Innovative policies for improving citizens' health and wellbeing addressing indoor and outdoor lighting

Deliverable D5.3
Guidelines for the collection and the use of data

Contractual delivery date:
M12: 28.02.2022

Actual delivery date:
M12: 28.02.2022

1st Update: 16.01.2023

Lead beneficiary:
PB11-UU

The ENLIGHTENme project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 945238.

Grant agreement no.	H2020 - 945238
Project full title	ENLIGHTENme - Innovative policies for improving citizens' health and wellbeing addressing indoor and outdoor lighting

Deliverable number	D5.3
Deliverable title	**H - Requirement No. 1**
Type / Nature	☒ R - Document, report (excluding the periodic and final reports) ☐ DEM - *Demonstrator, pilot, prototype, plan designs* ☐ DEC - *Websites, patents filing, press & media actions, videos, etc.* ☐ ETHICS ☐ OTHER - *Software, technical diagram, etc.*
Dissemination level	☒ Public (PU) ☐ Confidential, only for members of the consortium and the Commission Services (CO)
Work package number	5
Work package leader	UU
Primary Author(s) *(in alphabetical order)* **& ORCID if available**	Deborah Mascalzoni, UU
Other authors *(in alphabetical order)* **& ORCID if available**	
Reviewers *(in alphabetical order)*	Elisa Conticelli (UNIBO) Patricia Alveen (EURICE)
Language	English
Keywords	

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 945238.
The author is solely responsible for its content, it does not represent the opinion of the European Commission and the Commission is not responsible for any use that might be made of data appearing therein.

TABLE OF CHANGES	
§ 5.5	New paragraph added to address the minor comment outlined in the Review Report of the European Commission

1. Introduction

The objective of these Guidelines is to develop a Regulation (EU) 2016/679 (GDPR) compliant framework for the specific areas of ENLIGHTENme that include data coming from clinical studies and other activities involving extensive data collection through different levels of phenotyping, life movement and lifestyle monitoring, as well as bio-sample. They aim to provide internal guidance according to deliverable D5.3 which addresses some specific ethics and legal requirements the project must comply with under the Grant Agreement (GA), WP5 "Guidelines for the collection and the use of data (Access policy, informational and legal materials, open Access policy". This is reported below for the readers' convenience:

5.3 Guidelines for the collection and the use of data (Access policy, informational and legal materials, open Access policy (M12). Based on international standards (soft law provisions) and current regulations, D5.3 will provide internal guidance and ensure GDPR compliance. Internal policies will address the obligations of the beneficiaries conducting clinical research reflecting the development of the DMP throughout the project.

Since both biomedical and clinical research will start at a later stage, the guidelines may be updated before the start of the abovementioned studies. Importantly, further changes and clarifications might be added following the remarks of the Ethics Advisor.

2. Data protection compliance in ENLIGHTENme

All project activities must comply with H2020 (now Horizon Europe) Ethics principles and with applicable EU and national legislation. Several ENLIGHTENme tasks imply the processing of personal data, including special categories of data, such as genetic data and data concerning health, which are particularly sensitive data. Such tasks must be in line with the EU General Data Protection Regulation (GDPR).

The full text can be found here and a summary of the definitions and basic principles here.

ENLIGHTENme PBs[1] have all committed to full compliance with the GDPR.

The compliance with the GDPR of the ENLIGHTENme project will be constantly monitored.

[1] Project Beneficiaries (hereinafter PBs).

3. Data summary

The **main legal and ethical issues** addressed by these guidelines are raised by the following activities:

1. Biomedical research involving adults from which human cells/tissues collection is derived and analysis of human biological samples (saliva) obtained during the implementation of the lighting interventions within the target district.
2. Clinical data collected within the scope of monitoring health variations in relation to lighting.

Therefore, these guidelines address individual health and well-being data coming from biomedical and clinical research activities, such as:

1. Instrumental recordings
2. Genetic data
3. Clinical history of life-long morbidities.
4. Self-reported parameters for mental and physical health assessments
5. Sleep diary.

Data are collected for the following purposes and collected/stored in the following ways:

Types of data	**Purposes**	**Collection/storage**
Individual health and well-being data	Biomedical and clinical research developed in WP3	Pseudonymised data. Stored in 2 clouds belonging to provider companies based in an EU member state. A. Cloud to store pseudonymised data (including genetic data) protected through end-to-end encryption B. Cloud system to which data collected by actigraph sensors will be sent (Amazon cloud) Only PBs involved in biomedical and clinical research will have access

		to the cloud (as joint controllers)
Contact data	To invite people to participate in the clinical studies.	Stored separately from other data and accessible only to PBs who need them for the said purposes.

The guidelines are mainly based on the GDPR, namely on the minimum standards set out in the Regulation, as wells as on the definitions, key individuals, roles and responsibilities identified therein.

4. Key definitions

4.1 What is personal data?

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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 (1) GDPR).

4.2 Special category of personal data

Data concerning health and **genetic data** are special categories of personal data under Article 9 of the GDPR, that requires further requirements for processing.

Article 9 (Processing of special categories of personal data):

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data**, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
   (a) the data subject has **given explicit consent to the processing of those personal data for one or more specified purposes**, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Therefore, any processing of health and genetic data must:

1. Have a lawful basis under Article 6 of the GDPR; and
2. Fall within one of the grounds for the processing of special categories of personal data under Article 9 of the GDPR.

Since **the ENLIGHTENme Project relies on consent as the legal basis for data processing**, consent should be given by a clear affirmative action and the project's partners must implement adequate **informed consent procedures** in compliance with the GDPR and the applicable national regulations (see below).

What is data concerning health?

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (Article 4 (15) GDPR).

