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

Deliverable 1.4
First version Legal/Ethical Monitoring and Review

Work Package 1: Data protection, Ethical Impact and Interoperability

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

Grant Agreement ID: 875325

Start date: 1 November 2019

End date: 31 October 2022

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

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

Funding Scheme: IA - Innovation action

Disclaimer

The TeNDER consortium consists of the following Partners.

Table 1: Consortium Partners List

No	Name	Short name	Country
1	UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
2	MAGGIOLI SPA	MAG	Italy
3	DATAWIZARD SRL	DW	Italy
4	UBIWHERE LDA	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	Work Package 1: Data protection, Ethical Impact and Interoperability
Deliverable number	D1.4
Deliverable title	First version Legal/ Ethical Monitoring and Review
Responsible beneficiary	VUB
Involved beneficiaries	SERMAS, SKBA, UNITOV, SPO, APM
Type[1]	R
Dissemination level[2]	Public
Contractual date of delivery	M22
Last update	30 Aug 2021

[1] **R:** Document, report; **DEM:** Demonstrator, pilot, prototype; **DEC:** Websites, patent fillings, videos, etc.; **OTHER**; ETHICS: Ethics requirement; ORDP: Open Research Data Pilot.

[2] **PU:** Public; **CO:** Confidential, only for members of the consortium (including the Commission Services).

Document History

Version	Date	Status	Authors, Reviewers	Description
V0.01	21/12/2020	Draft	István Böröcz, Paul Quinn, Lisa Feirabend (VUB)	First outline of report
V0.02	14/03/2021	Draft	Danaja Fabcic Povse (VUB)	Collection of partner inputs
V0.03	14/04/2021	Draft	Danaja Fabcic Povse (VUB)	Begin data analysis
V0.04	30/04/2021	Draft	Paul Quinn, Danaja Fabcic Povse (VUB)	Internal check and review of work
V0.05	09/07/2021	Draft	Danaja Fabcic Povse (VUB)	Input in all sections and revised draft
V0.06	12/08/2021	Draft	Paul Quinn, Danaja Fabcic Povse (VUB)	Second internal check
V1.0	30/08/2021	Final	Gustavo Hernández (UPM)	Final Review

Acronyms and Abbreviations

Acronym/Abbreviation	Description
DPO	Data protection officer
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation; 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
MDR	Regulation on Medical Devices; 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
Mx	Month (where x defines a project month e.g. M8)
TeNDER	affecTive basEd iNtegrateD carE for betteR Quality of Life
Tx.x	Task
WPx	Work Package

Contents

List of Figures

List of Tables

Executive Summary

In the TeNDER project, legal and ethical work focuses on data protection and privacy, treatment of human participants in pilots, wider societal concerns, and regulation of medical devices, including their essential health and safety requirements. In this deliverable, we report on efforts carried out so far, drawing upon the applicable legal requirements and principles identified in D1.1 First version of fundamental rights, ethical and legal implications and assessment, and other relevant reports, such as ethics requirements of WP10.

The current report operationalises important data protection principles, especially accountability, informed consent, and data minimisation. **Accountability** refers to the duty of involved controllers to comply with data quality principles of art. 6 of the General Data Protection Regulation (GDPR): lawfulness, fairness and transparency; purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. We have strived to achieve accountability through definition of the roles of data controllers and processors, based on which data sharing agreements were concluded between user and technical partners as a part of pilot setup. Future impact assessments will analyse partners' compliance efforts in order to implement this principle further.

Data collection in TeNDER is based upon **informed consent** of the patients. This means that patients freely give their specific, informed and unambiguous indication that they agree to the processing of personal data relating to him or her, as required by art. 4(11) and 7 of the GDPR. Insofar sensitive personal data concerning health are processed, the consent must be explicit, as required in art. 9(2)(a).

Finally, measures to implement the principle of **data minimisation** have been taken in the context of using external services, such as Fitbit wearables. Dedicated accounts and emails have been set up for the purpose of carrying out the pilots; dedicated devices are used by participants instead of their personal devices, and approximate dates of birth are used wherever possible.

Section 3 deals with extraction of **personal data from video archives**. This report provides high-level guidelines on processing sensitive personal data, storage and erasure of data, transparency and information obligations of the controller, relevant technical and organisational measures necessary to implement privacy by design and ensure security of processing, as well as on implementation of specific provisions for use of video archives in research setting. The guidelines are based upon the GDPR and the expert opinion of the European Data Protection Supervisor (EDPB).

The final part of the report is dedicated to the first **impact assessment**. This is an exercise which helps consortium partners understand the consequences of implementation of products such as TeNDER, in the context of the first pilot. The main elements of the methodology are the following: determination of activities which require an IA; parsing out the scope of the IA; assessment of impacts; evaluation and treatment of impacts; and monitoring and review. Based on the methodology, three questionnaires have been drafted to be answered by the coordinating partners, technical partners and user partners (Annexes I, II and III, respectively). Our findings and recommendations in section 4.3 build on the partners' answers to questionnaires and will help verify whether the measures taken within

the design and implementation of the project will be sufficient to meet the requirements outlined. The application of the methodology this deliverable provides will be used to produce D1.5 Final version Legal/Ethical Monitoring and Review and D1.6 Final version of fundamental rights, ethical and legal implications and assessment, both due in M36.

Main recommendations given in the impact assessment concern the provision of relevant information to pilot participants and adjust the information digitally or verbally to keep informing the patients; ensuring further implementation of the data minimisation principle to ensure that the TeNDER system's operational configurations prevent unnecessary personal data processing; continuous consideration and review of legal and ethical requirements throughout the whole project; and conducting further impact assessments which will follow up on the preparation and execution of the second and third waves of pilots.

1 INTRODUCTION

1.1 Purpose and scope

The aim of this task is to monitor the impacts of TeNDER on the requirements identified in WP1 and WP2, as the ICT solutions are integrated, tested and evaluated. This will ensure that any new aspect or update of the TeNDER solutions or their potential application is tested against the relevant societal concerns, described in T7.1. The monitoring will be performed by VUB, who will have the right to access any information arising from the work of the project, to attend any meeting of the consortium and to interfere should it consider the work of the consortium incompatible with TeNDER.

This will ensure that the outcomes of the impact assessment are implemented by all partners, thus compliant with the relevant laws.

Monitoring compliance is an ongoing task in the TeNDER project, which began with the D1.1, First Version of Fundamental Rights, Ethical and Legal Implications and Assessment. In this deliverable, we provided the high-level overview of applicable legal framework and biomedical principles, which in turn helped identify the specific legal and ethical requirements that continue to be adhered throughout the duration of the project.

However, as D1.1 was due early in the project, we now follow up on the compliance efforts carried out until and including M21. We assess and evaluate the efforts leading up to the first wave of the TeNDER pilots in the context of the identified framework. We provide a risk-based impact assessment that seeks to address possible legal and ethical risks arising in the pilot. In this, we followed the methodology established by our work in projects ALADDIN[3], PROTEIN,[4] and FASTER.[5] The impact assessment reports on consequences of actions taken in the project, in order to identify potential benefits and adverse effects, and allow the consortium to take the most beneficial actions.[6]

1.2 Contribution to other deliverables

The findings of our work in T1.3 will feed into further legal and ethical work in the project, resulting in D1.5 Final version Legal/Ethical Monitoring and Review and D1.6 Final version of fundamental rights, ethical and legal implications and assessment, both due in M36. Two more impact assessments will be released in conjunction with the second and third pilot.

1.3 Structure of the document

First, we summarise the legal and ethical work carried out in the TeNDER project so far, with a special focus on data protection in TeNDER and specifically in Fitbit devices used in pilots. Principles, such as data minimisation, accountability and informed consent, are discussed. Then guidelines on obtaining personal data from video archives are given, based on the GDPR and the opinion of the European Data Protection Board (EDPB). Finally, the results of the impact assessment are given.

[3] https://aladdin2020.eu/
[4] https://protein-h2020.eu/
[5] https://www.faster-project.eu/
[6] D. Sarma, P. Quinn (VUB) ALADDIN D3.3, Framework for Impact Assessment Against SoEL Requirements, p. 9 ff

2 Previous legal and ethical work in TeNDER

Thorough assessment of legal, ethical and privacy aspects of TeNDER is one of the main tenets of the project. As a research project, TeNDER involves human participants (patients) whose personal data of a very intimate nature is being processed, in conjunction with technological tools, such as sensors, cameras, and wristbands. The goal of TeNDER is to provide assistive technology that will aid both patients and caregivers in managing AD, PD and CVD. As an eHealth project, it raises concerns on inclusion of human participants, processing their personal data, safety of medical devices, as well as wider societal technology safety and acceptance.

The technical work and piloting in TeNDER raise legal and ethical concerns due to inclusion of human participants, processing their personal data, safety of medical devices, as well as wider societal technology safety and acceptance of the final TeNDER product. At this stage, it is possible to make a distinction between 'TeNDER the research project' and 'TeNDER the exploitable product' as it relates to the applicability of the various legal frameworks and ethical principles, as we examined in D1.1. We follow this approach in the current deliverable as well where applicable.

The relevant framework applicable to TeNDER is:

- For involvement of human participants in the project:
  - General Data Protection Regulation (GDPR)[7] since participants are data subjects whose personal data are being processed in the context of the project.
  - EU Patients' Rights Directive[8] in the context of its data protection clause and the eHealth network it has set up.
  - Biomedical ethics contained in the Nuremberg code, the International Covenant on Civil and Political Rights, Oviedo Convention and Protocol, Helsinki Declaration and various other non-binding documents issued on international and national levels.
  - Clinical trials regulation[9] has been found not to apply to TeNDER. While the research participants involved in TeNDER pilots are taking medicinal products, this will be in the course of their existing treatment and is not something the project itself will be covering, other than offering reminders for participants to take their medication and monitoring medication intake using pill dispensers.
  - Patient autonomy, informed consent and the right to refuse to participate in biomedical research are the fundamental underlying principles. In the cases of patients who might not be able to give their full consent, additional measures following the Helsinki Declaration are suggested, such as seeking consent from an independent, appropriately qualified individual.

[7] 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)
[8] Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare ("EU Patients' Rights Directive")
[9] 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

- Data protection: principles of data minimisation, data security, accountability, and patient informed consent, which are further developed in the section 2.1. Data protection framework is extremely important since TeNDER processes intimate, sensitive personal data of patients involved in the trials.
- Broader societal and ethical aspects: frameworks regulating the uses of technologies, such as artificial intelligence (AI) and wearables are slowly emerging. When D1.1 was released, several non-binding documents and opinions already existed, such as the Ethics Guidelines for Trustworthy Artificial Intelligence, issued by High Level Expert Group on AI. In April 2021, the Commission released its proposal for an Artificial Intelligence Act,[10] which-if adopted- could become relevant in eHealth settings.
- The use of medical devices: Medical Devices Regulation[11] and the follow-up work of Medical Device Coordination Group set out the fundamental health and safety requirements medical technology must comply with in order to be marketable on the EU internal market.

