party devices such as wearables are given to the patient only, and monitor only the vital signs of one patient.

4.2.4 Privacy by design and by default approaches

Data minimisation principle is operationalised by the *obligation of data protection by design and by default*, which according to art. 25 of the GDPR, obliges the controller to implement **appropriate technical and organisational measures, such as pseudonymisation, in order to meet the requirements of the GDPR and to protect the rights of data subjects**. This obligation is also relevant in integrating different tools and devices into a single service for remote care; in practice it means that the onus for ensuring data protection is on the developer, not the user.[24]

On the premise that the processing personal data partially or completely supported by IT systems should always be the outcome of a design project, Data Protection By Design[25] requires the controller to embed safeguards and mechanisms throughout the lifecycle of the application/service/product to protect the right to data protection of the data subject; whereas Data Protection by Default[26] requires the activation and application of such safeguards as default settings.

In 2020, the EDPS issued its guidelines on implementing this principle[27] aiming to provide guidance to controllers and processors. The document further describes the key aspects of Data Protection by Design and outlines three possible steps for the operationalisation thereof. These are:

1. The definition of a methodology to integrate privacy and data protection objectives as part of projects implying the processing of personal data;
2. The identification and implementation of adequate technical and organisational measures to be integrated in those processes;
3. The integration of the support for privacy within organisations through the definition of tasks and allocation of resources and responsibilities.

Since its early stage, TeNDER partners have taken care to implement data protection by design and by default principles through interdisciplinary collaboration and through end user inclusion of patients in the co-creation process, aiming to define a set of ethical, legal and acceptance requirements. This in turn enabled the project partners to build a system that does not unduly put the burden of ensuring privacy onto the patient, but instead on the (future) controllers and processors.

Key actions in this regard have been the three **impact assessments**, which monitored the legal and socio-ethical risks and provided appropriate responses, as well as technical development

[24] See Article 29 Working Party, 'Letter to time.lex about the new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive' (2018) < https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52056>.
[25] Art. 25(1) GDPR.
[26] Art. 25(2) GDPR.
[27] European Data Protection Board, 'Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default' (2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>.

giving patients **privacy options** through manually turning the devices off and on. Regarding third parties, the principle was operationalised through the absence of covert monitoring and ensuring that only the patient's vital signs were monitored, instead of unnecessarily processing another person's data.

4.2.5 TeNDER as a recommendation system outside the scope of art. 22 GDPR

According to art. 22, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This is one of the most debated provisions of the regulation in light of the advancements in artificial intelligence technologies; as described above in section 3.3.1, a case is being heard at the CJEU to determine whether this article constitutes an ex ante ban on automated decision-making, or whether it is a right that data subjects can exercise ex post facto.[28]

What constitutes automated decision-making is explained by the expert opinion of the former Article 29 Working Party (now EDPB).[29] According to this opinion, profiling refers to automated processing of personal data to evaluate personal aspects relating to a patient (art. 4(4) of the GDPR), and patients can exercise their right to not be subject to automated decision-making in specific instances.

Profiling can broadly be broken down into two frameworks under GDPR:

(i) The taking of **significant, solely automated decisions**

(ii) General rules on **profiling**, which also apply to significant automated decisions.

Profiling is composed of three elements (see pp.6-7):

- it has to be an automated form of processing;
- it has to be carried out on personal data; and
- the objective of the profiling must be to evaluate personal aspects about a natural person.

The opinion notes that classifying individuals based on age, sex and height may not be considered profiling, since the evaluation aspect is missing.

Automated decision-making, on the other hand, is defined as the ability to make decisions by technological means without human involvement (p. 8).

Profiling may or may not lead to automated decision-making, and vice versa. There are three possible scenarios where profiling may be used:

(i) general profiling;
(ii) decision-making based on profiling; and

[28] *Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) – OQ v Land Hesse* (n 10).
[29] Article 29 Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) WP251rev.01 <https://ec.europa.eu/newsroom/article29/items/612053>.

(iii) solely automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject (Article 22(1))

The difference between the second and third examples is who makes the decision – the human or the machine.

In TeNDER only **general profiling** in the sense of the WP29 opinion is used – the purpose is to *build patient profiles based on which recommendations* are given to improve their quality of sleep or daily movement. The system cannot autonomously make any decision – rather, it is a recommendation system that helps inform the physician/caregiver and the patient who have the final say in the decision-making. Specifically, the virtual assistant will give general recommendations to improve the patient's wellbeing, such as advising to go for a walk, or take a nap. Since sensitive data have been used to create the recommender system, the project has relied on data subject's explicit consent from art. 9(2)(a), as also required by the guidelines.[30]

4.2.6 Third party service providers

The responsibility of the controller for ensuring compliance with the data protection requirements is complicated by the fact that many remote care technologies are provided by external providers. To a certain extent, the privacy risks can be mitigated by measures taken by developers and users, including patients, caregivers and organisations. These counter measures can help minimise the amount of data processed by external parties when opt-out of data sharing is not possible. Normally, the controller and the processor will adopt relevant agreements, i.e. the controller-processor agreement (art. 28(3)) of the GDPR); however, with external service providers that is sometimes not feasible, and the terms of use/terms of service apply instead.

Data protection in the wearables market calls for special attention as the functionalities of wearables become even more sophisticated, and provided for wide-ranging data collection. Personal data of the most intimate nature – activity, moods, emotions, and bodily functions – can be combined with other sources of data, raising such potential harms as discriminatory profiling, manipulative marketing, and data breaches.[31] The lack of data privacy protections could be addressed a greater adoption of the data protection by design principle and more transparency, especially regarding privacy policies.[32]

In TeNDER pilot sites we have used fitness wearables such as FitBits, in order to follow up on patients' rehabilitation and daily routines, by tracking events such as energy expenditure, sleep and activity. The wearables were connected to smart phones and tablets, and the data from wearables was extracted in order to paint a comprehensive picture of the patient's movement.

[30] ibid 24.

[31] Centre for Digital Democracy, 'Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection' (2016) <https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf>.

[32] ibid; T Mulder and M Tudorica, 'Privacy Policies, Cross-Border Health Data and the GDPR' (2019) 28 Information & Communications Technology Law 261.