For the ENLIGHTENme project

Data concerning health are:

1. Instrumental recordings (actigraphic recordings assessing rest-activity circadian rhythms and wearable light sensors).
2. Clinical history of life-long morbidities.
3. Self-reported parameters for mental and physical health assessments, with particular reference to quality of sleep, mood and chronotype.
4. Sleep diary.

What is genetic data?

Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (Article 4 (13) GDPR).

For the ENLIGHTENme project

Genetic data are:

Biological material (saliva) for genotyping and circadian biomarker (melatonin) assessments.

4.3 What does processing mean?

According to Article 4 (2) of the GDPR, processing 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

This includes accessing and sharing personal data.

For the ENLIGHTENme project

PBs involved in the biomedical and clinical research are processing personal data (including data related to health and genetic data) whenever they are performing any operation or set of operations on these data or on sets of personal data, both on paper and in digital form, including the operations listed above.

5. Key individuals, roles, and responsibilities

The GDPR identifies some key individuals.

5.1 Data subject: the identified or identifiable natural personal whose data is being processed (Article 4 (2) GDPR).

For the ENLIGHTENme project

The data subject is the research participant.

In these guidelines, they will be referred to as the data subject.

5.2 Data controller (Article 4 (7) GDPR)**:** 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 (whereas more practical aspects of implementation can be delegated to the processor).

The data controller has responsibility for implementing the appropriate technical and organisational measures to ensure and to be able to demonstrate that all processing of personal data are performed in accordance with the GDPR (art. 24). This includes the storage, access, use and sharing of any samples and personal data up-and downloaded via shared clouds/platforms.

For the ENLIGHTENme project

Each PBs involved in biomedical and clinical research (UNIBO, AUSL, UTARTU, VUA, C@W, SURREY) is a separate controller for any other processing of personal data that may be carried out outside a shared platform for their respective purposes.
Each data controller:

- Determines the purposes and means of the processing (i.e., collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, etc..) of the above-mentioned personal data and bio-samples.
- Shall ensure that all processing of personal data is compliant with the GDPR through the adoption and implementation of appropriate legal, ethical, technical, and organisational measures.
- Shall be able to demonstrate this compliance (e.g.: the consent of the data subject to the processing of his/her personal data; the implementation of the required security measures, etc.)

Responsibilities are linked to the specific role played by each PBs as identified in the GA.

5.3 Joint controllers (Article 26 GDPR): two or more controllers who jointly determine the purposes and means of processing.
According to the guidance issued by the EDPB on this point, the over-arching criterion for consideration of a joint controllership is "the joint participation of two or more entities in the determination of the purposes and means of a processing operation"[2].
Joint participation can take the form of:

1. Joint controllership by means of a common decision, i.e., the partners decide together, and the decision involves a common intention.
2. Joint controllership by means of converging decisions. In this case "the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing". The processing by each party would not be possible without both parties' participation in determining the purposes and means: the processing is inseparable, i.e., inextricably linked.

For example: if several institutes feed the personal data they collect or generate into a shared platform and use the data provided by other project's partners through the platform for carrying out the project-related activities, this relationship is usually included among the examples of collaborative projects provided by the EDPB guidance.

[2] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021.

In this case, each partner qualifies as **joint controller** for the personal data processing that is done by storing and disclosing information to the platform.

For the ENLIGHTENme project

The data controllers are the PBs who determine the purposes and means of the processing (i.e., collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, etc.) of the above-mentioned personal data and bio-samples, namely: UNIBO, AUSL, UTARTU, VUA, C@W, SURREY.
If these PBs share the data as part of a collaborative project and together decide the purpose of the processing and the means to be used, joint controllership from a converging decision will arise.
Whenever applicable, data processing agreements will be signed between the PBs.

5.3 Data processor (Article 4 (8) GDPR): a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

If any PB contracts with a third party to carry out certain processing activities on samples and/or on personal data and dictates the purpose and means, this PB acts as data controller and the third party is the data processor.

Therefore, there are two basic cumulative conditions for qualifying as processor:

a) that the processor is a *separate entity* in relation to the controller (i.e., the data processor will not be an employee of the data controller); and
b) that the processor processes personal data *on behalf of the controller*.

In this case, GDPR compliance requires the data controller to have written data processing agreements in place with all partners acting as data processors on their behalf.

For the ENLIGHTENme project

Example1: ENLIGHTENme PBs who contract with a third party, e.g., a cloud provider, to store, sync, and share samples and/or on personal data, and dictate the purpose and means, act as joint-controllers and the third party is the data processor.

Example 2: some ENLIGHTENme PBs may decide to act as data processors if they don't play a critical role in deciding on the purpose of the processing of personal data and/or on the means to be used, neither through a common decision with other partners nor through a converging decision.

Whenever applicable, data processing agreements will be signed between the PBs.

5.4 Data Protection Officer (DPO)

The DPO is the individual designated to assist the data controller or the data processor to ensure the protection of personal data and monitor compliance with the GDPR.

A DPO must be appointed in several instances. These include cases where the processing is carried out by a public authority or body, as well as the processing of large scale of special categories of data, including genetic data and data concerning health (see above).

The DPO must be a person with expert knowledge of data protection law and practices (Recital 97 GDPR). The contact details of the DPOs shall be made available to all data subjects involved in the research.

For the ENLIGHTENme project

The PBs' DPOs must perform a joint assessment needed for the Ethics requirements imposed by the Grant Agreement (GA), WP8 "Ethics requirements" (Deliverable D8.6), and will submit declarations and documentations covering the following:

1. The DPO declares that the PB is compliant with the respective national legal framework and indicate the applicable data protection national legislation. The DPO also declares if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place.
2. The DPO confirms that:
   - S/he has been duly appointed as DPO by the PB and her/his contact details are made available to all data subjects involved in the research
   - The PB has a lawful basis for the data processing and that appropriate technical and organisational measures are in place to safeguard the rights of the data subjects. The DPO also indicates the lawful basis.
3. The DPO evaluated the ethics risks related to the data processing activities of the project and provide a brief description of the identified ethics risks, if any.
4. The opinion of the DPO on whether or not a Data Protection Impact Assessment under Article 35 General Data Protection Regulation 2016/679 should be conducted.