Further measures have been adopted as part of WP10 – Ethics requirements. Between M5 and M12, all WP10 ethical deliverables were prepared and submitted, setting out the various procedures for recruitment of participants, the informed consent procedures and the informed consent forms. Moreover, the various intended technical and organisational security measures have been set out and a recommendation for conducting a DPIA has been provided. This work was closely connected to the work performed in WP1. Measures have been taken by TeNDER partners to protect the patients' personal data; more specifically:

1. Procedures & criteria for identifying and recruiting participants (D10.1)
2. Informed consent procedure for human participation in research (D10.2)
3. Informed consent forms in English and translated into the local languages of the pilot locations (D10.3)
4. Informed consent procedure for those incapable of providing consent (D10.4)
5. Description of technical and organisational measures to protect the fundamental rights and freedoms of data subjects (D10.5). In the context of this deliverable, data sharing agreements based on art. 28(3) of the GDPR were drafted.
6. Description of security measures in the context of electronic health records and contacts of their respective DPOs (D10.6)
7. Description of anonymisation and pseudonymisation techniques in the recruitment phase, during piloting and in the TeNDER system (D10.7)
8. Informed consent procedure for collection of personal data (D10.8)
9. Evaluation of the ethical risks relating to the data processing activities, including an opinion to conduct a DPIA (D10.9), which inter alia provides the basis for the impact assessment contained in the current document.

2.1 Data protection in TeNDER project

Data protection legislation applies when 1) personal data are 2) being processed.

[10] 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

[11] 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

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).

In the pilot activities, the data subjects will be the patients, as well as the persons in the care pathway (i.e. the caregivers), and representatives of TeNDER partners, especially those involved in the trials and their organisations' DPOs. The partners will be acting as controllers and processors, as laid out in the Data Sharing Agreements.[12]

Elementary principles of data processing are set out in art. 5(1) of the GDPR: 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).

- Lawfulness, fairness and transparency: personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.[13]
- **Purpose limitation** means that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[14] This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[15]
- Data must be collected in a way that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed according to the **data minimisation** principle.[16]
- Under the **accuracy** principle, data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[17]

[12] The Data Sharing Agreements were provided as an annex in the D1.1, Fundamental Rights, Ethical and Legal Implications and Assessment (First Version), and signed by the TeNDER partners as part of trial set-up.
[13] Article 5(1)a of the GDPR.
[14] Article 5(1)b of the GDPR.
[15] Article 29 Working Party, Opinion on Purpose Limitation, p. 4.
[16] Article 5(1)c of the GDPR.
[17] Article 5(1)d of the GDPR.

- According to **storage limitation** principle, data must be 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. It may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1).[18]
- **Integrity and confidentiality** principle requires data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[19]

Accountability means that controllers involved in data processing are responsible for, and must be able to demonstrate compliance with the above-mentioned principles. The roles of data controllers and processors were defined earlier in the project and enshrined in data sharing agreements, concluded between user and technical partners as a part of pilot setup. Future impact assessments will analyse partners' compliance efforts in order to operationalise this principle further.

Data collection in TeNDER is based upon **informed consent** of the patients, meaning "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (art. 4(11) of the GDPR). Insofar sensitive personal data concerning health are processed, the consent must be explicit, as required in art. 9(2)(a).

In the information sheets given to the participants as data subjects, the partners as data controllers have provided the data subject with all of the following information:

- the identity and the contact details of the controller,
- the contact details of the data protection officer,
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- the categories of personal data concerned,
- the recipients or categories of recipients of the personal data, if any,
- if applicable, information about transfers to third countries.[20]

The full disclosure of relevant information as part of pilot execution contributes to the exercise of data subjects' rights and enhances fairness and transparency as fundamental principles of data protection.

For patients who are unable to give consent specific procedures have been drafted. Since TeNDER intends to provide a platform that will facilitate the application of integrated care, with a specific focus toward elderly and/or chronically ill persons, such participants may well be involved in the pilots. While it is recommended not to automatically label a member of a certain group as vulnerable, some characteristics make it reasonable to assume that certain individuals are vulnerable. Participating partners assess and determine whether the potential participant has capacity to consent, or whether consent from their legal representative will

[18] Article 5(1)e of the GDPR.
[19] Article 5(1)f of the GDPR.
[20] Articles 13(1) and 14(1) of the GDPR.

need to be sought. Hence, information will be provided both to the participant, and to their representative, if applicable.

Data minimisation is one of the main guiding principles of data collection in TeNDER. Wherever possible, pseudonyms or codes are used instead of full names, e.g. in EUSurvey tool, and in wearables. All partners have cooperated on an ad-hoc basis to determine what personal data is in fact adequate, relevant and limited to what is necessary in relation to the project objectives.

2.2 Wearables and data protection

Fitness wearables, specifically FitBits, have been used on TeNDER pilot sites in order to follow up on patients' rehabilitation and daily routines. The devices track events such as energy expenditure, sleep and activity, which can help patients and people in general to live a healthier lifestyle by providing insights of how their body responds, moves, or rests, allowing them to adapt or change their daily routines. The specific device used was Fitbit Band Versa 2. The Fitbit band was chosen due to several reasons:

- The possibility of creating apps (code) that can be inserted directly in the band. This allows controlling the data flow.
- It permits us to create a TeNDER scenario that includes only the band and the smartphone, skipping the pc.
- It allows extracting raw measurements from the accelerometer, which enables us to permit a procedure called re-association, which consists in matching the patient's band with the skeletons detected by the depth sensor, avoiding use of sensitive information while improving accuracy by using multiple modalities (skeletons, acceleration, and patient's location).[21]

Wearables collect personal data in order to provide their services. 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.[22] The data collection practices of service providers vary a lot.[23]

The details of FitBit's privacy policy can be found on their website, with additional information provided for European data subjects on exercise of their rights under the GDPR, with the Irish company Fitbit International Limited acting as the data controller.[24] In order to function as necessary, Fitbit wearable device requires connection to a Fitbit account with a phone, tablet,

[21] Information taken from TeNDER D6.2, Report on first wave of pilots

[22] Centre for Digital Democracy, Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection, p. 14., https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf

[23] In 2016 the Norwegian Consumer Council issued a comparative study of consumer policies, including data sharing practices, of four providers: FitBit, Garmin, Mio and Jawbone. See Norwegian Consumer Council, Consumer protection in fitness wearables https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf

[24] https://www.fitbit.com/global/us/legal/privacy-policy#european-privacy-disclosures

or computer; the connection allows the transfer and sync of data between the account and the wearable.[25]

Since Fitbit is not a member of the consortium, and as the service provider can access all data on the device or band, the TeNDER partners decided to adopt mitigation measures in order to assure the protection of patients' personal data. Fitbit blog provides some tips on enhancing privacy and data protection while using their services, including going incognito. Fitbit allows editing the profile and display name, making personal stats such as birthday, height, and weight private, hiding badges, and adjusting for different location settings.[26]

In the project, dedicated accounts and emails have been set up for the purpose of carrying out the pilots; dedicated devices are used by participants instead of their personal devices, and approximate dates of birth are used wherever possible. These safeguards contribute to data minimisation principle since opting out of data sharing with the service provider (Fitbit) is not possible.[27] If the participants in TeNDER pilots do not possess the relevant digital skills, their caregivers or physicians can ensure the privacy-friendly options on the devices are activated.

[25] https://help.fitbit.com/articles/en_US/Help_article/1873.htm

[26] https://blog.fitbit.com/fitbit-privacy-settings/ and https://blog.fitbit.com/go-incognito/

[27] The Norwegian Consumer Council provide an interesting comparison between the four service providers on their different understanding of data minimisation and privacy by default; of the providers analysed, only Mio allows opting out of data sharing with the service providers. See Norwegian Consumer Council, Consumer protection in fitness wearables, p. 13. https://fil.forbrukerradet.no/wp-content/uploads/2016/11/2016-10-26-vedlegg-2-consumer-protection-in-fitness-wearables-forbrukerradet-final-version.pdf More research is likely necessary to understand how to maximise the use of wearables in health research in a privacy-friendly manner, considering the market is overwhelmingly run by large, US-based companies.

3 Guidelines on data protection in the use of video archives

From a data protection perspective, the use of video cameras is a data processing activity insofar it concerns video footage of individuals, or footage from which those individuals can be identified (e.g. infrared cameras). Video cameras can be used in a variety of situations, both in a law enforcement context, public security (e.g. cameras in shopping malls, warehouses, public parks), private security (e.g. antitheft home measures), as well as in healthcare setting, such as TeNDER pilots, to monitor and follow-up on patients.

According to answers submitted by user partners, in the pilots, the RGB and/or KinectAzure cameras will be used to keep track of patients' rehabilitation processes and to alert the carer should the patient fall. The cameras will collect sensitive personal data and biometrics, such as skeleton outlines. Here we provide guidelines on use of cameras, based on the GDPR and the opinion of the EDPB.[28]

3.1 Processing of sensitive personal data: lawfulness and legal grounds

Video surveillance, like any another data processing activity, must be lawful. The requirement of 'lawfulness' is a data protection principle[29] which makes clear that the processing of personal data must be based on, and limited to, a legal ground. The lawfulness requirement creates an obligation for the data controller to rely on one of the six legal grounds provided in article 6 of the GDPR.

Processing of sensitive data is on principle prohibited. Exceptionally, the processing of the sensitive personal data concerning health is allowed in specific situations provided for by article 9, 2 of the GDPR.[30]

When a video surveillance system is used in order to process special categories of data, as might be the case in TeNDER, the data controller must identify both an exception for processing special categories of data under Article 9 as well as a legal basis under Article 6.

As we explained in the D1.1, consent (and the exception of explicit consent in case of sensitive data) of the research participant will be one of the most essential legal bases. A caveat regarding consent: EDPB point out that "entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent."[31] In the TeNDER context, the patients as well as the physicians will have been fully briefed about the video surveillance, and procedures to obtain informed consent have been put in place. However, in a post-project context, data controllers might need to rely on different legal grounds should obtaining consent not be realistic.

[28] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", version 2.0, adopted on January 29 2020. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

[29] Article 5, 1, (a) of the GDPR.

[30] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 68.

[31] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 46.

Another interesting option insofar TeNDER video surveillance processes sensitive data is to consider 'scientific research purposes' under Article 9(2)(j). In this regard, it is noteworthy that the GDPR provides that this "should be interpreted in a broad manner, including for example technological development and demonstration". he processing of sensitive personal data is also allowed if it is necessary to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent.[32] This legal ground will only be applicable in exceptional situations of emergency, for instance when a hospital monitors a patient for medical reasons.[33] This type of legal grounds may be relevant in a post-project setting.