The potential access of Fitbit to the data on the device and the wearable, as the service provider, has been identified as a challenge in the D1.4 and D1.5. The Fitbit blog provides some tips on enhancing privacy and data protection while using their services, including going incognito and editing the profile and display name, making personal stats such as birthday, height, and weight private, hiding badges, and adjusting for different location settings.[33] However, generally opting out of data sharing with the service provider is not possible. Considering the project involves very vulnerable population, additional safeguards were adopted in the process: setting up dedicated accounts, email addresses, using devices specifically for the project purposes, and no real names or specific dates of birth were used insofar that was possible. This contributes to the implementation of the principle of data minimisation, set in art. 5(1)(c) of the GDPR, which is one of the keystones of privacy and data protection by design.[34]

4.3 Regulation of medical devices

While many technological tools can be used in a medical context, not every such tool will qualify as a medical device under the Medical Devices Regulation (MDR).[35]

The MDR applies to the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU (art. 1(1) of the MDR), as well as to the groups of products without an intended medical purpose that are listed in Annex XVI, such as contact lenses, substances or items used for facial filling, or equipment that delivers electrical currents to the cranium (art. 1(2) of the MDR). The regulation also applies to devices with both a medical and a non-medical intended purpose, which must cumulatively fulfil the requirements applicable to devices with an intended medical purpose and those applicable to devices without an intended medical purpose (art. 1(3) of the MDR).

Medical device is defined as (art. 2(1) of the MDR):

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,

[33] https://blog.fitbit.com/fitbit-privacy-settings/ and https://blog.fitbit.com/go-incognito/ (both accessed 28/03/2022).

[34] Norwegian Consumer Council, 'Consumer Protection in Fitness Wearables' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf>; European Data Protection Board, 'Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default' (n 27).

[35] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC 2020.

- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
- and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices (art. 2(1) of the MDR):

- devices for the control or support of conception;
- products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) (i.e., medical devices, accessories for medical devices, and products listed in Annex XVI) and of those referred to in the above points.

Possible classification as a medical device under the MDR thus depends on the purpose for which the tool had been built. Namely, art. 2(1) of the MDR states that any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used for a specific medicinal goal, such as monitoring. Following the reasoning of CJEU's decision in the case C-219/11[36], a device is a medical device only if it was meant to be used for the purpose of investigation of a physiological process, and *a for product which is not conceived by its manufacturer to be used for medical purposes, certification as a medical device cannot be required* (par. 30 of the judgment).

It is worth noting that under art. 2(1) of the MDR, software is considered a medical device, insofar it meets one of the medical purposes mentioned. Indeed, medical AI may well fall under the scope of the MDR as well as the AI act as it currently stands. However, product owners should not neglect their transparency and accountability obligations when building software of AI meant to be used for medical purposes.[37]

Clinical decision support (CDS) technologies likewise fall under the scope of the MDR. CDS is defined as "any software system that integrates personal patient data with external sources of medical knowledge to assist healthcare professionals in their decision-making process"[38] However, unlike the practice of the regulatory agencies in the United States, the EU has not been very active in regulating the risks of clinical decision systems as of 2022.[39]

On the other hand, wearables are widely considered[40] not to fall under the regime in the MDR unless they had been specifically designed for a specific medical purpose. In all other cases,

[36] *Brain Products GmbH v BioSemi VOF, Antonius Pieter Kuiper, Robert Jan Gerard Honsbeek, Alexander Coenraad Metting van Rijn* [2012] Court of Justice of the European Union C-219/11.
[37] Anastasiya Kiseleva, 'AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability?' (2020) 4 European Pharmaceutical Law Review 5.
[38] Reed T Sutton and others, 'An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success' (2020) 3 npj Digital Medicine 1.
[39] Sven Van Laere, Katoo M Muylle and Pieter Cornu, 'Clinical Decision Support and New Regulatory Frameworks for Medical Devices: Are We Ready for It? - A Viewpoint Paper' (2022) 11 International Journal of Health Policy and Management 3159.
[40] Jan Benedikt Brönneke and others, 'Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring' (2021) 21 Sensors 4937; 'Smart Wearables Regulations in the EU - Omcmedical.Com' (*Medical O. M. C.*, 19 July 2022) <https://omcmedical.com/smart-wearables-regulations-in-the-eu/> accessed 20 March 2023; Fabian Nagtegaal and others, 'Internet of Things.

such as wearables that are used for fitness and lifestyle decisions, the MDR is deemed to not apply. Further, the court states in para. 31 of the Brain Products judgment that if sports goods that enable performance measurement without any medical use were required to seek a certification procedure in accordance with the MDR, there would be no justification for such a requirement.[41]

For these reasons, we consider that TeNDER is not a medical device. It was not designed to pursue a medical outcome, but rather to rely on the use of wearables and other general purpose technology in order to connect caregivers and patients and improve the latter's quality of life.

However, all of the above does not mean that technologies that serve to aid patients could never fall under the scope of the MDR. If such a technology is built with the purpose of allowing investigation of a physiological process, then it falls under the rules of the regulation. An example could be custom-made software, developed to support clinical decisions to care for patients remotely, or devices meant to warn about insulin deficiencies, or blood pressure monitors which send reports to the doctor.[42][43] Nor is it entirely unlikely that a component of TeNDER could be used a part of a medical device in the future. For those cases, we provide recommendations below.

4.4 Other key legal and socio-ethical areas

As a health technology research project, TeNDER has crossed a number of different legal frameworks outside of the GDPR and the MDR. Below, we discuss some additional implications.

4.4.1 The bioethical approach: beyond compliance

The overarching approach in TeNDER has been to go beyond mere compliance with applicable legal frameworks. Since the beginning, patients have been involved in the co-design process (WP2) which allowed the technical partners to develop technologies and functionalities in line with the patients' wishes and motivations.

Furthermore, bioethical principles were also considered in the design of consent procedures. Since many patients with Alzheimer's and Parkinson's diseases experience decrease of cognitive function, ensuring the informedness of the consent has been one of the main requirements of the TeNDER system. While the GDPR contains special rules for *children's consent* (art. 8 of the GDPR), there is no similar rule for obtaining *informed consent from*

Wearable Technology' (Business Innovation Observatory 2015) Case study 44 <https://ec.europa.eu/docsroom/documents/13394/attachments/3/translations/en/renditions/native>.

[41] *Brain Products GmbH v BioSemi VOF, Antonius Pieter Kuiper, Robert Jan Gerard Honsbeek, Alexander Coenraad Metting van Rijn* (n 36).

[42] https://www.insiderintelligence.com/insights/remote-patient-monitoring-industry-explained/ (accessed 28/03/2023).

[43] Under the revised MDR, the Commission has set up a database of authorised medical devices, which can be accessed at https://ec.europa.eu/tools/eudamed/#/screen/home (accessed 28/03/2023). Using the search query "remote monitoring" or "remote" under device nomenclature the database reveals inter alia products that help monitor cardiac events and smart ingestible pills.

incapable adults, nor is this addressed in the relevant guidelines of the European Data Protection Board (EDPB).[44]

To resolve this legal gap and ensure the patients were fully briefed, they were provided with both original and simplified information sheets, following bioethical recommendations contained in several (non-binding) international documents, such as the Helsinki declaration[45] and the Council of Europe Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults[46]. When necessary, a trusted representative could accompany the patient when expressing the will to participate in the project. While none of these are requirements for consent under binding law, they contribute to better involvement of patients with Alzheimer's in research projects.[47]

Further details on the consent procedure can be found in the WP10, specifically D10.2, D10.3 and D10.4.