Importantly, the project activities will not start until the submission of the relevant documentation to the European Commission.

5.5 Update on roles and responsibilities (January 2023)

Although the PBs involved in the activities regulated by these guidelines have indicated the names of the personnel involved in data protection, for greater protection of participants' rights it is essential that the responsibility lies with each PB and the institution to which it belongs. Individuals may indeed change.

These guidelines have a general and guiding value for all project activities falling within their scope and must therefore apply independently from the professional career path of the individuals involved in the project.
In addition, the PBs have signed a specific joint ownership agreement to regulate the project activities covered by these guidelines. This agreement defines in detail the roles and responsibilities of each PB and indicates the names of the relevant persons.
From a legal point of view roles and responsibilities are thus clearly defined and are compliant with the relevant national and European legislation.
In addition, Deliverable 8.6 contains specific statements by the DPO of each PB attesting its compliance with these regulations.

The persons designated by the PBs are:

for AUSL: Francesco Nonino

for UNIBO: Valerio Carelli

for VUA: Meike Bartels, Anne Landvreugd

for UTARTU: Toomas Haller

for SURREY: Debra Skene, Daan Van Der Veen

for C@W: Michelle Luxwolda or Marijke Gordijn

for LSE: David McDaid

6. Basic principles for the processing of personal data

The GDPR sets out the minimum standards that must be met in the processing of personal data. In particular, personal data shall be processed in compliance with the following principles:

- **lawfulness, fairness, transparency**
- **purpose limitation**
- **data minimisation**
- **accuracy**
- **storage limitation**
- **integrity and confidentiality**
- **accountability**

Not only the GDPR but all applicable rules and regulations (including national regulations) must be respected when processing personal data

Lawfulness: there must be a lawful basis on which to process personal data. Article 6 of the GDPR sets out six grounds.

Article 6 (Lawfulness of processing), par. 1, a):

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the **data subject has given consent to the processing of his or her personal data for one or more specific purposes**

Article 9 (Processing of special categories of personal data):

1. Processing of […] **genetic data**, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation **shall be prohibited**.
2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has **given explicit consent to the processing of those personal data for one or more specified purposes**, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Transparency: processing must be transparent, i.e., **detailed information must be provided to the data subject before data collection.**

For the ENLIGHTENme project

The **legal basis** for the processing of personal data in the ENLIGHTENme project is **consent** pursuant to article 6 and article 9 of the GDPR. Consent shall be given by a **clear affirmative action**, i.e., a **written statement**, based on a **detailed information given before collecting data.** PBs must implement adequate **informed consent procedures** in compliance with the GDPR and the applicable national regulations. Conditions for consent and withdrawal of consent, content, and purposes of the information, as well as the related principles set out by the GDPR and the applicable regulations are reported in Deliverable 8.1, and below, Annexes 2, 3 and 4. You can find a template in Deliverable 8.1.

Purpose limitation

Data are collected **only for specified, explicit and legitimate project-related** activities, as specified in the information sheets. Data shall not be further processed in a manner that is incompatible with those purposes.

For the ENLIGHTENme project

PBs can collect and process data only for the specific purposes detailed in the information sheet

Data minimisation

Only necessary data are collected, i.e., data that are **adequate**, **relevant,** and **limited** to what is necessary to the purpose of the project.

For the ENLIGHTENme project

PBs can only collect those data which are really needed to achieve their purposes. For example: if they process data to send an invitation or a newsletter they only need the recipient's e-mail, not residence, phone number, gender or age.

Accuracy

Personal data collected/generated by the project must be accurate and, where necessary, kept up to date.

For the ENLIGHTENme project

Each PBs is responsible to take every reasonable step to ensure accuracy of data having regard to the purposes for which they are processed and erase or rectify inaccurate data without delay. If there are any inaccuracies, data must be erased or rectified as soon as possible.

Storage limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the project-related purposes for which they have been processed.

Pursuant to article 89 of the GDPR, data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and only if appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject are implemented.

For the ENLIGHTENme project

Each PBs is responsible for:

- Keeping personal data, including data concerning health and genetic data, in a form which permits identification of data subjects for no longer than is necessary to achieve the purposes of the biomedical and clinical research as described in the GA (clinical annex) and as identified in the information sheet.
- Implementing any appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject

Please note that keeping old e-mails attachments or documents in the archive is still an act of processing.

After the end of the project runtime only data shall be made publicly available, which has already been stored in pseudo-anonymized (see below) form or which has been already published e.g., in scientific papers or conferences.

Please also note that Article 89 of the GDPR provides several features of the mentioned safeguards:

- They must be appropriate.
- They must be in accordance with the GDPR.
- They must ensure that technical and organizational measures are in place in particular to ensure respect for the principle of data minimization (see Deliverable 8.6 and below §§10 and 11)
- The said measures may include pseudonymization, provided that research purposes can be fulfilled in that manner (see DMP and Deliverable 8.6).
- Where research purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner (anonymization - see DMP and Deliverable 8.6).

The European Data Protection Board (EDPB) has provided some guidance on safeguards. According to the Preliminary Opinion on Data Protection and Scientific Research of the European Data Protection Supervisor, appropriate safeguards could include:

- Conducting a DPIA of likely risks.
- Appointing a DPO.
- Notifying data subjects of a data breach.
- Ensuring data security.
- and data minimisation through pseudonymisation or anonymization,
- informed consent (see Deliverable 8.1)
- access limitations
- professional ethical standards.