Finally, not every exception of article 9, 2 will be appropriate in the context of video surveillance. For example, article 9, 2, (e), which relates to the processing of personal data that are manifestly made public by the data subject, can generally not be invoked by the controller. Merely moving into range of a camera does not mean that the data subject intends to make public his/her special categories of personal data and other legal grounds are necessary.[34]

3.2 Storing and erasing data

Personal data processed by video surveillance must always be adequate, relevant, limited, and kept in a form which permits identification of data subject for no longer than what is necessary for the purposes for which they are processed, according to the principles of data minimization and storage limitation.[35] It is possible that member states have introduced specific storage periods for video surveillance activities.[36] In practice, the appropriate storage period will depend on the purposes of processing. For example, video surveillance may serve the purpose of preserving evidence, which warrants a longer storage period than the sole purpose of detecting vandalism. Consequently, a longer storage period requires more weight to the legitimacy of the purpose and necessity of the storage measure.[37]

The EDPB points out that the longer the data are stored for (especially when that is more than 72 hours), the stronger the required argumentation for the legitimacy of processing and the necessity of storage. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. The GDPR is based upon the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with them.[38]

[32] Article 9, 1, (c) of the GDPR.
[33] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 64.
[34] Ibid.
[35] Article 5, 1, (c) and (e) of the GDPR.
[36] Article 6, 2 of the GDPR.
[37] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 70.
[38] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 121.

3.3 Transparency and information obligations

Data subjects should in general be aware of the video surveillance activities as much as possible. According to the guidelines on transparency under the GDPR, [39] it is the art. 13 that applies in video surveillance context, since the personal data is collected from the data subject.

These obligations entail that the data subject should be informed about the surveillance activities in a detailed and transparent manner. For video surveillance, a layered approach is often preferred, where information is provided through multiple channels, such as a warning sign, information sheet, website, etc.[40]

The first layer of information should be provided by placing a warning sign. This is often done in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner an overview of the intended processing activities.[41] The aim is to inform the data subject in such a way that he/she recognizes the circumstances of the surveillance activities before entering the area in question. The context of surveillance and which areas are under surveillance must be clear to the data subject. This warning sign, as a first channel of information, should provide the most important information (e.g. details on the purposes of processing, the legal basis, the identity of the controller, the rights of data subject, the contacts details of the DPO, etc.) and, if applicable, any special information (e.g. transfer to third parties, storage periods, etc.). It should also make a clear reference to the second layer of information, which provides more detailed information.[42]

The second layer of information, to which the first layer must clearly refer, should provide all the necessary information of article 13 in a detailed manner. This layer must be easily accessible and can be made available both digitally (such as on a website) or non-digitally (e.g. an information sheet, a poster, etc.). It is recommended that, in case the second layer is provided digitally, a non-digital channel should exist as well. In any case, the second layer of information should be accessible without entering the surveilled area.[43]

According to the requirement of transparency, all of this information must be communicated in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[44] It must be noted that these transparency and information obligations are often further specified under applicable national law, which should also be taken into account.

[39] Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25th 2018
[40] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 112 ff.
[41] Article 12, 7 of the GDPR.
[42] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 112 ff.
[43] Ibid.
[44] Article 12, 1 of the GDPR.

3.4 Technical and organizational measures to ensure data protection by design and security of data processing

In the context of security[45], the application and implementation of the data protection principles[46], and safeguarding the rights and freedoms of the data subject, controllers are required to implement appropriate technical and organizational measures.[47] These measures must be, implemented at the time of the determination of the means of processing and at the time of processing itself, on the basis of data protection by design and by default principle.[48] In general, organizational measures relate to enforcing the proper management frameworks, procedures, and policies (e.g. a DPIA, access policies, training program, transfer policies, incident management, etc.), while technical measures involve the inclusion of requirements in the design and specification of the system architecture (e.g. cybersecurity measures, physical protection, encryption, access rights, authentication and authorization measures, system restoration, etc.). The controller should also aim for the implementation of privacy-friendly technologies and measures, but only to the extent that they are necessary (e.g. integrated scrambling and editing software, limited movement and zoom capabilities, limited analytics).[49]

3.5 Specific provisions for using video footage in research

The principle of purpose limitation requires that data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with art. 89 is not considered incompatible with this principle.

Whether this authorises the re-use of existing video archives without obtaining new legal grounds is uncertain.

Purpose limitation means that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[50] This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[51] It consists of two building blocks:

- data is collected for specified, explicit and legitimate purposes,
- further processing of collected data must not be done in a way incompatible with those purposes (Article 5(1)b of the GDPR).

Specific purpose means that the purpose must be 'sufficiently defined to enable the implementation of any necessary data protection safeguards and to delimit the scope of the processing operation'. An explicit purpose is one that is 'sufficiently unambiguous and clearly

[45] Article 32 of the GDPR.
[46] Article 5 and 25, 1 of the GDPR.
[47] Article 24 of the GDPR.
[48] Article 25, 1 of the GDPR.
[49] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 123 ff.
[50] Article 5(1)b of the GDPR.
[51] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 4.

expressed'. The notion of legitimate purpose goes beyond the scope of privacy rules and requirement of legal grounds for data processing.[52]

Purpose specification is related to concepts such as data transparency (visibility of purpose), predictability of data processing and user control, i.e. giving data subjects certain rights regarding the collected data.[53]

In its art. 89, GDPR provides for certain derogations when processing personal data for for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This means that EU or national law may provide for derogations from the data subject rights, such as the right of access, right to rectification, restriction of processing, and the right to object to processing of personal data which is based on point (e) or (f) of Article 6(1) (i.e. task in the public interest, or legitimate interests of the controller); these derogations are permissible insofar technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Moreover, WP29 points out that it should be ensured data is then not reused to make decisions about any single individual.[54] The EDPS, following WP29's argument, further states that the principles of purpose limitation and lawfulness should be understood cumulatively: reusing data requires a new legal basis, even if done so for scientific purposes.[55]

Opinions and recommendations are of course non-binding legal texts. Nevertheless, in the absence of clear diction in the statute, they should be adhered to wherever possible as an example of a highly possible interpretation. Therefore, we advise data controllers to obtain valid legal grounds, such as consent, to use personal data in video footage for research purpose, whenever that is feasible.

[52] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 12.
[53] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 13-14.
[54] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 33.
[55] European Data Protection Supervisor, Preliminary Opinion on data protection and scientific research, January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

4 First TeNDER impact assessment

4.1 The motivation for impact assessment

In the TeNDER project, the importance is legal and ethical aspects is tightly intertwined with technical development and medical research. Hence, the consortium has promised to carry out an impact assessment, in order to assess the risks to patients' fundamental rights and freedoms that might occur during the project research activities and beyond. An impact assessment contributes to human rights protection in advance in the light of the provisions of the EU law on data protection and privacy. Often, the risks go beyond the conception of privacy, since information collection and the potential use of those data can interfere with other fundamental human rights.[56] In TeNDER, we look beyond the normative legal framework and also take into account common societal and ethical norms, thus providing a comprehensive overview of risks, their likelihood and impact, and the consortium's planned responses. The impact assessment reflects the project development before M15 (January 2021). The exercise will be carried out again before the end of the project in order to reflect future development and evaluate our approach. In this manner, the experience of TeNDER impact assessment can inform policy-makers, industrial best practices and academic researchers.

4.2 Methodology

This First TeNDER Impact Assessment Report is part of T1.3 in WP1 Data Protection, Ethical Impact and Interoperability of the TeNDER project. In the context of WP1, the aim of the impact assessment is to identify the risks related to social, ethical, legal and privacy issues and suggest the measures to mitigate them. The analysis of these risks consists of the following stages:

- Defining and describing the legal and ethical framework applicable to TeNDER's developments and activities (resulted in D1.1 – First Fundamental rights, ethical and legal implications and assessment);
- Conducting the impact assessment in TeNDER that consists of the following stages:
  - Preparing questionnaires addressed to all partners to collect the information on their activities in the project and their impact from legal, privacy and ethical perspectives (presented in Annexes I, II and III);
  - Collecting and clarifying the answers of partners;
  - Identification, analysis and description of social, legal, ethical and privacy risks, and measures to mitigate them (presented in this first impact assessment report).

Reflecting the structure of the questionnaire, the impact assessment consists of 3 sections depending on the type of the risks: data protection, privacy, and ethical and societal risks. Every section provides an overview of the risks' context, a description of the related processes and activities and adds the contribution to the fundamental rights, ethical and legal compliance framework when it is needed (based on the project's progress). Further, every section contains a table with the list of risks.[57] The assessment is structured as follows:

[56] Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment* (Springer Netherlands 2012) <https://doi.org/10.1007/978-94-007-2543-0_2> accessed 12 August 2019.
[57] A. Kiseleva, P. Quinn (VUB), FASTER, SELP Impact Assessment Report ("FASTER"), p. 7, 8.

- the risks are **named** (risk name) and **described** (risk description);
- risks are assessed according to their **probability of occurrence**: remote, possible or probable;
- risks are assessed according to their **impact on the fundamental rights**, ethical and legal compliance framework: minimal, significant or severe;
- a **risk response plan and a responsible partner** for following up on the issue at stake are proposed.

The probability of risk to occur has been rated using a three-grade scale:[58]

- **Remote** – Risk nature is known but no known occurrences of the risk happened in similar activities. Depending on the nature of the risk, the risk can be ignored, although a preventive action may still be proposed.
- **Possible** – Risks of similar nature have happened in similar activities or the situation may be conducive to the occurrence of the risk. A response plan should be suggested in case the risk manifests.
- **Probable** – There is a significantly high chance that risk will occur, or the situation is favourable to occurrence of risks. Mitigating actions should be discussed and monitored.[59]

The identified risks may have an impact with respect to social, legal, ethical and privacy issues. The scale used to rate the impact is the following:[60]

- **Minimal** – In case of occurrence, the risk does not hinder on any relevant interests, e.g., safety, or the rights and freedoms of the individual, thus no modification or adaption is needed. It is also possible that the occurrence of the risk only requires minor adaptations.
- **Significant** – In case of occurrence, interests, rights and freedoms of the individual are affected, thus hindering the goals of the project. Significant revision and re-orientation may be necessary.
- **Severe** - In case of occurrence, interests, rights and freedoms of the individual are severely affected, meaning that the project will not achieve one or more goals. The activity or the functionality may be unlawful or contrary to ethical principles. This warrants for substantial revision and re-orientation of the project.[61]

As mentioned above, the risks are classified according to different areas. The number of relevant risks identified per category is as follows:

1) Risks related to the protection of personal data (DP): 12;
2) Privacy risks (P): 3;
3) Ethical and societal risks (E): 4;
4) Risks related to the potential use of medical devices (MD): 3.

Finally, measures are suggested to mitigate the identified risks. These measures take into account legal and ethical requirements, the activities carried out by partners and the facilities they have, and the probability and impact of the risk. Importantly, the risks are assessed and

[58] A. van Scharen, E. Mantovani (VUB), PROTEIN, Impact Assessment Report, ("PROTEIN") p. 11; FASTER, p. 7, 8.
[59] *Ibid*.
[60] *Ibid*.
[61] *Ibid*.

the measures to mitigate them are suggested in relation to the project's objectives. At this phase, the project activities are focused on developing prototype solutions rather than commercialising them. This aspect is taken into consideration in the risk response plan and enables the use of more controllable solutions. However, the impact assessment is a continuous process and if the context of project's activities is changed, the necessary updates in the risk response plan will be made. Moreover, consideration is also given at the exploitation of the TeNDER system upon completion of its development. While the risks might arise in different areas and are related to different project activities, the mitigating measures have been assigned to specific partners; in most cases, it is VUB as the leader of WP1 and the partner responsible for the WP or task where the risk might occur.