4.4.2 Explainable AI

This is an emerging field of law that asks a fundamental question: is there a right to an explainable AI? Whether the GDPR contains such a right is unclear,[48] though some aspects may be answered by the pending CJEU case C-634/21 (see section 3.3.1). However, the proposed AI act does contain some explainability requirements. The covered entities have transparency obligations that permit a user to understand the overall operation of the algorithm, its weaknesses, how it was developed and trained, and its approved use environments – the so-called "global explainability". On the other hand, "local explainability", referring to a specific person's ability to understand the algorithmic decision, is missing in the proposal.[49]

In the TeNDER project, the explainability has been underpinned by patient-led co-design process (WP2), data protection documentation available in patients' first languages and/or simplified formats (WP10), and building a recommendation system instead of automated decision-making one, which could have led to the black-box problem.

4.4.3 Additional usability requirements

[44] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (n 18).
[45] World Medical Association. *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects* (June 1964).
[46] Council of Europe. *Principles Concerning the Legal Protection of Incapable Adults: Recommendation No. R (99) 4* (23 February 1999).
[47] Alzheimer Europe, *Understanding dementia research,* https://www.alzheimer-europe.org/research/understanding-dementia-research (last visited 15/03/2023).
[48] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 Harvard Journal of Law & Technology (Harvard JOLT) 841.
[49] Centre on Regulation in Europe, 'Towards an EU Regulatory Framework for AI Explainability. Key Takeaways from CERRE Event' (Centre on Regulation in Europe 2022) <https://cerre.eu/wp-content/uploads/2022/11/AI-Explainability-3-Pager.pdf>.

Based on general bioethical principles, the project developed alongside a number of usability requirements aimed to ensure safety and accessibility of TeNDER services. As described in the impact assessments, the physical tools are designed in a way that seeks to minimise physical or mental harm to the patient. Inter alia, this includes teaching patients how to use smartphones, using patient-friendly interfaces in the app, and involving a caregiver (formal or informal) that checks whether the device is functioning normally, as well as professional support to patients and carers to make appropriate use of technology and to resolve doubts.

4.5 Conclusions

As discussed in the methodology section, the above evaluation was based on three assumptions:

> **First**, TeNDER is a recommendation system outside the GDPR's notion of automated decision-making, since it ensures the final decision will always rest with the human user.
>
> **Secondly**, TeNDER is a health and wellness devices outside the scope of the MDR, since it does not aim to diagnose, prevent, monitor, predict etc. an illness or disability by itself. Instead, it helps the patient and the caregiver to monitor the former's vital signs and connect with the latter.
>
> **Finally**, TeNDER is a health information system based on a dedicated set of services, which process patients' personal data to improve their quality of life.

The conclusions found herein can serve to inform future developers of integrated care systems, such as TeNDER.

4.5.1 The main legal and ethical requirements

1. Privacy and data protection

We present key considerations under the GDPR as the overarching legal regime, taking into account the above assumptions. The requirements contained herein should be considered a summary of the above analysis and are by no means exhaustive, as controllers may be bound by other laws and regulations on EU or national level, as well as industry standards and/or obligations given by research bodies.

Table 2: Essential data protection and privacy requirements for integrated care systems

Requirement no.	Description	Comment
PDP1	Complying with the fundamental principles of data processing (art. 5(1) of the GDPR)	Need to ensure that processing of personal data complies with the **fundamental principles** of art. 5(1) of the GDPR – **lawfulness, fairness and transparency; purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality**.

PDP2	Accountability of the data controller (art. 5(2) + 24(1) of the GDPR)	The data controller is the entity who determines the means and purposes of processing. In the project, the user partners acted as controllers; on the market, the adopters such as healthcare organisations are going to act in this role. Data controllers are responsible for ensuring the fundamental principles are respected (**the accountability principle**). In the case of TeNDER, the user partners acted as controllers, and the technical partners as processors, as stated in the data processing agreements provided in the WP10.
PDP3	Legal basis for processing patients' sensitive personal data (art. 6 + 9 of the GDPR)	Patients' data, considered to be sensitive data in the sense of art. 9(1) of the GDPR, are processed based on their **explicit consent**, which is one of the exceptions from art. 9(2) GDPR. While there is no specific regime in the GDPR for **adults experiencing cognitive decline**, the consortium decided to adopt additional safeguards based on expert recommendations, such as simplified consent forms and involvement of a trusted representatives, where necessary. The **lack of legal safeguards** for incapable adults is, in our opinion, one of the most important legal gaps the project has faced. We suggest recommendations to improve the legislative framework in section 5.2.1.
PDP4	Ensuring proportionality of third parties' (visitors, care givers, other patients etc.) data processing despite incidental capture (art. 6(1) of the GDPR)	Ensure third parties' privacy is not disproportionately affected. Processesing personal data of other **persons who are not the target patient** (incidental capture) through the use of video and other devices. Since it is not clear what the legal basis

		for processing of third party data through incidental capture in patient care is, the consortium decided to adopt technical and organisational measures aimed at fostering the privacy of third parties. These measures include patient consultations, using infra-red cameras, options to turn the devices off, etc.
PDP5	Data protection/privacy by design and by default (art. 24 + 25 of the GDPR)	Adopting **the privacy/data protection by design and by default approach**, where protecting patients' data takes centre place in the development and testing process. A key outcome of this process is the (data protection) **impact assessment**, which were documented in D1.4 and D1.5 (First and final version of legal and ethical monitoring, respectively).
PDP6	No automated decision-making (art. 22 of the GDPR)	Ensuring that the **decisions are taken by a human, and not the system**, if the decision could have legal or other important impacts on the patient. While TeNDER can provide lifestyle and wellness recommendations, the final decision shall always remain with the human.
PDP7	Privacy and third party service providers (art. 5(1)(c) + 25(2) of the GDPR)	When **third party technologies or services** are used which could have a detrimental effect on patients' privacy, **mitigation measures** can be taken. Such measures include but are not limited to: setting up dedicated accounts, email addresses, using devices specifically for the project purposes, and not using real names or specific dates of birth etc.

2. Medical devices regulation and exclusion from its scope of application

The second assumption focuses on the TeNDER system falling outside the scope of application the MDR. As stated in the case-law,[50] the intention of the developer is the determining factor in assessing whether the device is a medical device or not. In the case of TeNDER, the system is not designed with a medical aim in mind, and thus does not fall under the scope of application of the MDR. However, it is possible that certain parts of functionalities of an integrated care system could be used in conjunction with other devices to form a medical device in the future.