Integrity and confidentiality

Appropriate security of data must be ensured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

For the ENLIGHTENme project

PBs must ensure appropriate security in processing the personal data collected/generated. They are responsible to use appropriate technical or organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Accountability

The principle of accountability is closely linked to the GDPR's risk-based approach. Accordingly, data protection should be proportionate to the risks for the data subjects entailed in the data processing: "the higher the risk to individuals, the higher the level of protection, therefore of positive obligations, and safeguards to implement for data controllers and processors"[3].

This principle requires data controllers and data processors to:

- Take responsibility for their processing activities and for having in place measures and records.
- Demonstrate compliance.

For the ENLIGHTENme project

When processing personal data as controllers or as joint controllers, PBs are responsible for the compliance with the mentioned principles. They must also be able to demonstrate compliance. Therefore, adequate documentation must be kept (e.g., signed copies of information sheet, description of security measures, records of processing activities, contracts with data processors).

7. Focus on: the rights of the data subject

The right to the protection of personal data is a fundamental right according to the Charter of Fundamental Rights of The European Union (Article 8). Moreover, the GDPR regulates certain specific rights of the data subject.

The ENLIGHTENme project partners shall implement adequate measures to safeguard the rights and freedoms of the data subjects/research participants in compliance with the GDPR and the applicable national regulations.

Under the GDPR the data subject has the following rights:

- **Right to information (Articles 12, 13, 14)**: each ENLIGHTENme PB acting as data controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 of the GDPR

[3] EDPS, A Preliminary Opinion on data protection and scientific research, 6 January 2020.

relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

- **Right to withdraw consent (Article 7 (3))**: the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- **The right to lodge a complaint with a supervisory authority.**
- **Right of access (Article 15)**: the data subject has the right to obtain from the data controller confirmation that it is processing personal data concerning him or her, access to the personal data and the information included in Article 15, e.g., information concerning the purposes of the processing, the categories of personal information, retention period, and if need be the third parties or intended third parties to whom it has been disclosed.
- **Right to rectification (Article 16)**: the data subject has the right to obtain from the data controller the rectification of inaccurate personal data concerning him or her.
- **Right to erasure (right "to be forgotten", Article 17)**: the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds provided for by art. 17 applies.
  This also includes the right to ask for deletion of data / parts of data on shared cloud-
  This can be done without giving any reason by sending an informal e-mail to an email address that will be made available on the Project website.
- **Right to restriction of processing (Article 18):** in specific cases the data subject has the right to obtain a restriction of processing, and namely where the accuracy of the personal data is contested, where processing is unlawful and the data controller opposes the erasure of personal information and the data subject requests a restriction of its use instead, the controller no longer needs the personal data for processing but are required to keep it for a legal claim, or where the data subject has object to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.
  This also includes the right to restriction of data usage on the shared cloud.
  This can be done without giving any reason by sending an informal e-mail to an e-mail address that will be made available on the Project website.
- **Right to data portability (Article 20)**: Where the processing is based on consent (as in the case of ENLIGHTENme) the data subject has the right to receive his/her personal data in "a structured, commonly used and machine-readable format" and the right to transmit that data to another data controller. This can include the data controller transmitting to another data controller. The exercise of this right should not adversely affect the rights and freedoms of others, including the right to scientific freedom. However, this would need to be demonstrated.

Furthermore, the data subject has the following rights, which do not apply if the processing is based on the data subject's explicit consent, as it is the case of ENLIGHTENme:

- **the right to object (Article 21)**, i.e., the right to object if it falls within one of the grounds set out by Article 21.
- **the right not to be subject to automated decision-making, including profiling (Article 22)**, i.e., the right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her.

8. New data

8.1 Informed consent.

Each data subject must receive detailed information on personal data processing before their data are collected the first time.

For example:

- purposes and legal basis of processing

- data subjects' rights

- details on data controller

- recipients of personal data

- duration of processing

Article 13 - Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information

For the ENLIGHTENme project

- PBs must have the information sheet dated and signed to obtain consent (see the templates in Deliverable 8.1).
- copies of the (fully filled in) information sheets must be kept.
- support to clarify the content of the information sheet must be given, where needed.
- the signed documents must be kept in a secured (locked) place, only accessible to the PB's team.
- all documents must be destroyed when no longer needed.

8.3 Data privacy

The above-mentioned principles apply.

For the ENLIGHTENme project

- all the data collected/generated in the biomedical and clinical research must be fully pseudo-anonymised (see Deliverable 8.6).
- all data of administrative databases are either anonymised or aggregated data.

- roles and responsibilities (data controllers, joint controllers, and data providers) must be clearly defined with reference to each cluster of activities. Data processing agreements based on the foreseen activities and data use/exchange must be used. If needed, follow up addendum will be considered.
- the PBs required to do so have appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For PBs not required to appoint a DPO under the GDPR, a detailed data protection policy for the project will be implemented.

For data security see below, §§ 10 and 11.

8.4. Further ethical principles

Please note that as far as clinical research is concerned, the following principles also apply to the relationship between researchers and research participants.

WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects (excerpts)

General principles
It is the duty of the physician to promote and safeguard the health, well-being and rights of patients, including those who are involved in medical research.

Medical research is subject to ethical standards that promote and ensure respect for all human subjects and protect their health and rights.

While the primary purpose of medical research is to generate new knowledge, this goal can never take precedence over the rights and interests of individual research subjects.

Medical research involving human subjects must be conducted only by individuals with the appropriate ethics and scientific education, training and qualifications.

Groups that are underrepresented in medical research should be provided appropriate access to participation in research

Risks, Burdens and Benefits
All medical research involving human subjects must be preceded by careful assessment of predictable risks and burdens to the individuals and groups involved in the research in comparison with foreseeable benefits to them and to other individuals or groups affected by the condition under investigation.