4.3 Risk assessment and response

Before each table: explanation, short description (in this table, we describe what is the risk, how likely is it going to happen to us, what do we do if it does happen)

4.3.1 Risks related to the protection of personal data

The TeNDER activities involve processing of personal data with different variables. The legal framework applicable to protection of personal data in the project was described in the First Fundamental rights, ethical and legal implications and assessment (D1.1). The preliminary analysis of the reasons to conduct a DPIA in the TeNDER Project was described in the D1.1 as well as D10.9. The TeNDER project intends to utilise various technologies, including wearables, sensors and scanners, home safety devices, microphone and mobile devices, and artificial intelligence algorithms, resulting in personalised models for each patient to identify abnormalities, raising alerts for a rapid intervention in case of need, and making personalised recommendations for the patient's care plan.[62] The first two categories under Article 35(3) could apply to the TeNDER project. The use of artificial intelligence algorithms and technologies has the potential affect the rights of the data subject substantially. Furthermore, the TeNDER project will be processing sensitive data, including data concerning health. Especially noting the type of data to be collected and processed, and the type of data subjects, it was recommended that a DPIA was to be conducted in the context of the TeNDER project.

For this purpose, every partner was asked through the questionnaire (Annexes I, II and III) to provide information on their processing of personal data in the project. Additional information was received from the D2.3 'First Version of TeNDER Architecture and Blueprint, Pilots and Definition', communications with partners through requests for clarifications. The received information was accumulated and analysed by the authors of this deliverable. The results are provided below. The processing of personal data in TeNDER is described in general, followed by the identified risks and measures to reduce those risks.

Context of processing

Processing of personal data in the context of the TeNDER project is related to the preparation and carrying out of pilots. Depending on the role of the relevant partner, processing activities are divided into two main categories: development and operation of technology in the project (by technical partners) and engagement of humans in pilots (by user partners). Most of the processing activities by user partners are carried out with the use of several technologies and

[62] GA, Annex 1, Part B, pp. 4, 25.

thus are interconnected with the processing activities of technical partners. This processing takes place through the project's technical infrastructure described in the Deliverable 2.3 'First Version of TeNDER Architecture and Blueprint, Pilots and Definition'. This infrastructure consists of three main tiers:

- **Low level subsystem**;
- **High level subsystem**;
- **Related services**.

Each layer has its own specific features of data processing: types of data, scope of partners involved, and processing activities. As set out in D2.3, it is necessary to specify that all the sensitive data collected is stored and processed locally, while general information (metadata) is sent to the cloud where it is processed in the high-level secure layer subsystem which mostly implies the adoption of protocols for communication over the Internet that protects the integrity and confidentiality of data exchanged between computers and sites, such as HTTPS (Hypertext Transfer Protocol Secure) and the implementation of RabbitMQ, i.e. message-oriented middleware, also known as messaging broker implementing the Advanced Message Queuing Protocol (AMQP) for the integration of real-time data from detection devices. The visual representation of TeNDER technical infrastructure is presented below in Figure 1.

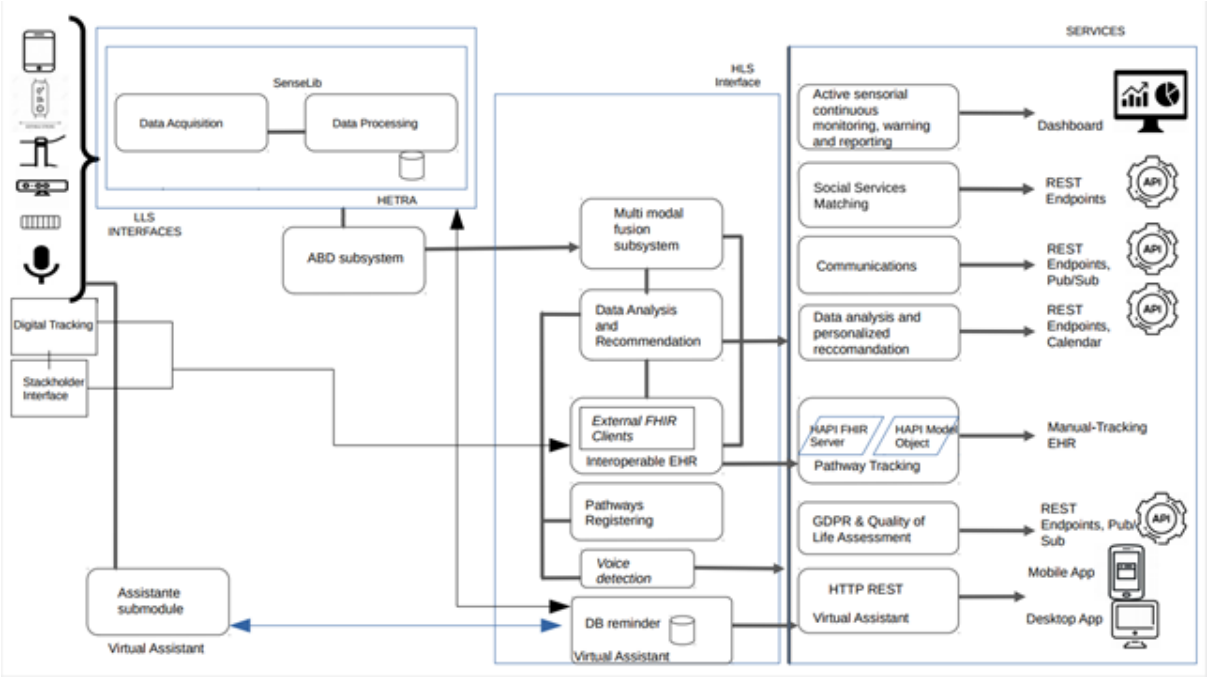

Figure 1: TeNDER Data Flow[63]

Legal grounds of data processing

The First Fundamental rights, ethical and legal implications and assessment (D1.1) provided the description of legal grounds potentially applicable to the TeNDER project, being consent, and for the processing of sensitive personal data, explicit consent or scientific research purposes. Thus, the legal ground for processing of personal data (both general and sensitive

[63] Source: TeNDER D3.2, First version of Patient interface interaction and Pathways tracking

categories) is explicit informed consent of the data subject. The consent forms will vary based on the types of data subjects and processing activities they are involved in. The informed consent forms and the information sheets about processing of personal data have been set out in D10.3.

Purposes of processing

The purpose of personal data processing in TeNDER is to enable the development, testing and use of technologies within the project and carry out the relevant demonstration activities. This is necessary to reach the main goal of the project (as set out in D2.3 and the TeNDER Grant Agreement, No. 875325): to improve the quality of life of patients and those around them, including caregivers and socio-healthcare professionals through the TeNDER tool based on different technological devices.

Groups of data subjects

There are three main groups of data subjects in TeNDER processing activities:

- Persons with AD, PD and/or CVD co-morbidity;
- those in the care pathway (including health professionals, social workers, caregivers (professional and informal) and others (administrative staff, hospital IT, day care centre workers etc.));
- representatives of project partners and stakeholders.

Types of personal data to be processed

The types of personal data to be processed vary based on the type of data subject (and processing activities he/she is involved in). Generally, these are the following data types:

- Persons with AD, PD and CVD:
  a) identifying data (incl. name, place and date of birth, address, sex, age);
  b) contact data;
  c) information regarding their living situation;
  d) data concerning their health status and treatment;
  e) data gathered from sensorial components etc.;

- Persons in the care pathway:
  a) identifying data (incl. name, place and DoB, address, ID/social system number);
  b) contact data;
  c) professional status etc.;

- Representatives of TeNDER partners and stakeholders
  a) Identifying data (e.g. name, last name, data of birth, age, gender, email, phone, role/title, organisation)
  b) Contact details of the responsible DPOs (e.g. name, last name, email, phone, organization)

Involved partners and their roles

While the TeNDER architecture is a complex and interconnected system aimed, inter alia, to collect and analyse data from different devices to be used in multiple pilots, almost all partners are involved in the processing of personal data. The processing activities depend on the role of the partner in the project: technical or user partner. The TeNDER user partners

and UPM as coordinating partner in TeNDER define the purposes and means of data processing. Therefore, they will be considered data controllers as defined by art. 4 of the GDPR. The technical partners are involved in the project's technical infrastructure and will be processing personal data on behalf of the user partners and therefore act in the role of data processors.

Necessity and proportionality

The purpose of personal data processing is to achieve the main goal of the project. Real patient data is used by the project partners since the use of synthetic or other non-personal data would not have been sufficient or adequate to develop the products, evaluate their performance or follow-up on patients' health situations. Nevertheless, pseudonymising measures are used to the highest extent possible in order to prevent a disproportionate impact on the patients' rights.

The table below presents the identified data protection risks and measures to mitigate them:

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 2: Risks related to the protection of personal data

RISKS RELATED TO THE PROTECTION OF PERSONAL DATA						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
LAWFULNESS, FAIRNESS AND TRANSPARENCY						
DP.1	Consent lacks informativeness	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.	Possible	Significant	The information provided in the information sheets (D10.3) will be changed, adapted or amended to reflect the project developments in order to ensure transparency toward patients and other users. Participants will be informed about their rights,	VUB, user partners

		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 purposes of processing, the identity of the data controller etc., as required by art. 13 of the GDPR, according to the procedures identified in WP10 (Ethics requirements).	
PURPOSE LIMITATION						
DP.2	Purpose of data processing is not clearly defined	The purpose of personal data processing is conducting the research activities in the project. However, due to the complexity of the project, the mentioned purpose is deemed to be too wide and might lack sufficient specification	Possible	Severe	The general purpose will be layered to sub-purposes and accompanied with clear description of the project and its goals (in informational sheets, on the website). This will ensure that the purpose is detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with	Partner processing the data + VUB

					the law can be assessed and data protection safeguards applied.	
DP.3	Processing of personal data outside the scope of the purpose it was collected for	The project's pilots will engage healthcare providers already actively engaged with their patients. In this case, some of their personal data is already being processed by the respective partners. Depending on the description of initial purposes of data processing, it might be incompatible with processing activities in the project	Possible	Severe	While engaging patients and providers in pilots or other project activities, the conditions of their data processing (including purpose, legal basis, processing activities) will be defined separately from the existing processing activities in their organisation. This will enable compatibility with the purpose.	Partner processing the data + VUB
DATA MINIMIZATION						
DP.4	Processing of data not necessary for the purposes	TeNDER will collect data via different means and different technologies, which will be processed by different partners. It might happen that data collected by one partner for its purposes is provided to another partner but this	Possible	Severe	For every processing activity the scope of the data necessary to achieve the purpose of processing will be defined. Additionally, the list of partners involved in that processing activity as well as their respective roles will be specified.	VUB + partners involved in data processing