The table below assumes that the integrated care developers wish to design a system that supports the patient, but does not in itself have a medical goal, such as diagnosis or alleviation of a disease or disability.

Table 3: Self-assessment test whether the integrated care system falls outside the scope of the Medical Devices Regulation

Requirement no.	Description	Comment
MD1	Is the device meant for human use, or an accessory thereof? (art. 1(1) of the MDR)	Only devices meant for human use fall under the scope of the MDR.
MD2	Does the device pursue a medical goal?	Medical goal such as: a) diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease b) diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability c) investigation, replacement or modification of the anatomy or of a physiological or pathological process or state d) providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations.

[50] *Brain Products GmbH v BioSemi VOF, Antonius Pieter Kuiper, Robert Jan Gerard Honsbeek, Alexander Coenraad Metting van Rijn* (n 36).

MD3	In case of medical software used in integrated care system, is the product a 'Software' according to the definition of MDCG 2019-11	Medical software is defined as 'software that 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'. If the answer is no, the software in the integrated care system is not considered a medical device.
MD4	Same as above, is it a MDR Annex XVI device?	Annex XVI counts as medical devices the following devices: contact lenses, products that are inserted into the human body through a surgically invasive procedure, equipment intended for brain stimulation etc. If the answer is no, the software in the integrated care system is not considered a medical device.
MD5	If any above questions are answered "yes", was the device conceived by its manufacturer to be used for medical purposes?[51]	Unless the device is conceived with such a purpose, it does not need to seek certification as a medical device.
MD6	Is the device a wearable fitness device, such as a Fitbit?	In the EU, fitness wearables are not considered medical devices under the MDR, except for when used in conjunction with Fitbit's ECG app.[52]

3. Socio-ethical considerations, including bioethical requirements beyond compliance, explainable AI and usability

The TeNDER approach has gone beyond the minimal requirements laid down by applicable laws.

Table 4: Socio-ethical requirements for integrated care systems

Requirement no.	Description	Comment
SOE1	Informed consent procedure	Ensure patients can understand what their consent entails, taking into account the state of

[51] ibid.

[52] See the manufacturer's website https://www.fitbit.com/global/uk/legal/terms-of-service and https://medicaldevicescommunity.com/md_news/fitbit-to-launch-first-ecg-app-in-u-s-europe-next-month/

		their cognitive understanding. If necessary, a trusted representative can take place in the process, or simplified consent forms can be provided.
SOE2	Explainable AI: prevent "surprise decisions" for the patient	Where the decision is made by the system, ensure the patient can understand what the decision entails. Patient co-design and appropriate documentation provided to the patient or the caregiver can contribute to the transparency.
SOE3	Minimise the potential harm to the patient	Minimising mental, physical or emotional harm stemming from the use of technologies. This may entail training the patients to use the devices, or designing appropriate use-friendly interfaces to facilitate the use of technology.
SO4	Ensure the device is functioning as planned	Train the patient or the caregiver and give them technical support, to ensure the device is functioning properly.

4.5.2 Legal gaps identified

The project TeNDER has identified the following gaps in the governing legal frameworks. We provide policy recommendations in section 5.2.

1. There is no specific regime for (**older) adults who are experiencing cognitive decline**. This could be detrimental to ensuring they can fully understand what they consent to in research projects, as informativeness is one of the key components of valid consent under the GDPR.[53]
2. **Incidental capture in health and patient care when using video devices**. Since video inherently captures sensitive personal data, and the audience is undefined, reliance on explicit consent is not feasible. Nor can legitimate interests be relied on, since the processing of sensitive data is unlikely to pass the test in art. 6(1)(f).
3. The **possible application of the Medical Devices Regulation** can have severe impacts on research projects. While it does not apply to TeNDER's final result, the legal uncertainty involved could lead to either unnecessary costs for the project, or trouble with regulators once the devices are placed on the market. The key questions are the applicability of the MDR to fitness wearables such as Fitbit, and the position of

[53] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (n 18).

software when it is not developed with a medical goal, but is nevertheless later used for one.

5 Recommendations

5.1 Recommendations to future adopters of TeNDER

In this section, we provide guidance to future adopters based on lessons learned in TeNDER.

Disclaimer: the recommendations herein may not cover all use-cases present in a post-project scenario, as that is impossible to determine. Integrated or remote care technologies can be used in many different contexts, depending on the type of organisation (hospital, GP, among family members, patient support groups …); in one or several different countries at once, or perhaps specific TeNDER services only. The specific manner of use may prompt the application of e.g. Patients' Rights Directive[54] in case of cross-border health care, or Clinical Trials Regulation[55] in case of a sponsored clinical trial involving patients using TeNDER devices. Depending on the type of organisation, the adopter may also be covered by the Data Governance Act or the emerging European Health Data Space Regulation.[56]

Whatever the use-case in question, we advise the adopters to keep up legal and ethical monitoring, for which the TeNDER impact assessment templates can be used. Studies point out that monitoring legal challenges is necessary due to changes in communication between patient and practitioner, changing access to care delivery services and patient interaction with telehealth tools.[57] Nor are all types of health services appropriate to be performed remotely, considering especially the elderly population is less likely to own a smartphone or have internet connection that is sufficient for digital health activity.[58]

We also encourage future adopters to use TeNDER products in a manner that supports the patients' autonomy and privacy, in line with the principles of beneficence, non-maleficence and justice; to use the technologies in a manner that supports quality of life for patients with complex diseases; and to refrain from using them in a manner which could exclude patients from receiving quality (health) care for any reason whatsoever.

5.1.1 Responsible implementation of patient data protection

1. <u>Data protection by design and by default approach</u>

[54] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare 2011 (OJ L 88).

[55] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance 2014 (OJ L).

[56] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space (n 4); Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) 2020 [COM(2020) 767].

[57] Craig E Kuziemsky and others, 'Ethics in Telehealth: Comparison between Guidelines and Practice-Based Experience -the Case for Learning Health Systems' (2020) 29 Yearbook of Medical Informatics 44.

[58] European Parliamentary Research Service, 'The Rise of Digital Health Technologies during the Pandemic' (European Parliamentary Research Service 2021) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690548/EPRS_BRI(2021)690548_EN.pdf>.

Key underlying principle of TeNDER design has been to prioritise privacy and data protection from the beginning to the end of the development process.

With Art. 25, GDPR has formally introduced the principles of **Data Protection by Design** and **Data Protection by Default** within the EU data protection legal framework**.**

On the premise that the processing personal data partially or completely supported by IT systems should always be the outcome of a design project, Data Protection By Design[59] requires the controller to embed **safeguards and mechanisms throughout the lifecycle** of the application/service/product to protect the right to data protection of the data subject; whereas Data Protection by Default[60] requires the activation and application of such **safeguards as default settings**.