Measures to minimise the risks must be implemented. The risks must be continuously monitored, assessed and documented by the researcher.

Vulnerable Groups and Individuals
Some groups and individuals are particularly vulnerable and may have an increased likelihood of being wronged or of incurring additional harm.
All vulnerable groups and individuals should receive specifically considered protection.

Medical research with a vulnerable group is only justified if the research is responsive to the health needs or priorities of this group and the research cannot be carried out in a non-vulnerable group. In addition, this group should stand to benefit from the knowledge, practices or interventions that result from the research.

Scientific Requirements and Research Protocols
Medical research involving human subjects must conform to generally accepted scientific principles, be based on a thorough knowledge of the scientific literature, other relevant sources of information, and adequate laboratory and, as appropriate, animal experimentation.

Research Ethics Committees
The research protocol must be submitted for consideration, comment, guidance and approval to the concerned research ethics committee before the study begins.

Informed Consent
Participation by individuals capable of giving informed consent as subjects in medical research must be voluntary.

In medical research involving human subjects capable of giving informed consent, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study. The potential subject must be informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without reprisal. Special attention should be given to the specific information needs of individual potential subjects as well as to the methods used to deliver the information.

After ensuring that the potential subject has understood the information, the physician or another appropriately qualified individual must then seek the potential subject's freely-given informed consent, preferably in writing. If the consent cannot be expressed in writing, the non-written consent must be formally documented and witnessed.

All medical research subjects should be given the option of being informed about the general outcome and results of the study.

For medical research using identifiable human material or data, such as research on material or data contained in biobanks or similar repositories, physicians must seek informed consent for its collection, storage and/or reuse. There may be exceptional situations where consent would be impossible or impracticable to obtain for such research. In such situations the research may be done only after consideration and approval of a research ethics committee.

Research Registration and Publication and Dissemination of Results
Every research study involving human subjects must be registered in a publicly accessible database before recruitment of the first subject.

Researchers, authors, sponsors, editors and publishers all have ethical obligations with regard to the publication and dissemination of the results of research. Researchers have a duty to make publicly available the results of their research on human subjects and are accountable for the completeness and accuracy of their reports. All parties should adhere to accepted guidelines for ethical reporting. Negative and inconclusive as well as positive results must be published or otherwise made publicly available. Sources of funding, institutional affiliations and conflicts of interest must be declared in the publication. Reports of research not in accordance with the principles of this Declaration should not be accepted for publication.

ICH Guidelines

The principles of ICH Good Clinical Practice
2.1. Clinical trials should be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, and that are consistent with GCP and the applicable regulatory requirement(s).
2.2. Before a trial is initiated, foreseeable risks and inconveniences should be weighed against the anticipated benefit for the individual trial subject and society. A trial should be initiated and continued only if the anticipated benefits justify the risks.
2.3. The rights, safety, and well-being of the trial subjects are the most important considerations and should prevail over interests of science and society.
2.4. The available nonclinical and clinical information on an investigational product should be adequate to support the proposed clinical trial.
2.5. Clinical trials should be scientifically sound, and described in a clear, detailed protocol.
2.6. A trial should be conducted in compliance with the protocol that has received prior institutional review board (IRB)/independent ethics committee (IEC) approval/favourable opinion.
2.7. The medical care given to, and medical decisions made on behalf of, subjects should always be the responsibility of a qualified physician or, when appropriate, of a qualified dentist.
2.8. Each individual involved in conducting a trial should be qualified by education, training, and experience to perform his or her respective task(s).
2.9. Freely given informed consent should be obtained from every subject prior to clinical trial participation.
2.10. All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification.
ADDENDUM
This principle applies to all records referenced in this guideline, irrespective of the type of media used.
2.11. The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).
2.12. Investigational products should be manufactured, handled, and stored in accordance with applicable good manufacturing practice (GMP). They should be used in accordance with the approved protocol.
2.13. Systems with procedures that assure the quality of every aspect of the trial should be implemented.

9. Data already collected in previous initiatives or projects

If PBs already have some data and wish to use this in the ENLIGHTENme project, they should

- Check whether the data can be lawfully used in compliance with the GDPR, and namely the origin of the data.
  For example: get written documentation from the person in charge of the previous project and possibly a declaration authorising to lawfully use such data; the compatibility of the new processing in ENLIGHTENme with the processing in the old project must be checked.
- Get a copy of the information sheet and consent form on which the original data recording and processing was based and check if the intended use of the data in the ENLIGHTENme project is in line with it.
- Use only the data needed for the ENLIGHTENme purposes

10. Technical and organisational measures to safeguard the rights and freedoms of data subjects/research participants

Please note that each PBs is responsible for safeguarding the rights and freedoms of the data subject/research participants in compliance with GDPR and the applicable national regulations.

For the ENLIGHTENme project

The technical and organisational measures are described in Deliverable D.8.6, and include:

- Informed consent procedures.
- Policies and procedures to inform without undue delay the data subject/research participants on the processing of personal data pursuant to articles 12-21 GDPR, with particular reference to the rights and freedoms of the data subject/research participants (see above and Deliverable 8.1 and Annex 1),
- Policies and procedures to facilitate and guarantee the management of requests to exercise the rights of the data subject/research participants, relating to the processing of personal data, in a standardised manner and in compliance with the applicable European and national regulations
- Security policies through IT Systems and IT tools
- Data processing registers with risk analysis, impact evaluation and organizational and technical tools to protect personal data
- Procedures to inform about data breach
- Procedures for managing violations in the processing of personal data
- Training courses for administrative staff supporting research teams

11. Security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing

To comply with the GPDR, all PBs will «implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk» (art. 32) and «adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default» (Recital 78).