		data is not needed to achieve the goals of those partners				
INTEGRITY AND CONFIDENTIALITY						
DP.5	Insufficient security of data processing, transfer and storage	TeNDER's technical architecture is complex and will include different layers and several means of collecting and processing data (several types of devices, local COPs, hardware, middleware). This all might create the security risks such as risks of data loss, breach of confidentiality)	Possible	Severe	In every scenario where the High-level services of TeNDER do not require the identification of a certain person, data can be anonymised (as well as aggregated) for analysis and evaluation. All data from/to TeNDER platform are transited over encrypted sessions (ex. HTTPS).	Technical partners
DP.6	Storage of data in the cloud	The TeNDER technical architecture will include internet cloud layer. Cloud technologies in general might pose some risks related to security of data stored there	Possible	Severe	Defining what kind of data can be stored in the cloud is necessary. In addition, the security, pseudonymisation and anonymization techniques will be used. Data access is protected by Keycloak authentication and authorisation mechanisms and only logged-in users with specific permissions can access it. Further details on data	VUB + MAG

					storage in the cloud will be decided by the TeNDER partners in the next stages of the project.	
STORAGE LIMITATION						
DP.7	Different periods of data storage	TeNDER includes different partners processing different types of personal data and with regards to different processing activities. Partners might store the personal data for different periods of time	Probable	Significant	The TeNDER partners shall agree on the minimum and maximum periods for storing personal data to ensure respect of the storage limitation principle, taking into account applicable national legislation.	VUB + all partners
ACCOUNTABILITY						
DP.8	The roles of partners are not clearly defined	Involvement of almost all partners in processing of personal data with respect to different purposes and activities creates the risk of lack of accountability (‘everyone is responsible for everything’=’no one is responsible’)	Minimal/ possible	Severe	All partners shall define their role (controller/ processor of personal data), the partners they cooperate with and how. They will specify the purposes of data processing, types of data and relevant activities, as laid out in the Deliverable D1.1 and the Data Sharing Agreements	VUB + all partners
DP.9	Access to data by unauthorized subjects	TeNDER includes different companies, organisations and	Possible	Severe	TeNDER partners have taken high-level measures to ensure access controls and other	VUB + partners whose servers have been breached

		universities. While some representatives are continuously involved in the project activities and are informed on the necessary procedures, other employees might get access to the data not being aware of the rules of its protection			organisational and technical measures to ensure data is not access by unauthorised parties. High-level measures are described in D10.6 and will be further determined in the D2.4, which is due in M19. As required by art. 30 of the GDPR, partners shall keep the record of processing activities describing the type of data processed, by whom (including the person within organization) and for which purpose. The scope and amount of people having access to the personal data shall be limited.	
RESPECT OF DATA SUBJECTS' RIGHTS						
DP.10	Limited right to erasure of personal data	If conditions of art. 17(1) GDPR are met, the patient or other data subject can request deletion of their data	Possible	Significant	Evaluate whether the personal data collected are still necessary to achieve the goal, whether consent has been revoked and if other criteria in art. 17 of the GDPR are met	VUB + user and technical partners involved in the specific data processing
DP.11	Limited data portability	It is not defined if the data processed	Probable	Low	This issue is likely to occur post-project rather	Entity exploiting TeNDER

		within TeNDER might be technically transferred to another data controller under the request of data subject			than during the project research phase. Right to portability will be evaluated in the light of upcoming EU policies (the scope and nature of the right and its relevance for TeNDER users); this evaluation will if relevant be included in the final legal assessment and recommendations report (D1.6).	
OTHER RISKS						
DP.12	Risks related to processing of personal data of caregivers	TeNDER will implement technologies aimed to monitor the health status of patients and this ensures their safety. However, it is likely that caregivers might need to disclose their own personal data, such as name, email address, workplace, etc. to use the device.	Probable	Significant	System can distinguish between the patient and other people, which will help prevent unnecessary processing of caregivers' personal information. Legal grounds for such data processing: processing is necessary in order to protect the vital interests of the data subject or of another natural person; or necessary for the purposes of the legitimate interests pursued by the controller or by a third party.	VUB + all partners

4.3.2 Privacy risks

As described in the First Fundamental rights, ethical and legal implications and assessment (D1.1), the right to privacy is a fundamental right guaranteed by international treaties (such as the Universal Declaration of Human Rights), at the level of the Council of Europe (the European Convention of Human Rights) and the European Union (the Charter of Fundamental Rights of the European Union). The right to privacy means that *everyone has the right to respect for his or her private and family life, home and communications. This right might be limited only in cases provided by law and with respect the essence of the right (subject to the principle of proportionality).* Privacy is a complex concept and might include different aspects. In addition to those described in the First Fundamental rights, ethical and legal implications and assessment (D1.1), several types of privacy are identified:[64]

- **privacy of the person** *(*encompasses the right to keep body functions and body characteristics private);
- **privacy of behaviour and action (**concerns activities that happen in public space, as well as private space and might include sensitive issues such as sexual preferences and habits, political activities and religious practices);
- **privacy of communication** (aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail message);
- **privacy of thoughts and feelings** (people have a right not to share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like);
- **privacy of location and space** (the right to move about in public or semi-public space without being identified, tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office);
- **privacy of association** (concerned with people's right to associate with whomever they wish, without being monitored).

The table below presents the identified privacy risks and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 3: Privacy Risks

PRIVACY RISKS

[64] M.Friedewald, et al. Seven Types of Privacy. In: European Data Protection: Coming of Age. Springer,2013. Editors: Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet. Also see FASTER, p. 17.

Risk ID	Name	Description	Probability of occurrence	Impact	Risk response plan	Responsible partner
P.1	Affecting privacy through the use of cameras	During some pilots, cameras (RGB/Azure) will be used in skeleton view to evaluate movement and support the patient in case they fall, or a similar emergency occurs	Probable	Significant	The camera records the skeleton only, not the individual as a whole. The recordings will not be identifiable without additional information, which is kept separately.	User partners using cameras (UNITOV, SERMAS, SKBA, SPO, APM)
P.2	Affecting privacy through the use of microphone	Microphone will be one of the sensors used to help monitor patients. Apart from the voice of the patient, a microphone could pick up the voices of other users (care-givers, family members, casual visitors etc.)	Probable	Significant	The system is capable of distinguishing between the characteristics of the patients and the other people, thus minimising the potential impact on other persons' right to privacy	User partners using microphones (UNITOV, SERMAS, SKBA, SPO)
P.3	Affecting privacy of person through individualized bio-monitoring of patients	Comprehensive monitoring of patients through the use of different sensors (Audio/microphone, Fitbit, Kinect camera, RGB	Probable	Significant	Patient monitoring will be limited in scope. Biosensor devices such as	VUB + all partners

		sensor, Localisation sensor, sleep tracker, binary sensor)			portable devices will be used to measure heart rate, body temperature, blood glucose or blood pressure, but not other aspects of the private life which fall outside the scope of the TeNDER project. Moreover, health records will not be included in the Slovenian pilot. Finally, the invasiveness of technology in the piloting is being constantly evaluated by all partners involved.	

4.3.3 Ethical and societal risks

The general framework for ethical and societal concerns arising out of TeNDER are initially described in the First Fundamental rights, ethical and legal implications and assessment (D1.1). As set out in D1.1, there are a number of different factors related to the TeNDER project that can give cause to ethical and/or societal concerns. One of these concerns relates to the participation of vulnerable groups in scientific research. Furthermore, the use of new

technologies, their acceptance by the society and trust in such technologies is something to assess and consider. Finally, the balancing of various fundamental rights and vital interests of different groups of people is another.

In TeNDER, informational awareness shall include the technologies used in the project, the corresponding risks, benefits and the way to use them. This will enable all groups to make informed decisions, which increases the safety and trust in the technologies used. The ethical and societal risks that might arise out of the project and the measures to mitigate them are described in the table below:

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).
- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 4: Ethical and Societal Risks

ETHICAL AND SOCIETAL RISKS						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
E.1	Lack of trust in the use of new technologies from the side of users	Lack of trust in new technologies if users do not understand how those technologies work, or why they are necessary/useful.	Remote	Severe	Training, explanation, user-friendly interfaces for both the patient and the care-giver	VUB + all partners, especially partners involved in front end/UX development
E.2	Lack of trust in the technologies by society	Lack of trust in new technologies is a common issue as people do not fully understand how the technologies work and what might be the side effects.	Remote	Significant	TeNDER will be designed according to safety requirements and in full respect of applicable legislation and bioethical principles Transparency toward the user on risks and benefits	Entity exploiting TeNDER

E.3	Affecting the fundamental rights of people not participating in the pilot/using the TeNDER system	When equipment is installed in the pilot sites, there is an inherent risk that the sensor, camera, depth sensors or microphone will pick up activity from others than those participating in the pilot/using the technology - one person's desire to use such assistive technology in a group setting may infringe upon another's right to privacy or the other person may object to the use of a certain device or equipment	Probable	Minimal	Some parts of the system are capable of distinguishing between the user (target person) and others. The other person is aware of the monitoring technology being used (the device is not concealed). Moreover, sensors bearing the risk of picking up activities or data from other persons will not be implemented in rooms used by other persons than the participants	VUB + all partners
E.4	Use of assistive technology for people with neurodegenerative illnesses such as PD and AD	In the case of dementia and other neurodegenerative illnesses, the people using the technology are not necessarily able to fully understand the implications and may not have the capacity to give full consent or where its use	Possible	Significant	Co-design process with users (WP2), addressing the shortcomings. Inter alia, the co-design process will adapt the technology's material features, affordances, and aesthetic	VUB + all partners

		may result in shame, stigma and embarrassment, yet its use may be beneficial, enabling them to accomplish tasks that they would otherwise be unable to manage			properties; a distributed knowledge of the individual and the places they wandered through; and a collective and dynamic interpretation of risk. After pilots are carried out, surveys will be conducted to evaluate users' (especially patients') experience.[65] Providing transparency and information to the users, which are adapted to the level of understanding appropriate to the specific patient (consent forms given in D10.3)	

4.3.4 Risks related to the use of medical devices

The table below presents the identified risks related to the use of medical devices and measures to mitigate them.

- Identifies the risks that might occur in the project scenario when personal data are processed by the TeNDER consortium (**name and description**).

[65] TeNDER D2.3 and D2.4 (*currently in progress*) describe procedures on involvement of stakeholders, especially patients and caregiver organizations.

- How likely they are to occur (**probability of occurrence**) and what would be their **impact** on patients' rights.
- How the consortium commits to avoid the risk from occurring (**risk response plan**), or to answer the risk if it occurs, and which partners will be **responsible** for the risk mitigation action.

Table 5: Risks related to the use of medical devices

RISKS RELATED TO THE USE OF MEDICAL DEVICES						
Risk ID	**Name**	**Description**	**Probability of occurrence**	**Impact**	**Risk response plan**	**Responsible partner**
MD.1	Non-compliance with Medical Devices Regulation (MDR)[66]	A medical device is any device (or instrument, software, implant or any article) intended to be used for medical purposes. If a device falls under this definition, it must meet the occupational health & safety requirements as mandated by the regulation, before it can be put on the European Union market.	Possible	Severe	The partners will monitor the applicability of the Medical Devices Regulation, keeping in mind the main purpose of the TeNDER technology being developed. The main goal of the technology developed is to assist the people in their decision-making; it serves to warn and monitor, and not treat illnesses or disabilities, which does not seem to fall under the MDR's scope of application. As part of the co-design process and pilot evaluation, the partners will should take into account the notion of 'manufacturer', the definition of a	VUB + all partners involved in pilots

[66] Regulation 2017/745 of 5 April 2017 on medical devices.