The guidelines issued by the European Data Protection Board[61] aim to provide guidance to controllers and processors for the implementation of the principle. The document further describes the key aspects of Data Protection by Design and outlines three possible steps for the operationalisation thereof. These are:

1. The definition of a **methodology** to integrate privacy and data protection objectives as part of projects implying the processing of personal data;
2. The identification and implementation of adequate **technical and organisational measures** to be integrated in those processes;
3. The integration of the support for privacy within organisations through the definition of tasks and allocation of resources and responsibilities.

Adopters can therefore continue to implement appropriate technical and organisational measures, such as pseudonymisation, 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. They should also keep in mind the elderly population's gap in technical and digital skills. Thus, in practice it means that the onus for ensuring data protection is on the controllers (adopters), not the user.

2. The identity of the controller

The data controller is the entity responsible for general compliance with the GDPR. Hence, it will be very important to determine who the data controller in a market scenario is.

The data controller is a central entity in charge of the processing activity, which determines the purposes and means of the processing (art. 4(7) of the GDPR). In order to process data, a controller must comply with data quality principles, such as data minimization and accuracy (art. 5(3) and 5(4) of the GDPR, respectively), and ensure the existence of valid legal grounds as per art. 6 of the GDPR. Controllers can engage processors to help them carry out the processing operation—art. 4(8) of the GDPR defines a processor as a natural or legal person,

[59] Art. 25(1) GDPR.
[60] Art. 25(2) GDPR.
[61] European Data Protection Board, 'Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default' (n 27).

public authority, agency, or other body which processes personal data on behalf of the controller.

Since TeNDER relies on different technologies and different service providers, defining the controller and the processor may be difficult. Recent decisions of the Court of Justice of the EU, such as *Wirtschaftsakademie*[62] and *Fashion ID*[63] as well as advisory opinions[64] point to an "essential means" test. Essential means are key elements which are closely linked to the purpose and the scope of the data processing, such as whose data will be processed, which data types, for how long and who shall have access to them. The entity that determines the essential means of processing is therefore the data controller.

Determining the controller is important for ensuring that the right party can demonstrate compliance with the applicable principles and obligations ("accountability" —art. 5(2) of the GDPR). Among them are the data quality principles of art. 5(1): lawfulness, fairness and transparency; purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality. The controller is further responsible for implementing appropriate technical and organizational measures ensuring compliant processing (art. 24(1) of the GDPR), and for building privacy into the system by design and by default (art. 25(1)-(2) of the GDPR). Moreover, proactively implementing data protection during the development process helps eventual adopters in ensuring compliance, especially with the data protection by design approach.[65]

The entity using the TeNDER system (whether a GP, or a hospital, or other) is likely going to be considered the controller – the key factor is that it determines the essential means by inter alia, deciding to use the TeNDER system. Whether TeNDER technical partners remain processors will depend on what their level of access to the personal data in the system will entail.

3. Data protection impact assessment

Key means of showing responsibility for compliance is **carrying out a data protection impact assessment** under art. 35 of the GDPR. According to WP29,[66] DPIA is a "process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing them and determining the measures to address them".

[62] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, ECLI:EU:C:2018:388 (June 5, 2018).

[63] Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, ECLI:EU:C:2019:629 (July 29, 2019).

[64] Eur. Data Prot. Bd., Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, (2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.

[65] Ann Cavoukian, 'International Council on Global Privacy and Security, By Design' (2016) 35 IEEE Potentials 43.

[66] 'Article 29 WP - 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'.

The DPIA is a requirement set by Art. 35 GDPR and it is mandatory when a type of processing is '**likely to result in a high risk'** to the rights and freedoms of natural persons. In this process, the controller must carry out an evaluation of the risks associated with a processing of personal data and define the measures needed to mitigate the envisaged risks.

When processing is done on a large scale of special categories of data referred to in Article 9(1), it is likely to result in a high risk (art. 35(3)(c)), this necessitating a data protection impact assessment. In the TeNDER research, it was deemed necessary to perform and DPIA, and the same will likely be required from TeNDER adopters.

The TeNDER impact assessment template can be used for the DPIA performed by adopters; several other methodologies and templates for carrying out a compliant GDPR are also available online, for example by the CNIL (the French data protection supervisor),[67] by the Luxembourg data protection authority,[68] or by the European Commission.[69] Furthermore, a comprehensive DPIA can be created by any organisation with sufficient skills and knowledge, or outsourced to a third party, for example a law firm. Whatever the choice, a DPIA must contain at least (Art. 35(7) of the GDPR):

1) a systematic description of the envisaged processing operations and the purposes of the processing, including, the legitimate interest pursued by the controller (the organisation using TeNDER);

2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

3) an assessment of the risks to the rights and freedoms of data subjects referred to in Article 35(1); and

4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

In other words: an organisation must map the high-risk processing activities, assess whether they are necessary and proportionate (i.e. whether a less intrusive measure would have been possible), the risks such processing poses, as well as the counter-measures against the risks.

When carrying out a DPIA, several departments will likely be involved – legal service, IT department, the DPO, if the organisation has one; potentially also the HR and employees' representatives. Constant dialogue between the stakeholders involved is a necessary condition for a comprehensive and effective DPIA.

It is important that the DPIA be constantly re-assessed and updated in order to take into account potential new risks and monitor whether the existing measures are still an appropriate response to them.

[67] CNIL's website section on DPIA: https://www.cnil.fr/en/guidelines-dpia.
[68] CNPD's website section on DPIA: https://cnpd.public.lu/en/actualites/international/2017/04/G29-pleniere-avril.html.
[69] European Commission's website on data protection for SMEs: https://ec.europa.eu/justice/smedataprotect/index_en.htm.

4. Legal basis: best practices for consent

Given the legal gaps in regulation of older adults' consent for data processing, our main recommendation for adopters is to go beyond the law, and adhere to bio-ethical principles of autonomy, beneficence and non-maleficence. The consent procedures used in TeNDER can inform practice in two ways: first, the adopters can opt to involve a patient's trusted representative in the process, which can help the patient feel empowered; secondly, clear and accessible language used in our simplified consent forms can be adjusted to the specific patient's level of understanding.

5. Proportionality and the use of intrusive technologies

Depending on the specific TeNDER service used by the adopter, the patients may see the technologies used as potentially intrusive. This could especially be the case if cameras are used, or if the patient is monitored inside their home, including their private room at the care facility or the hospital. During the TeNDER pilots, following the patients' wishes, the cameras were only used for physiotherapy sessions, and they only recorded the skeleton outlines. Thus, the impact on patients' privacy and discomfort was significantly lessened. Adopters can therefore follow the same approach: consult with the patients on their preferences regarding video monitoring, place the device so that it is not hidden to the patient, ensure the devices can easily be turned off by the patient.