In addition, all personal data must be stored in computers, laptops, intranet directories, hard-drives, or cloud storage systems protected with security measures, which may include:

- Secure access credentials (i.e., username and password, badge).
- Secure institutional and periodically changed passwords.
- Authorisation levels and identification of role and responsibilities in processing data.
- Automatically updated antivirus, antimalware, anti-ransomware.
- Automatic execution of critical and optional software updates.
- Limitations to the download of executable files.

- E-mail spam filters and automatic checks.
- Automatic backup of all files in PBs servers (at least daily).
- End-to-end encryption.
- Further manual backup on external HDDs.

For the ENLIGHTENme project

The security measures are described in the DMP and in Deliverable D.8.6.

As far as biomedical and clinical research is concerned, please note that the highest level of security must be ensured to comply with the relevant national and European regulations, and especially with the GDPR's strict requirements on implementing data security measures and privacy by design.

The PBs involved in biomedical and clinical research must chose a cloud provider that ensures that high level of security. In particular:

- Personal data will be protected through end-to-end encryption during the whole research project.
- Only PBs involved in biomedical and clinical research will have access to the cloud (as data joint controllers). Permission settings will be used to guarantee that personal data are shared with only those who need to work with them.
- To minimise the risk of data exposure, encryption keys will be controlled by the end-users (i.e., the PBs involved in the biomedical and clinical research), and they will not be accessible to other PBs nor to the service provider.
- No personal data will be transferred/shared outside the cloud (e.g., via email) between PBs or between them and the service providers.
- The cloud will be based in an EEA country.

Data collected by actigraph sensors will be sent to a cloud system belonging to a provider company based in an EEA country. In particular, a Mini-AT Gateway is responsible for creating a seamless interface with both sensors and the Cloud System through wi-fi connection. Both sensor devices have a battery capable of withstanding 1 month with a single charge and uses Bluetooth communication to transmit the data acquired. The cloud platform is a web-based system that gives access upon an authentication to control the hardware devices.

Safety features include:

- HTTPS Communication.
- JSON Web Token (JWT) Authentication.
- Anti-Spoofing Filter.
- Server Location: Digital Ocean Server, compliant with privacy regulations.

Before uploading personal data to the shared cloud, personal data must be stored locally on encrypted parts of a hard disk and backups shall be made in local and password-protected networks.

12. Third-party access to personal data

Health-related data and genetic data collected in the ENLIGHTENme project shall not be accessible to non-project partners. If the ENLIGHTENme PBs will decide to provide third-party access to the data, these guidelines will regulate the related ethical, legal and technical issues. In any case, health-related data and genetic data can be shared on an access-controlled basis only. An appropriate access system must be developed to be compliant with GDPR and other national provisions and this data must be shared under specific access rules. Importantly, access to non-project members will not be provided until the update of these guidelines is submitted.

13. Open Access

With reference to publications, all PBs shall be familiarised with the two main routes to make their research articles available open access, namely by publishing directly in an open access journal (i.e., the 'gold' route) or by self-archiving, i.e., by depositing their final peer-reviewed publication into an appropriate institutional, a subject-based or a centralised repository (i.e., the 'green' route). Gold route OA is preferred in ENLIGHTENme, and sufficient budget has been requested to make this possible.
A publication strategy (deliverable D6.3) details the rules, selection of journals, review processes, guidelines on authorship, acknowledgements etc. This will support publication activities, clarify responsibilities, and avoid delays, disagreements, and misunderstandings, while at the same time allowing for the evaluation of possible IP issues emerging from the research before public release. The evaluation will take place on a case-by-case basis, with all due care, and in good faith. As a rule, no background or results may be disseminated without the approval of its owner.

14. Secondary use

Secondary use is the further processing of data initially collected for another purpose.

While the further processing of anonymous data is generally permissible, personal data, especially health-related data and genetic data, cannot follow the general open access strategy implemented by PBs since such data can be shared on an access-controlled basis only. This means that an appropriate access system must be developed that ensures compliance with GDPR and other national provisions. In particular, this data must be shared under specific access rules and with suitable oversight mechanisms. These may include an access committee reviewing access requests to assess that the data sharing complies with data protection law and fully respects the rights of the data subjects.

Furthermore, data subjects must be adequately informed of secondary uses and their consent must be acquired since data collection. A dynamic consent model supported by seamless and transparent communication may enable the participants to initially give their consent to share data for certain areas of scientific research and then adjust their preferences *vis-à-vis* proposed secondary uses of their data.

Thus, if secondary uses will be foreseen, the PBs must acquire the informed consent of the data subjects and agree on a detailed and legally and ethically compliant access policy, with a clear and transparent allocation of the respective GDPR compliance duties and responsibilities.

15. Breach of personal data

In the case of any personal data breach, the ENLIGHTENme PBs acting as data controller must notify it to the competent supervisory authority without any undue delay, but no later than 72 hours (art. 33 GDPR). Reasons for the delay must accompany the notification to the supervisory authority where it is not made within 72 hours.

The notification shall at least include:

- the description of the nature of the personal data breach;
- the approximate number of personal data records concerned;
- the name and contact details of the DPO or some other contact point or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- the measures taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible (and in so far as it is not possible) to provide the information at the same time, the information may be provided in phases without undue further delay.

The communication of a personal data breach to the data subject depends on a risk assessment of whether the breach "is likely to result in a high risk to the rights and freedoms" of the data subject (art. 34 GDPR).

The data controller is not required to notify the data subjects if:

- It has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the data breach, in particular those that render the personal data as unintelligible to any person who is not authorised to access it (e.g., encryption).
- It has taken effective measures to mitigate against the risks identify and ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
- If the communication of the personal data breach to the data subjects would involve a disproportionate effort. In such cases, a public communication or other equally effective information measures may suffice.