					'medical device', and the purpose they want to attribute to the OSHW project.[67]	
MD.2	Use of unsafe medical devices	The device or technology used in the project poses a safety risk to the user (patient or care giver).	Minimal	Significant	All sensors used in TeNDER have a CE mark. Devices have been used extensively and the user experience has been largely positive.	Technical partners
MD.3	Information conveyed by the device does not assist in health monitoring, warning or evaluation	A malfunction of the device due to low battery, poor connection or similar technical problem, resulting in broken data flow (no reminders, notifications, alerts…)	Possible	Significant	The partners involved will carry out a technical examination of the malfunction and correct it (e.g. replace battery, adapt settings, connect device to the network…) Check whether the device is being used properly (e.g. whether the patient takes it outside with them)	Technical and user partners (depending on the source of malfunction)

4.4 Summary of findings and recommendations

In the impact assessment, we analysed the risks to fundamental rights of patients and addressed wider societal concerns, relevant to TeNDER pilots and product development. We went beyond the requirements of art. 36 of GDPR in order to present a comprehensive picture of how fundamental rights are likely to be affected by our work, and how to respond appropriately.

[67] Elisabetta Biasin and Erik Kamenjašević, 'Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges' (2020) 4 Journal of Open Hardware 7.

Based on the current outcomes of the TeNDER IA, the consortium should consider the treatment of the identified risks and carry out the advised activities, with special attention to the applied mitigating measures and to the following:

- The consortium should continue to provide relevant information to pilot participants and adjust the information digitally or verbally to keep informing the patients about their data subject rights, the purposes of data processing, that they have the right to withdraw from the project research, and any other relevant consideration.
- Technical and user partners should continue to ensure that the TeNDER system's operational configurations prevent unnecessary personal data processing.
- Technical and user partners should, in cooperation with VUB, continue to consider legal and ethical requirements throughout the whole project, and the activities should be regularly overviewed.
- After the end of the project, documentation on any personal data processing operations should be made easily accessible and/or centralized.
- Further impact assessments should follow up on preparation and execution of the second and third waves of pilots, and should likewise be made public to inform similar projects and assist their compliance efforts.

Future impact assessment will report on the implementation of these guidelines.

5 CONCLUSIONS

In this deliverable, we reviewed the legal and ethical work that has been carried out in TeNDER, with a focus on the use of wearables, extracting information from video archives, and provided the first impact assessment.

The main recommendation of the first impact assessment, contained in section 4.4 will be implemented in further development and piloting efforts, and final legal evaluation will follow in D1.6, due M36. There are two more impact assessments planned to correspond with the second and the third wave of pilots; the impact assessments will be released together with the D1.5, Second version Legal/Ethical Monitoring and Review (due M36).

REFERENCES

Literature

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

E. Biasin and E. Kamenjašević, 'Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges' (2020) 4 Journal of Open Hardware 7.

European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", version 2.0, adopted on January 29 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

European Data Protection Supervisor, Preliminary Opinion on data protection and scientific research, January 2020, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

M. Friedewald, et al. Seven Types of Privacy. In: European Data Protection: Coming of Age. Editors: Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet. (2013)

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

P. De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in D. Wright and P. De Hert (eds), Privacy Impact Assessment (2012) https://doi.org/10.1007/978-94-007-2543-0_2

Reports

D. Sarma, P. Quinn (VUB) ALADDIN D3.3, Framework for Impact Assessment Against SoEL Requirements

A. Kiseleva, P. Quinn (VUB), FASTER, SELP Impact Assessment Report

A. van Scharen, E. Mantovani (VUB), PROTEIN, Impact Assessment Report

Other TeNDER deliverables

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

TeNDER D2.3 First version of TeNDER Architecture Blueprint, Pilots definition

TeNDER D2.4 Intermediate version of User Requirements and Data Model

TeNDER D3.2 First version of Patient interface interaction and Pathways tracking

TeNDER D6.2 Report on first wave of pilots

Legal sources

Directive 2011/24/EC of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare

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)

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

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

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

Annex I – Questionnaire Coordinating Technical Partners

Dear TeNDER partner,

The present questionnaire is the part of the continuous legal and ethical monitoring and review for TeNDER project (WP1, T1.3).

The key legal and ethical issues that might arise out of the project are preliminary described in the Deliverable 1.1 - Fundamental Rights, Ethical and Legal Implications and Assessment (First Version). This questionnaire aims to collect information from the partners and, on that basis, to tailor the framework set out in D1.1 with regard to the legal and ethical risks the project poses to the individuals and society.

The answers to this impact assessment questionnaire are necessary for us to anticipate the risks and adopt a mitigation strategy for the further development of the technology in the project and running pilots. This first questionnaire aims to get a clear overview of the overall intended functioning of the TeNDER system and project as a whole. As the project proceeds, the impact assessment will be repeated on a regular basis and the assessment will evolve towards progress of the project.

This process will ensure that the TeNDER system, and any new aspects thereof, will be tested against the relevant legal, ethical and societal concerns, through the implementation of the impact assessment outcomes by all partners, that it will be compliant with relevant laws.

Instructions for completion

Please read the below instructions carefully prior to completing the questionnaire.

- Please note the questionnaire aims to addresses two scenarios: (i) TeNDER the project and (ii) TeNDER as exploitable product. Answers to some of the questions might differ based on which scenario is being considered. Accordingly, each question will indicate whether an answer for one or both scenarios is requested. Should the answer to a question be the same in both scenarios, please indicate so clearly.

- Where a question is accompanied by instructions, please read them carefully. The instruction will provide you with guidance on what information is sought, explain certain terms or refer you to where further guidance can be found. Should a question remain unclear, please reach out to Lisa Feirabend (lisa.feirabend@vub.be) for assistance.

- Please answer each question in as much detail as possible and try to answer each question in laymen's terms. This will avoid the VUB having to reach out to seek clarifications. In the event a certain question cannot be answered, because an aspect is still under development, please indicate this clearly and provide, where possible, a brief description of the intended approach or options that are being considered.

- Please answer the questions in connection to the specific component(s) that you are developing, contributing to, using or testing, or, where possible and appropriate, in relation to the TeNDER system as a whole. If you are answering in connection to the TeNDER system as a whole or multiple components, please indicate this clearly and, where possible, separate your answer per component.

- Please fill out the questionnaire as soon as possible, but no later than Monday, 23 November 2020.

1. Questionnaire for Coordinating Tech Partners

1.1 Questions related to your role in the project

1. Will your organisation develop any technology (or component) for the project or contribute thereto?
If yes, please name and describe it.

TeNDER the project:
[answer]

2. Will your organisation use any technology for the project?
If yes, please name and describe it and the purpose of its use. Also specify the source of the technology.

TeNDER the project:
[answer]

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium? If so, what types of data?
Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4.

TeNDER the project:
[answer]

1.2 Questions related to the protection of personal data.

4. What types of data will be collected and processed by the TeNDER system?
Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
b. Personal features
c. Financial data
j. Hobbies and interests
k. Consumption patterns
l. Residence or home address
m. Education

d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
n. Occupation and employment
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

TeNDER as exploitable product:
[answer]

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

6. What is the legal basis for processing of personal data? What is the purpose of processing the data and what are the expected benefits?
For more details on legal grounds for processing, please see D1.1 (section 4.3.3.3). When identifying the purpose of processing the data please indicate both the overall purpose of the collection of data and, where possible, the specific purpose separated with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected for the purpose of xx TeNDER service).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

7. If the data is collected on the legal basis of consent of the data subject, how do you guarantee that the consent is informed, specific and freely given?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

8. Is the processing of personal data really necessary to achieve the purpose identified above? Why would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome?

This question is asked to make sure that there is compliance with the data minimisation principle.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

9. Who has responsibility for control of the processed personal data and who decides how it can be used?

I.e. who are the data controlling partners in the TeNDER project, and who/what entity is the data controller in connection to TeNDER system as an exploitable product. For more details on the role and responsibility of a data controller, please see D1.1 (section 4.3.3.5).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

10. Will a data processor be used? If yes, explain who and why.

I.e. who are the data processing partners in the TeNDER project, and who/what entity is the data processing in connection to TeNDER system as an exploitable product, if any. For more details on the role and responsibility of a data processor, please see D1.1 (section 4.3.3.6).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

11. What are the sources of personal data and how will they be received?

Please specify the sources (from data subjects, other partners/sources) and means of receiving (sensors/ video recordings/ software/ questionnaires/ other means) with regards to all categories of personal data expected to be received.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

12. Describe the flow of personal data (i.e. the route from the data from recording until deletion) and how the data will be used.

Please describe briefly the datasets of personal data, the information flows (i.e. what data is collected, where did it come from, where does it go) and the use of each category of personal data.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

13. How and where will personal data be stored?
Please describe the location (e.g. office servers, cloud, third parties).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

14. Will an online tool or other cloud computing solution (connected to the internet) be used to process personal data?
If so, which one? Do you know the geographical location of such tool or cloud?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

15. How long will personal data be retained? What will happen with the personal data afterwards in terms of erasure, anonymisation or otherwise?
Next to the data protection principle of storage limitation relevant to both scenarios, please also consider the requirements of good clinical practice in maintaining a trial file in connection to TeNDER as a project.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

16. What is the scale of the processing?
Please give the approximate number of research participants engaged and/or personal data/datasets you hope to collect or need to use?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

17. What measures will be taken to ensure the security of personal data?
This includes measures for secure storage, transfer and access to the personal data as well as precautions against cyberattacks and unauthorised access.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

18. As part of the security measures, will anonymisation or pseudonymisation techniques be used, and if so, how?
If so, please describe them in as much detail as possible. For further details on the difference between anonymisation and pseudonymisation, please see D1.1 (sections 4.3.3.1, 4.3.3.5) and D10.7.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

19. As part of the security measures, how are the processing operations documented? How are records maintained? What are the rules of access to this documentation?
Such documentation will help in identifying risks both for the controller and supervisory authority. For more details on this obligation for data controllers, please see D1.1 (section 4.3.3.5).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

20. Will the TeNDER system technology be able to profile data subjects and/or take decisions based solely on automated processing of personal data from the data subject? If so, what kind of decisions?
For more details on the issue of profiling and automated decision-making(including through the use of algorithms), please see D1.1 (sections 4.3.3.1, 4.3.3.8).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

21. How will data subjects be informed about the processing activity of personal data and how will they be informed about their rights?
Please specify any technical measures (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide information to the data subjects) that will be put in place?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.3 Questions related to privacy

22. In what way could the technology impact on the privacy of individuals?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

23. Is the impact on the privacy of individuals adequate and necessary to achieve the purpose of the TeNDER system? Or are there less invasive solutions which can be used to achieve the same purpose effectively?
This relates to the necessity of the use of certain technologies.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

24. What measures are implemented to ensure a balance is struck between the potential intrusion of privacy resulting from the technology and the intended benefits from the technology?
Such potential intrusion could be limited by, for instance, the type of equipment used, the duration of such use and limiting where such equipment is used and who has access to the footage captured by the sensor or other technology used. For further details, see D1.1 (section 3.2.2).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

25. In relation to limiting the potential intrusion of privacy, will the access to personal data be restricted? What are the rules of access?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

26. In relation to limiting potential intrusion of privacy, can the features of the technology be programmed on a case-by-case basis?
This relates to the proportionality in the use of technologies, i.e. the level of intervention should be restricted to what is really needed for a particular person in a particular situation.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

27. Is unused data deleted automatically? If so, when and how often does this occur?
Regular deletion of data reduces the privacy risks as a result of malevolent action of others (e.g. that someone would be able to access and steal data).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

28. Is there a risk that the technology (either the system itself or technologies used for data gathering) will pick up activity from others than those testing or using the TeNDER system? If so, how is this addressed?