We provided some guidelines on video monitoring in the D1.4, based on the GDPR and the EDPB guidelines.[70] The guidelines refer to the legal basis for data processing, conditions for data storage and data erasure, transparency and information obligations, as well as an overview of technical and organisational measures to foster data protection by design approach. The research exemption implications only apply insofar TeNDER is used in another research project. Furthermore, adopters should keep in mind that the use of cameras is largely regulated by national laws, which may impose additional requirements upon the operators.

5.1.2 Fundamental cybersecurity considerations

Preventing and mitigating cyberattacks can be a concern for developers and users of integrated care. Here we provide recommendations based on two frameworks: GDPR, NIS directive, while the potential relevance of the MDR is discussed in the next section.

Art. 32 of the GDPR is concerned with the security of personal data. Both the controller and the processor are required to implement appropriate technical and organisational measures given the risk, 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. Some examples the article gives for appropriate measures are encryption and pseudonymisation, continuous security assessment, availability of systems despite a breach etc. (art. 32(1) of the GDPR). In case of a personal data breach, according to art. 33 of the GDPR the controller must notify the competent authorities without undue delay, i.e. not later than 72 hours after having become

[70] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (n 22).

aware of it, and under certain conditions notify the data subject as well, as per art. 34 of the GDPR.

The notion of risk, which pervades many obligations under the GDPR, is related to the risks to fundamental rights – especially when it may result from personal data processing which could lead to physical, material or non-material damage, including in cases when data concerning health or related to health evaluation are concerned (according to rec. 75 of the GDPR, and further developed by the Article 29 Working Party[71]). In remote care, the risks concern the rights and freedoms of vulnerable population, the patients whose personal data, especially data concerning health are being processed. Hence, the level of security measures must necessarily be high: authorisation and authenticated access to personal data and processing equipment, the principle of data minimisation, support of forgetting functionality, and data pseudonymisation to the highest extent possible and anonymisation where possible.

Adopters should also assess whether they fall under the NIS (Network and Information Security Systems) directive:[72] the act of using integrated care technologies will not bring an organisation under the ambit of the directive, though healthcare organisations may fall under it by virtue of the services they provide.

Under the NIS directive, operators of essential services[73] must comply with certain obligations. Entities in the health sector count as operators of essential services if they cumulatively meet three criteria (art. 5(2) of the NIS): (1) they provide a service which is essential for the maintenance of critical societal and/or economic activities; (2) provision of that service depends on network and information systems; and (3) an incident would have significant disruptive effects on the provision of that service.

An operator must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations, and to prevent and minimise the impact of accidents, according to art. 14 of the NIS directive. Furthermore, in case of an incident having a significant impact on the continuity of the essential services it provides, the operator must inform the competent authorities; the authorities can issue binding instructions in case of security deficits in order to remedy the deficiencies (art. 15(3) of the NIS directive).

Organisations such as hospitals who use TeNDER may well qualify as operators of essential services, if they meet the three above criteria. However, it is unlikely that the act of using a care system in itself could trigger the application of the NIS framework. TeNDER can be said to fall under the definition of the network and information system – understood as any device (or group of interconnected or related devices) which performs automatic processing of digital data by a program, it would be difficult to see patient care performed on a small scale as a critical societal or economic activity.

[71] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA)' (2017) wp248rev.01 29 <https://ec.europa.eu/newsroom/article29/items/611236/en>.
[72] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union 2016 (OJ).
[73] In the NIS II proposal replaced by 'important and essential entities'.

5.1.3 Medical devices considerations

As we explain above, TeNDER should not be considered a medical device. However, it could in the future be used as a part of software or AI for a medical goal, and would thus no longer qualify as stand-alone software in the meaning of the MDR.[74] This might imply the application of the MDR to the software in which TeNDER components are used.

Inter alia, such software would need to comply with the cybersecurity obligations, undergo clinical investigations, post-market surveillance and other requirements laid out in the MDR.

The cybersecurity obligations are risk-based – risk is defined in art. 2(23) of the MDR as the combination of the probability of occurrence of harm and the severity of that harm. The obligations apply not to users of devices but to their manufacturers,[75] i.e. the natural or legal persons who manufacture or fully refurbish a device or have a device designed, manufactured or fully refurbished, and market that device under its name or trade mark (art. 2(30) of the MDR).

Manufacturers of medical devices must also comply with certain cybersecurity obligations, depending on the applicability of the MDR.

Technologies used in remote care that do fall under the ambit of the MDR do need to comply with its cybersecurity obligations. The latter are risk-based – risk is defined in art. 2(23) of the MDR as the combination of the probability of occurrence of harm and the severity of that harm. The obligations apply not to users of devices but to their manufacturers,[76] i.e. the natural or legal persons who manufacture or fully refurbish a device or have a device designed, manufactured or fully refurbished, and market that device under its name or trade mark (art. 2(30) of the MDR).

Manufacturers must comply with a number of cybersecurity obligations, which can be split into pre-market and post market obligations. The principle of security-by-design underpins the development of the device and its marketing, complementing the principles of safety and effectiveness of the medical device.[77] Among the pre-market cybersecurity obligations are: secure design of the device, establish risk control measures; validation, verification and risk assessment (Annex I to the MDR), technical documentation (in Annex II and III to the MDR), conformity assessment (art. 52 of the MDR). Post-market cybersecurity obligations include

[74] Defined as "software which is not incorporated in a medical device at the time of its placing on the market or its making available" - 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

[75] The group clarifies that while the MDR addresses other stakeholders as well, for example importers, refurbishers and operators, the responsibility for implementing cybersecurity measures and the security-by-design principle rests firmly on the manufacturer, although the manufacturer should always take into account the others' interests throughout the development process.. See Medical Device Coordination Group Document, 'Guidance on Cybersecurity for Medical Devices' (European Commission 2019) 12–14 <https://ec.europa.eu/docsroom/documents/41863>.

[76] The group clarifies that while the MDR addresses other stakeholders as well, for example importers, refurbishers and operators, the responsibility for implementing cybersecurity measures and the security-by-design principle rests firmly on the manufacturer, although the manufacturer should always take into account the others' interests throughout the development process.. See ibid.

[77] ibid 14.

post-market surveillance, including establishing a surveillance system (art. 83 of the MDR), plan (art. 84 of the MDR), and report (art. 85 of the MDR), which must be periodically updated (art. 86 of the MDR). Vigilance duty as part of post-market obligations of manufacturers includes reporting serious incidents immediately after they have established the causal relationship between that incident and their device or that such causal relationship is reasonably possible and not later than 15 days after they become aware of the incident (art. 87(3) of the MDR).