Attachments

Annex 1 DEFINITION OF TERMS AND BASIC PRINCIPLES

PERSONAL DATA (art. 4, par. 1 GDPR)	**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**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
GENETIC DATA (art. 4, par. 13 GDPR)	Personal data relating to the **inherited or acquired genetic characteristics** of a natural person which give **unique information about the physiology or the health** of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
DATA CONCERNING HEALTH (art. 4, par. 15 GDPR)	means personal data related to the **physical or mental health** of a natural person, including the **provision of health care services**, which reveal information about his or her **health status**
PROCESSING (art. 4, par. 2 GDPR)	**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
CONSENT OF THE DATA SUBJECT (art. 4, par. 11 and recital 32, GDPR)	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.**

	(Silence, pre-ticked boxes or inactivity should not therefore constitute consent)
CONDITIONS FOR CONSENT AND WITHDRAWAL OF CONSENT (Recital 32 and art. 7, GDPR)	- Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has **multiple purposes**, **consent should be given for all of them**. - If the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is **clearly distinguishable from the other matters**, in an intelligible and easily accessible form, using clear and plain language. - Prior to giving consent, the data subject shall be **informed** thereof. - The data subject shall have the **right to withdraw** his or her consent at any time. - It shall be **as easy to withdraw as to give consent**. - Where processing is based on consent, the controller shall be able to **demonstrate that the data subject has consented to processing** of his or her personal data.
COMMUNICATION (Articles 12)	The controller shall take appropriate measures to provide any information and any communication relating to processing to the data subject in a **concise, transparent**, **intelligible** and **easily accessible form**, using **clear and plain language.** The controller **shall facilitate the exercise of data subject rights** under GDPR.
INFORMATION	Where personal data relating to a data subject **are collected from the data subject**, **the controller shall**, at the time when personal data are obtained, **provide the data subject with all of the following information**: a) the **identity and the contact details of the controller** and, where applicable, of the controller's representative; b) the **contact details of the DPO**, where applicable; c) the **purposes of the processing** for which the personal data are intended as well as the legal basis for the processing; […] e) the recipients or categories of recipients of the personal data, if any; f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation […]
FURTHER INFORMATION NECESSARY TO ENSURE FAIR AND TRANSPARENT PROCESSING	a) the **period for which the personal data will be stored**, **or** if that is not possible, **the criteria used to determine that period**; b) the **existence of the right to** request from the controller **access** to and **rectification or erasure** of personal data or **restriction of processing** concerning the data subject or to **object to processing** as well as the **right to data portability**; c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the **existence of the right to withdraw consent at any time**, without affecting the lawfulness of processing based on consent before its withdrawal;

	d) the **right to lodge a complaint** with a supervisory authority; […] f) the **existence of automated decision-making, including profiling** […]
FURTHER PROCESSING FOR A PURPOSE OTHER THAN THAT FOR WHICH THE PERSONAL DATA WERE COLLECTED	The controller shall provide the data subject **prior to that further processing** with **information on that other purpose** and with **any relevant further information to ensure fair and transparency processing**.
DATA CONTROLLER (art. 4, par. 7 GDPR)	The natural or legal person, public authority, agency or other body which, **alone or jointly with others, determines the purposes and means of the processing of personal data.**
DATA PROCESSOR (art. 4, par. 8 GDPR)	A natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller.**
JOINT CONTROLLERS (art. 26, GDPR)	Where two or more controllers **jointly determine the purposes and means of processing**, they shall be joint controllers.
PSEUDONYMISATION (art. 4, par. 5 GDPR)	The processing of personal data in such a manner that **the personal data can no longer be attributed to a specific data subject without the use of additional information**, provided that such **additional information is kept separately** and is **subject to technical and organisational measures** to ensure that the personal data are not attributed to an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. GDPR provides indications as to what should be intended as "identifiable": - To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used**, such as singling out, either by the controller or by another person **to identify the natural person directly or indirectly**. - To ascertain whether means are reasonably likely to be used to identify the natural person, **account should be taken of all objective factors**, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. (Recital no. 26, GDPR).
ANONYMOUS INFORMATION (Recital 26)	Information which does **not relate to an identified or identifiable natural person** or to **personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable**. Therefore: **Anonymous data** are data that have no links to the individual (e.g., the data and/or the samples have never been associated with identifiers), and the risk of identification is very low.

	Anonymised data are data (or samples) that have been identified or coded, but there is no longer any link to the individual since the identification, or the code and the code key have been destroyed. According to the GDPR: - **whenever identifying data are not needed** to achieve the specific purposes of data processing, **anonymous data should be used** (e.g., aggregated data for statistical purposes); - if data are anonymous, **GDPR does not apply**, as data do not refer to an identified or identifiable natural person.
PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (art. 5, GDPR)	Personal data shall be processed in compliance with the following principles: - **lawfulness, fairness, transparency** - **purpose limitation** - **data minimisation** - **accuracy** - **storage limitation** - **integrity and confidentiality** - **accountability**
FURTHER OBLIGATIONS FOR PBs	- Adequate technical and organisational measures - Records of processing activities - Data Protection Impact Assessment - Appointment Of Data Protection Officer (DPO)
SAFEGUARDS AND DEROGATIONS RELATING TO PROCESSING OF PERSONAL DATA FOR SCIENTIFIC OR HISTORICAL RESEARCH (ART. 89 GDPR)	Processing is subject to **appropriate safeguards for the rights and freedoms of the data subject**. Those safeguards: - shall ensure that **technical and organisational measures** are in place in particular in order to ensure respect for the **principle of data minimisation**. - Those measures may include **pseudonymisation** provided that research purposes can be fulfilled in that manner. - Where research purposes can be fulfilled **by further processing which does not permit or no longer permits the identification of data subjects,** those purposes **shall be fulfilled in that manner.** Union or Member State law may provide for derogations from the rights referred to in Articles 15 (Right of access by the data subject), 16 (right to rectification), 18 (Right to restriction of processing) and 21 (right to object) of the GDPR only: - subject to the said **conditions and safeguards** - in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