When equipment is installed, there is an inherent risk that the sensor, depth sensors or microphone will pick up activity from others, such as family members living in the home or other patients, staff or visitors in the hospital. Although the general notion of picking up of activity from others by these technologies does not necessarily mean the processing of their personal data, it holds the possibility of affecting fundamental rights of others in some cases. For further information, please see D1.1 (section 3.3).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.4 Questions related to ethical and societal concerns

29. What do you think will be the claimed benefit for the user of the technology and society?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

30. Are there any safety risks for the users related to the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

31. What kind of skills, training and information will be needed for the end-users of this technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

32. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

TeNDER the project:	TeNDER as exploitable product:

[answer]	[answer

33. What other measures could be taken to increase trust of society and individuals in the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.5 Questions related to the technologies being developed and used

34. Will technology be <u>developed</u> that monitors the health status of end-users?
If yes, please name and describe the technology.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

35. Will technology be <u>used</u> to monitor the health status of end-users?
If yes, please name, describe the technology and specify the source.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

36. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

37. Does the technology send data to health care providers to monitor an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

38. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

39. Has the technology that is being developed or used received a CE marking?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

Annex II – Questionnaire Technical Partners

Dear TeNDER partner,

The present questionnaire is the part of the continuous legal and ethical monitoring and review for TeNDER project (WP1, T1.3).

The key legal and ethical issues that might arise out of the project are preliminary described in the Deliverable 1.1 - Fundamental Rights, Ethical and Legal Implications and Assessment (First Version). This questionnaire aims to collect information from the partners and, on that basis, to tailor the framework set out in D1.1 with regard to the legal and ethical risks the project poses to the individuals and society.

The answers to this impact assessment questionnaire are necessary for us to anticipate the risks and adopt a mitigation strategy for the further development of the technology in the project and running pilots. This first questionnaire aims to get a clear overview of the overall intended functioning of the TeNDER system and project as a whole. As the project proceeds, the impact assessment will be repeated on a regular basis and the assessment will evolve towards progress of the project.

This process will ensure that the TeNDER system, and any new aspects thereof, will be tested against the relevant legal, ethical and societal concerns, through the implementation of the impact assessment outcomes by all partners, that it will be compliant with relevant laws.

Instructions for completion

Please read the below instructions carefully prior to completing the questionnaire.

- Please note the questionnaire aims to addresses two scenarios: (i) TeNDER the project and (ii) TeNDER as exploitable product. Answers to some of the questions might differ based on which scenario is being considered. Accordingly, each question will indicate whether an answer for one or both scenarios is requested. Should the answer to a question be the same in both scenarios, please indicate so clearly.

- Where a question is accompanied by instructions, please read them carefully. The instruction will provide you with guidance on what information is sought, explain certain terms or refer you to where further guidance can be found. Should a question remain unclear, please reach out to Lisa Feirabend (lisa.feirabend@vub.be) for assistance.

- Please answer each question in as much detail as possible and try to answer each question in laymen's terms. This will avoid the VUB having to reach out to seek clarifications. In the event a certain question cannot be answered, because an aspect is still under development, please indicate this clearly and provide, where possible, a brief description of the intended approach or options that are being considered.

- Please answer the questions in connection to the specific component(s) that you are developing, contributing to, using or testing, or, where possible and appropriate, in relation to the TeNDER system as a whole. If you are answering in connection to the TeNDER system as a whole or multiple components, please indicate this clearly and, where possible, separate your answer per component.

- Please fill out the questionnaire as soon as possible, but no later than Monday, 23 November 2020.

1. Questionnaire for Tech Partners

1.1 Questions related to your role in the project

1. Will your organisation develop any technology (or component) for the project or contribute thereto?
   ***If yes**, please name and describe it.*

TeNDER the project:
[answer]

2. Will your organisation use any technology for the project?
   This could include technologies such as sensors or wearables. If yes, please name and describe it and the purpose of its use. Also specify the source of the technology.

TeNDER the project:
[answer]

3. Will your organisation process or intend to process personal data on behalf of the data controlling partners in the TeNDER consortium? If so, what types of data?
   Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. This includes the processing of pseudonymised data. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 4. Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor).

TeNDER the project:
[answer]

1.2 Questions related to the protection of personal data.

4. What types of data will be collected and processed by the component(s) of the TeNDER system that you are developing or contributing to?
   Where possible, please separate this with respect to the relevant technologies/components and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

   a. Identification data (e.g. name, last name, data of
   j. Hobbies and interests
   k. Consumption patterns

birth, age, gender, email, phone)
b. Personal features
c. Financial data
d. Physical, physiological or behavioural characteristics of a natural person, allowing or confirming their unique identification (please specify)
e. Genetic data
f. Biometric data
g. Other information regarding health, incl. mental health
h. Habits
i. Family composition
l. Residence or home address
m. Education
n. Occupation and employment
o. Social security number
p. Racial or ethnic background
q. Philosophical or spiritual orientation
r. Information on sexual preferences
s. Political orientation or opinion
t. Membership of trade union or affiliation
u. Other memberships
v. Video footage
w. Other, namely:

TeNDER as exploitable product:
[answer]

5. Whose personal data is being processed?
Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

6. What is the legal basis for processing of personal data? What is the purpose of processing the data and what are the expected benefits?
For more details on legal grounds for processing, please see D1.1 (section 4.3.3.3). When identifying the purpose of processing the data please indicate both the overall purpose of the collection of data and, where possible, the specific purpose separated with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected for the purpose of xx TeNDER service).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

7. If the data is collected on the legal basis of consent of the data subject, how do you guarantee that the consent is informed, specific and freely given?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

8. Is the processing of personal data really necessary to achieve the purpose identified above? Why would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome?
   This question is asked to make sure that there is compliance with the data minimisation principle.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

9. What are the sources of personal data and how will they be received?
   Please specify the sources (from data subjects, other partners/sources) and means of receiving (sensors/ video recordings/ software/ questionnaires/ other means) with regards to all categories of personal data expected to be received.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

10. Describe the flow of personal data (i.e. the route from the data from recording until deletion) and how the data will be used.
    Please describe briefly the datasets of personal data, the information flows (i.e. what data is collected, where did it come from, where does it go) and the use of each category of personal data.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

11. How and where will personal data be stored?
    Please describe the location (e.g. office servers, cloud, third parties).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

12. Will an online tool or other cloud computing solution (connected to the internet) be used to process personal data?
    If so, which one? Do you know the geographical location of such tool or cloud?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

13. How long will personal data be retained? What will happen with the personal data afterwards in terms of erasure, anonymisation or otherwise?
Next to the data protection principle of storage limitation relevant to both scenarios, please also consider the requirements of good clinical practice in maintaining a trial file in connection to TeNDER as a project.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

14. What is the scale of the processing?
Please give the approximate number of personal data/datasets you hope to collect or need to use?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

15. What measures will be taken to ensure the security of personal data?
This includes measures for secure storage, transfer and access to the personal data as well as precautions against cyberattacks and unauthorised access.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

16. As part of the security measures, will anonymisation or pseudonymisation techniques be used, and if so, how?
If so, please describe them in as much detail as possible. For further details on the difference between anonymisation and pseudonymisation, please see D1.1 (sections 4.3.3.1, 4.3.3.5) and D10.7.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

17. As part of the security measures, how are the processing operations documented? How are records maintained? What are the rules of access to this documentation?
Such documentation will help in identifying risks both for the controller and supervisory authority. For more details on this obligation for data controllers, please see D1.1 (section 4.3.3.5).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

18. Will the TeNDER system technology be able to profile data subjects and/or take decisions based solely on automated processing of personal data from the data subject? If so, what kind of decisions?
For more details on the issue of profiling and automated decision-making(including through the use of algorithms), please see D1.1 (sections 4.3.3.1, 4.3.3.8).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

19. How will data subjects be informed about the processing activity of personal data and how will they be informed about their rights?
Please specify any technical measures (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide information to the data subjects) that will be put in place?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.3 Questions related to privacy

20. In what way could the technology impact on the privacy of individuals?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

21. Is the impact on the privacy of individuals adequate and necessary to achieve the purpose of the TeNDER system? Or are there less invasive solutions which can be used to achieve the same purpose effectively?
This relates to the necessity of the use of certain technologies.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

22. What measures are implemented to ensure a balance is struck between the potential intrusion of privacy resulting from the technology and the intended benefits from the technology?
Such potential intrusion could be limited by, for instance, the type of equipment used, the duration of such use and limiting where such equipment is used and who has access to the footage captured by the sensor or other technology used. For further details, see D1.1 (section 3.2.2).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

23. In relation to limiting the potential intrusion of privacy, will the access to personal data be restricted? What are the rules of access?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

24. In relation to limiting potential intrusion of privacy, can the features of the technology be programmed on a case-by-case basis?
This relates to the proportionality in the use of technologies, i.e. the level of intervention should be restricted to what is really needed for a particular person in a particular situation.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

25. Is unused data deleted automatically? If so, when and how often does this occur?
Regular deletion of data reduces the privacy risks as a result of malevolent action of others (e.g. that someone would be able to access and steal data).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

26. Is there a risk that the technology (either the system itself or technologies used for data gathering) will pick up activity from others than those testing or using the TeNDER system? If so, how is this addressed?
When equipment is installed, there is an inherent risk that the sensor, depth sensors or microphone will pick up activity from others, such as family members living in the home or other patients, staff or visitors in the hospital. Although the general notion of picking up of activity from others by these technologies does not necessarily mean the processing of their personal data, it holds the possibility of affecting fundamental rights of others in some cases. For further information, please see D1.1 (section 3.3).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.4 Questions related to ethical and societal concerns

27. What do you think will be the claimed benefit for the user of the technology and society?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

28. Are there any safety risks for the users related to the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

29. What kind of skills, training and information will be needed for the end-users of this technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

30. What technical measures might be implemented to assist end-users in a better and faster understanding the technology? What measures can be taken to ensure the right and efficient use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

31. What other measures could be taken to increase trust of society and individuals in the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

Annex III – Questionnaire User Partners

Dear TeNDER partner,

The present questionnaire is the part of the continuous legal and ethical monitoring and review for TeNDER project (WP1, T1.3).