5.1.4 Fostering trust in integrated healthcare technologies

Other relevant measures that TeNDER adopters can take to improve their users' trust in digital health technologies may include but are not limited to:

1. **Explainable AI**. Ensuring the users are aware of how the system processes their data, what is the meaningful logic behind the decision, and what it means for the patient's situation specifically. The proposed AI Act, if adopted in its current form, will require a certain level of global explainability, while the GDPR imposes an unclearly defined quasi-right to an explanation when automated decision-making is at stake.[78] We recommend adopters maintain the explainability as a key component of the system regardless of strict legal rights, with the explanation in form of factuals (in case of expected decision), and counter-factuals (in case of an unexpected decision).[79]
2. **Accessibility of apps and services**. Some adopters may be covered by the upcoming Accessibility Act,[80] which aims to ensure that disabled people can use more accessible products and services in the internal market at more competitive prices, and be presented with fewer barriers when accessing products and services (including transport, education and labour). Certain provisions, including those applicable to mobile apps and websites, will not enter into force until June 28 2025. They will apply to economic operators, who will need to comply with a set of accessibility requirements including user interface, functional design and customer support.
3. **Continue the co-design process** for any alternations to the TeNDER system, which will allow the services to cover patient needs instead of adhering to industry's for-profit concerns. Only by using patient centricity and patient design can the true potential of medicine (and thus devices used therein) be fully realised.[81]

5.2 Recommendations to policy-makers

This section describes potential legislative improvements to address legal gaps identified by the TeNDER project, which could serve to facilitate the execution of similar projects in the future, and thus to improved integrated care models within the EU. The recommendations contained herein are a result of the tasks carried out in WP1 and on the basis of the legal and ethical challenges and solutions envisaged throughout the TeNDER project.

[78] Wachter, Mittelstadt and Russell (n 48); Wachter, Mittelstadt and Floridi (n 48).
[79] Maria Riveiro and Serge Thill, '"That's (Not) the Output I Expected!" On the Role of End User Expectations in Creating Explanations of AI Systems' (2021) 298 Artificial Intelligence 103507.
[80] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance) 2019 (OJ L 151/70).
[81] Bertalan Meskó and Dave deBronkart, 'Patient Design: The Importance of Including Patients in Designing Health Care' (2022) 24 Journal of Medical Internet Research e39178.

5.2.1 Recommendation 1: Consent for adults experiencing cognitive decline

Given that the GDPR contains a specific legal regime for children, but not adults in cognitive decline, the latter's right to data protection may be at risk. We therefore advise the policy-makers to consider **implementing additional safeguards to ensure patients in cognitive decline are able to understand what their consent entails**, taking into account the recommendations of the Helsinki declaration and the Council of Europe Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults. Such safeguards should consider the ability of the person to understand (not just be informed), ensure that their participation is truly voluntary despite any cognitive limitations, and to balance their protection with their right to choose to participate. The latter could be ensured by allowing consent by proxy, or by involving a trusted representative, for example.[82]

Alternatively, in the absence of a specific binding legal regime, **internal ethical bodies** can ask for additional safeguards in research projects involving patients in cognitive decline. This option is however less desirable, as it would only apply to research project and not the industry. On the industry side, **standard-setting bodies** can also set more stringent requirements than the GDPR, for example in the field of clinical trials or clinical research.

5.2.2 Recommendation 2: Legal basis for incidental capture in patient care

Video devices used in eHealth or digital health have a high degree of possibility to capture other people ('incidental capture') apart from the patient who has consented to being included in the footage (for example, the caregiver, family members, casual visitors…). When, and under which conditions, those persons' sensitive data can be involved in the data processing, is unclear.

The EDPB's guidelines mention the options of 'scientific research purposes' under Article 9(2)(j), which should be "interpreted in a broad manner, including for example technological development and demonstration"[83], or processing necessary 'to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent'. However, these legal bases would only cover exceptional situations in hospitals, when e.g. a hospital monitors a patient for medical reasons.[84]

Neither of the two options would cover incidental capture of third parties in other situations, outside research projects or emergency care. Therefore, **policy-makers should clarify which legal basis controllers should rely on when they accidentally capture third parties' sensitive personal data**, since asking every third party for explicit consent to process data through video devices is not realistic. Nor should we rely on existent technical solutions to compensate for the lack of a comprehensive and consistent legal regime.[85]

---

[82] 'Ethical Issues' <https://www.alzheimer-europe.org/research/understanding-dementia-research/ethical-issues> accessed 29 March 2023.

[83] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (n 22).

[84] ibid 64.

[85] 'This Tech Aims to Prevent Incidental Facial Captures from IoT Devices' <https://iapp.org/news/a/this-tech-aims-to-prevent-incidental-facial-captures-from-iot-devices/> accessed 29 March 2023.

5.2.3 Recommendation 3: Integrated care systems and Medical Devices Regulation

Research project that develop integrated care technologies risk falling under the provisions of the MDR, which could have significant impacts on the project's budget and organisational considerations. The lack of legal certainty is due to several factors; in the case of TeNDER the question was raised due to the inclusion of wearables and using software/AI in a health context. While wearables as lifestyle devices are explicitly not medical devices,[86] arguments have been made that they should be. This is due to the blurred lines between wellness and health, and the increasing reliance of clinical and academic research on data from wearables, and that qualifying fitness wearables such as Fitbits might enable better health data readings and improved data accuracy.[87] Furthermore, it is not clear whether the upcoming EHDS regulation will apply to fitness wearables, which could likewise have a significant effect on research projects in the field of integrated care.

We therefore ask the policy-makers to **clarify whether combining fitness wearables with medical software outside the meaning of the MDR could ever be considered a medical device**, and if so, **under which criteria,** and whether those criteria would **apply to research projects**. Likewise, policy-makers should clarify **whether fitness wearables will fall under the scope of the EHDS proposal** if/when it is adopted by the legislators. Legal certainty would without doubt **facilitate innovative research projects across the EU.**

[86] *Brain Products GmbH v BioSemi VOF, Antonius Pieter Kuiper, Robert Jan Gerard Honsbeek, Alexander Coenraad Metting van Rijn* (n 36).

[87] Nagtegaal and others (n 40); Lisa Eadicicco, 'Fitbit and Apple Know Their Smartwatches Aren't Medical Devices. But Do You?' (*CNET*, 14 January 2022) <https://www.cnet.com/tech/mobile/features/fitbit-apple-know-smartwatches-arent-medical-devices-but-do-you/> accessed 28 March 2022; B Stanberry, 'Telemedicine: Barriers and Opportunities in the 21st Century' (2000) 247 Journal of Internal Medicine 615.