Annex 2 CONSENT TO THE PARTICIPATION IN RESEARCH

INFORMED CONSENT (adults) - DEFINITION	A subject's **free and voluntary** expression of his or her **willingness to participate** in research, **after having been informed** of all aspects of the biomedical and clinical research that are relevant to the subject's decision to participate.
GENERAL PRINCIPLES	Research may be conducted only if:

	(a) the rights, safety, dignity and well-being of subjects are protected and prevail over all other interests; and (b) it is designed to generate reliable and robust data.
INFORMED CONSENT – REGULATION (ART. 28, par. 1)	Informed consent shall be: - **written** - **dated** - **signed** by the person performing the interview and by the subject (or his or her legally designated representative) **after having been duly informed**. Where the subject is unable to write, consent may be given and recorded through appropriate alternative means in the presence of at least one impartial witness. The subject (or his or her legally designated representative) shall be provided with a copy of the document (or the record) by which informed consent has been given. The informed consent shall be **documented.** **Adequate time** shall be given for the subject (or his or her legally designated representative) to consider his or her decision to participate in the biomedical and clinical research.
INFORMATION (Art. 28, par. 2ff)	Information given to the subject shall: a) **enable the subject** (or his or her legally designated representative) **to understand**: (i) the nature, objectives, benefits, implications, risks and inconveniences of the research; (ii) the **subject's rights and guarantees** regarding his or her protection, in particular his or her **right to refuse to participate** and the **right to withdraw at any time without any resulting detriment** and **without having to provide any justification**; (iii) the **conditions under which the research is to be conducted**, including the expected duration of the subject's participation in the research. (b) be kept **comprehensive, concise, clear, relevant, and understandable** to a layperson. The **information shall be prepared in writing** and be available to the subject. In the interview: **- special attention shall be paid to the information needs** of specific patient populations and of individual subjects, as well as to **the methods used to give the information**. - it shall be **verified that the subject has understood the information**.

Annex 3 CONSENT TO THE PERSONAL DATA TREATMENT – Information included in the information sheet

A specific information sheet regarding the processing of personal data will be provided by each beneficiary – as an independent Data controller – to the participant (data subject), pursuant to

articles 13 and 14 of Regulation (EU) 2016/679 – GDPR, in addition to any other more stringent rules envisaged by the single beneficiary. In particular, this information sheet includes:

• the **identity and contact details of the data controller** and, where applicable, of its representative;
• the **contact details of the DPOs**;
• the **purposes and the legal basis of the processing**;
• any legitimate interests pursued by the data controller or third parties;
• the **categories of personal data processed and the source from which they originate**;
• any **recipients or any categories of recipients of personal data**;
• who has **access to the data** and **how third-party access** is regulated;
• in case, **the intention of the controller to transfer personal data to a third country** or an international organization and the existence or absence of a Commission adequacy decision or, in the case of transfers under articles 46 or 47, or to the second subparagraph of article 49, the reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
• the **period of storage** of personal data **or at least the criteria used to determine this period, specifying whether the data will be cancelled, destroyed or stored in a public database after the end of the project**;
• the existence of the **right to request from the controller access to and rectification or erasure of personal data or restriction of processing** concerning the data subject **or to object to processing** as well as **the right to data portability (specifying if the erasure of data is not possible)**;
• the existence of **the right to withdraw** consent at any time and how to exercise it, without affecting the lawfulness of processing based on consent before its withdrawal;
• the **right to lodge a complaint** with a supervisory authority;
• whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

Annex 4 COMMON PRINCIPLES AND PROCEDURES

The consent forms will include, on the one hand, consent to participate in the research, and, on the other hand, consent to the personal data treatment, if requested as the relative legal basis pursuant to art. 6, par. 1, a) of Regulation (EU) 2016/679 - GDPR.

- **The information sheets, as well as the consent forms, shall be in a language and will use terms fully understandable**, shall be **dated** and **approved** (signed if they are paper sheets; by an approval using a radio button if they are electronic sheets).
- The **participants will be asked to read, fill and sign consent forms in written** (or using a radio button), **declaring they have read and understood the information received**.
- **Participants will keep information sheets** and the **signed consent forms will be collected and stored by the researchers** (if it is a paper sheet).
- For all c**ases when the consent is not personally collected, the participant will be asked to connect to a secured server** in which he/she can give **online informed consent** even in this case both towards participation in the research, and the processing of personal data, if identified as its legal basis. A copy of those electronic documents will be stored on the secure research group storage system.
- If the consent cannot be given in writing, for example because of illiteracy, **the non-written consent will be formally documented and independently witnessed**.

- It is, in any case, the **responsibility of each beneficiary, as an independent Data controller, to identify and formalize any agreements of co-ownership with subjects outside the consortium**.
- The **information sheets** (regarding participation to the research and data protection) **and related consent forms will be administered to all participants.**
- Information will be presented by specifically instructed research staff **clearly, using short, understandable sentences** and **technical terms will be avoided as much as possible**.
- The researcher **will proceed with the participant only if s/he correctly and fully understands the information provided**.
- The information sheets and related consent forms will be **submitted to local Ethics Review committees** before the beginning of the study in accordance with local regulations.
- **No remuneration will be offered for participation** in the studies and particular care will be taken to ensure that consent is given freely and without any coercion.
- ENLIGHTENme **investigators will not collect or utilize samples that were collected for reasons unrelated to the project.**