The key legal and ethical issues that might arise out of the project are preliminary described in the Deliverable 1.1 - Fundamental Rights, Ethical and Legal Implications and Assessment (First Version). This questionnaire aims to collect information from the partners and, on that basis, to tailor the framework set out in D1.1 with regard to the legal and ethical risks the project poses to the individuals and society.

The answers to this impact assessment questionnaire are necessary for us to anticipate the risks and adopt a mitigation strategy for the further development of the technology in the project and running pilots. This first questionnaire aims to get a clear overview of the overall intended functioning of the TeNDER system and project as a whole. As the project proceeds, the impact assessment will be repeated on a regular basis and the assessment will evolve towards progress of the project.

This process will ensure that the TeNDER system, and any new aspects thereof, will be tested against the relevant legal, ethical and societal concerns, through the implementation of the impact assessment outcomes by all partners, that it will be compliant with relevant laws.

Instructions for completion

Please read the below instructions carefully prior to completing the questionnaire.

- Please note the questionnaire aims to addresses two scenarios: (i) TeNDER the project and (ii) TeNDER as exploitable product. Answers to some of the questions might differ based on which scenario is being considered. Accordingly, each question will indicate whether an answer for one or both scenarios is requested. Should the answer to a question be the same in both scenarios, please indicate so clearly.

- Where a question is accompanied by instructions, please read them carefully. The instruction will provide you with guidance on what information is sought, explain certain terms or refer you to where further guidance can be found. Should a question remain unclear, please reach out to Lisa Feirabend (lisa.feirabend@vub.be) for assistance.

- Please answer each question in as much detail as possible and try to answer each question in laymen's terms. This will avoid the VUB having to reach out to seek clarifications. In the event a certain question cannot be answered, because an aspect is still under development, please indicate this clearly and provide, where possible, a brief description of the intended approach or options that are being considered.

- Please answer the questions in connection to the specific component(s) that you are contributing to, using or testing, or, where possible and appropriate, in relation to the TeNDER system as a whole. If you are answering in connection to the TeNDER system as a whole or multiple components, please indicate this clearly and, where possible, separate your answer per component.

- Please fill out the questionnaire as soon as possible, but no later than Monday, 23 November 2020.

1. Questionnaire for User Partners

1.1 Questions related to your role in the project

1. Will your organisation engage human participants for the TeNDER pilots? If so, how many and for how long?

TeNDER the project:
[answer]

2. Has your organisation obtained ethical approval from the relevant ethical committee for conducting the TeNDER pilots?

TeNDER the project:
[answer]

3. Will your organisation use TeNDER technologies when you engage human participants during the pilots?
   If yes, please name the technologies (the relevant components of the TeNDER system).

TeNDER the project:
[answer]

4. Will your organisation use other technologies when you engage human participants during the pilots?
   This could include technologies such as sensors or wearables. If yes, please name, describe the technologies (the relevant sensors, devices and other technologies), their source (localisation, supplier) and the purpose of their use.

TeNDER the project:
[answer]

5. Will your organisation process personal data during the TeNDER project? If so, what types of data?
   Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, erasure or destruction. For more details on the terms 'personal data' and 'processing', please see D1.1 (section 4.3.3.1). For examples of categories of data please see question 8. Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx data will be collected with questionnaires).

TeNDER the project:

[answer]

6. Will you cooperate with other partners or external entities for processing of the personal data during the TeNDER project? For what purpose will this cooperation take place?
   For instance, consider the partners in the TeNDER project that will assist in the processing of personal data.

TeNDER the project:
[answer]

7. Do you follow or comply with any code of conduct, safety or other guidelines for the processing of personal data and/or the carrying out of activities in the project.
   Please identify the document and add a brief description.

TeNDER the project:
[answer]

1.2 Questions related to the protection of personal data.

8. What types of data will be collected and processed by the TeNDER system?
   Where possible, please separate this with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected with xx sensor, xx component will process xx data). The categories below are provided as an example.

   a. Identification data (e.g. name, last name, data of birth, age, gender, email, phone)
   b. Personal features
   c. Financial data
   d. Physical, physiological or behavioural characteristics of a person, allowing or confirming their unique identification (please specify)
   e. Genetic data
   f. Biometric data
   g. Other information re. health, incl. mental health
   h. Habits
   i. Family composition
   j. Hobbies and interests
   k. Residence or home address
   l. Education
   m. Occupation and employment
   n. Social security number
   o. Racial or ethnic background
   p. Philosophical or spiritual orientation
   q. Membership of trade union or affiliation
   r. Other memberships
   s. Video footage
   t. Other (explain)

TeNDER as exploitable product:
[answer]

9. Whose personal data is being processed?
   Please describe the data subjects, i.e. the (groups of) individuals whose personal data will be collected and processed.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

10. What is the legal basis for processing of personal data? What is the purpose of processing the data and what are the expected benefits?
    For more details on legal grounds for processing, please see D1.1 (section 4.3.3.3). When identifying the purpose of processing the data please indicate both the overall purpose of the collection of data and, where possible, the specific purpose separated with respect to the relevant technologies and other data collecting methods (e.g. xx data is collected for the purpose of xx TeNDER service).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

11. If the data is collected on the legal basis of consent of the data subject, how do you guarantee that the consent is informed, specific and freely given?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

12. Is the processing of personal data really necessary to achieve the purpose identified above? Why would other means (mock data, anonymous data set, fewer variables of personal data) be less satisfactory to achieve the same outcome?
    This question is asked to make sure that there is compliance with the data minimisation principle.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

13. Who has responsibility for control of the processed personal data and who decides how it can be used?
    I.e. who are the data controlling partners in the TeNDER project, and who/what entity is the data controller in connection to TeNDER system as an exploitable product. For more details on the role and responsibility of a data controller, please see D1.1 (section 4.3.3.5).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

14. Will a data processor be used? If yes, explain who and why.

I.e. who are the data processing partners in the TeNDER project, and who/what entity is the data processing in connection to TeNDER system as an exploitable product, if any. For more details on the role and responsibility of a data processor, please see D1.1 (section 4.3.3.6).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

15. What are the sources of personal data and how will they be received?
Please specify the sources (from data subjects, other partners/sources) and means of receiving (sensors/ video recordings/ software/ questionnaires/ other means) with regards to all categories of personal data expected to be received.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

16. Describe the flow of personal data (i.e. the route from the data from recording until deletion) and how it will be used.
Please describe briefly the datasets of personal data, the information flows (i.e. what data is collected, where did it come from, where does it go) and the use of all categories of personal data.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

17. How and where will personal data be stored?
Please describe the location (e.g. office servers, cloud, third parties).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

18. Will an online tool or other cloud computing solution (connected to the internet) be used to process personal data?
If so, which one? Do you know the geographical location of such tool or cloud?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

19. How long will personal data be retained? What will happen with the personal data afterwards in terms of erasure, anonymisation or otherwise?

Next to the data protection principle of storage limitation relevant to both scenarios, please also consider the requirements of good clinical practice in maintaining a trial file in connection to TeNDER as a project.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

20. What is the scale of the processing?
Please give the approximate number of research participants engaged and/or personal data/datasets you hope to collect or need to use?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

21. What measures will be taken to ensure the security of personal data?
This includes measures for secure storage, transfer and access to the personal data as well as precautions against cyberattacks and unauthorised access.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

22. As part of the security measures, will anonymisation or pseudonymisation techniques be used, and if so, how?
If so, please describe them in as much detail as possible. For further details on the difference between anonymisation and pseudonymisation, please see D1.1 (sections 4.3.3.1, 4.3.3.5) and D10.7.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

23. As part of the security measures, how are the processing operations documented? How are records maintained? What are the rules of access to this documentation?
Such documentation will help in identifying risks for the controller and supervisory authority. For more details on this obligation for data controllers, please see D1.1 (section 4.3.3.5).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

24. Will the TeNDER system technology be able to profile data subjects and/or take decisions based solely on automated processing of personal data from the data subject? If so, what kind of decisions?
For more details on the issue of profiling and automated decision-making (including through the use of algorithms), please see D1.1 (sections 4.3.3.1, 4.3.3.8).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

25. How will data subjects be informed about the processing activity of personal data and how will they be informed about their rights?
Please specify any technical measures (e.g. specific email address for requests, software or in-built secure system allowing data subjects to access their own personal data in a transparent way) and organisational measures (e.g. who will provide information to the data subjects) that will be put in place?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.3 Questions related to privacy

26. In what way could the technology impact on the privacy of individuals?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

27. Is the impact on the privacy of individuals adequate and necessary to achieve the purpose of the TeNDER system? Or are there less invasive solutions which can be used to achieve the same purpose effectively?
This relates to the necessity of the use of certain technologies.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

28. What measures are implemented to ensure a balance is struck between the potential intrusion of privacy resulting from the technology and the intended benefits from the technology?
Such potential intrusion could be limited by, for instance, the type of equipment used, the duration of such use and limiting where such equipment is used and who has access to the footage captured by the sensor or other technology used. For further details, see D1.1 (section 3.2.2).

TeNDER the project:	TeNDER as exploitable product:

[answer]	[answer

29. In relation to limiting the potential intrusion of privacy, will the access to personal data be restricted? What are the rules of access?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

30. In relation to limiting potential intrusion of privacy, can the features of the technology be programmed on a case-by-case basis?
This relates to the proportionality in the use of technologies, i.e. the level of intervention should be restricted to what is really needed for a particular person in a particular situation.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

31. Is unused data deleted automatically? If so, when and how often does this occur?
Regular deletion of data reduces the privacy risks as a result of malevolent action of others (e.g. that someone would be able to access and steal data).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

32. Is there a risk that the technology (either the system itself or technologies used for data gathering) will pick up activity from others than those testing or using the TeNDER system? If so, how is this addressed?
When equipment is installed, there is an inherent risk that the sensor, depth sensors or microphone will pick up activity from others participants/users, such as family members living in the home or other patients, staff or visitors in the hospital. Although the general notion of picking up of activity from others by these technologies does not necessarily mean the processing of their personal data, it holds the possibility of affecting fundamental rights of others in some cases. For further information, please see D1.1 (section 3.3).

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.4 Questions related to ethical and societal concerns

33. What do you think will be the claimed benefit for the user of the technology and society?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

34. Are there any safety risks for the users related to the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

35. What kind of skills, training and information will be needed for the end-users of this technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

36. What measures could be taken to increase trust of society and individuals in the use of the technology?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

1.5 Questions related to the technologies being developed and used

37. Will technology be developed that monitors the health status of end-users?
If yes, please name and describe the technology.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

38. Will technology be used to monitor the health status of end-users?
If yes, please name, describe the technology and specify the source.

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

39. Does the technology help prevent, diagnose or provide a prognosis of an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

40. Does the technology send data to health care providers to monitor an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

41. Does the technology suggest some type of treatment or provide some type of alleviation for an illness, injury or disability?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer

42. Has the technology that is being developed or used received a CE marking?

TeNDER the project:	TeNDER as exploitable product:
[answer]	[answer