6 References

Article 29 Working Party, 'Opinion 06/2014 on the "Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC"' (2014) WP217 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>

——, 'Guidelines on Data Protection Impact Assessment (DPIA)' (2017) wp248rev.01 <https://ec.europa.eu/newsroom/article29/items/611236/en>

——, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) WP251rev.01 <https://ec.europa.eu/newsroom/article29/items/612053>

'Article 29 WP - 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'

Brönneke JB and others, 'Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring' (2021) 21 Sensors 4937

Cavoukian A, 'International Council on Global Privacy and Security, By Design' (2016) 35 IEEE Potentials 43

Centre for Digital Democracy, 'Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection' (2016) <https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearables report_final121516.pdf>

Centre on Regulation in Europe, 'Towards an EU Regulatory Framework for AI Explainability. Key Takeaways from CERRE Event' (Centre on Regulation in Europe 2022) <https://cerre.eu/wp-content/uploads/2022/11/AI-Explainability-3-Pager.pdf>

Demetzou K, 'Introduction to the Conformity Assessment under the Draft EU AI Act, and How It Compares to DPIAs - Future of Privacy Forum' (*Future of Privacy Forum*) <https://fpf.org/blog/introduction-to-the-conformity-assessment-under-the-draft-eu-ai-act-and-how-it-compares-to-dpias/> accessed 16 September 2022

Eadicicco L, 'Fitbit and Apple Know Their Smartwatches Aren't Medical Devices. But Do You?' (*CNET*, 14 January 2022) <https://www.cnet.com/tech/mobile/features/fitbit-apple-know-smartwatches-arent-medical-devices-but-do-you/> accessed 28 March 2022

'Ethical Issues' <https://www.alzheimer-europe.org/research/understanding-dementia-research/ethical-issues> accessed 29 March 2023

European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2019)

——, 'Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1' (2020) 05/2020 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>

——, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2020) 07/2020 <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en> accessed 3 April 2022

——, 'Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default' (2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>

European Data Protection Board and European Data Protection Supervisor, 'Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' (2022) <https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf> accessed 1 April 2022

European Parliamentary Research Service, 'The Rise of Digital Health Technologies during the Pandemic' (European Parliamentary Research Service 2021) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690548/EPRS_BRI(2021)690548_EN.pdf>

Häuselmann A, 'The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber' (*European Law Blog*, 20 February 2023) <https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/> accessed 1 March 2023

Kiseleva A, 'AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability?' (2020) 4 European Pharmaceutical Law Review 5

Kuziemsky CE and others, 'Ethics in Telehealth: Comparison between Guidelines and Practice-Based Experience -the Case for Learning Health Systems' (2020) 29 Yearbook of Medical Informatics 44

Medical Device Coordination Group Document, 'Guidance on Cybersecurity for Medical Devices' (European Commission 2019) <https://ec.europa.eu/docsroom/documents/41863>

Meskó B and deBronkart D, 'Patient Design: The Importance of Including Patients in Designing Health Care' (2022) 24 Journal of Medical Internet Research e39178

Mulder T and Tudorica M, 'Privacy Policies, Cross-Border Health Data and the GDPR' (2019) 28 Information & Communications Technology Law 261

Nagtegaal F and others, 'Internet of Things. Wearable Technology' (Business Innovation Observatory 2015) Case study 44 <https://ec.europa.eu/docsroom/documents/13394/attachments/3/translations/en/renditions/native>

Norwegian Consumer Council, 'Consumer Protection in Fitness Wearables' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf>

Riveiro M and Thill S, '"That's (Not) the Output I Expected!" On the Role of End User Expectations in Creating Explanations of AI Systems' (2021) 298 Artificial Intelligence 103507

'Smart Wearables Regulations in the EU - Omcmedical.Com' (*Medical O. M. C.*, 19 July 2022) <https://omcmedical.com/smart-wearables-regulations-in-the-eu/> accessed 20 March 2023

Stanberry B, 'Telemedicine: Barriers and Opportunities in the 21st Century' (2000) 247 Journal of Internal Medicine 615

Stefanelli & Stefanelli, 'Artificial Intelligence, Medical Devices and GDPR in Healthcare: Everything You Need to Know about the Current Legal Frame' (*Lexology*, 20 March 2022) <https://www.lexology.com/library/detail.aspx?g=8cba1347-0323-4951-b9b5-69015f6e169f> accessed 7 April 2022

Sutton RT and others, 'An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success' (2020) 3 npj Digital Medicine 1

'This Tech Aims to Prevent Incidental Facial Captures from IoT Devices' <https://iapp.org/news/a/this-tech-aims-to-prevent-incidental-facial-captures-from-iot-devices/> accessed 29 March 2023

Van Laere S, Muylle KM and Cornu P, 'Clinical Decision Support and New Regulatory Frameworks for Medical Devices: Are We Ready for It? - A Viewpoint Paper' (2022) 11 International Journal of Health Policy and Management 3159

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

Wachter S, Mittelstadt B and Russell C, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2017) 31 Harvard Journal of Law & Technology (Harvard JOLT) 841

Case law:

Brain Products GmbH v BioSemi VOF, Antonius Pieter Kuiper, Robert Jan Gerard Honsbeek, Alexander Coenraad Metting van Rijn [2012] Court of Justice of the European Union C-219/11

Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, [2019] Court of Justice of the European Union C-40/17

OT v Vyriausioji tarnybinės etikos komisija [2022] Court of Justice of the European Union C-184/20

Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) – OQ v Land Hesse [2021] Court of Justice of the European Union C-634/21

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht [2018] Court of Justice of the European Union C-210/16

Y.g v Russia [2022] European Court of Human Rights 8647/12

Legal framework:

Council of Europe Recommendation No. R(99)4 on Principles Concerning the Legal Protection of Incapable Adults

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare 2011 (OJ L 88)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union 2016 (OJ)

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance) 2019 (OJ L 151/70)

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS 2021 [COM/2021/206 final]

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) 2020 [COM(2020) 767]

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space 2022 [COM/2022/197 final]

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

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC 2020

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance 2014 (OJ L)

TeNDER deliverables:

D1.1 First version of fundamental rights, ethical and legal implications and assessment

D1.4 First version of legal/ethical monitoring

D1.5 First version of legal/ethical monitoring

D5.1 First Report on the Health Record and Pathway Repository

D10.1 Procedure and Criteria Used to Identify and Recruit Research Participants

D10.2 Procedure for obtaining consent for participation in research - Final

D10.3 Informed Consent Forms & Information Sheet

D10.4 Procedure for obtaining consent of legal representatives of adults unable to give consent