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

Deliverable D5.4
Policy model for the assessment, governance and long term use of the biosamples and datasets.

Contractual delivery date:
M6: 28.02.2023

Actual delivery date:
M12: 28 02.2023

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	D5.4
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, Valerio Carelli (UNIBO)
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.

1 Introduction

The objective of this document is to develop a Regulation (EU) 2016/679 (GDPR) compliant framework for the specific areas of ENLIGHTENme that include bio-samples and datasets coming from biomedical studies (WP3). The policy aims to provide internal guidance according to deliverable D5.4 which addresses some specific ethics and legal requirements the project must comply with under the Grant Agreement (GA).
This is reported below for the readers' convenience:

"D. 5.4 – *Policy model for the assessment, governance and long-term use of the biosamples and datasets",* which, more precisely, is meant to be a "*Guidance for the long-term exploitation of the collected biomaterials ensuring sustainability plans".*
Further changes and clarifications might be added following the remarks of the Ethics Advisor.

1. Background

As a rule, ENLIGHTENme PBs[1] involved in the activities addressed by this policy will sign a joint controllership agreement according to which:

"The Parties agree that ***it is not possible to retain or process personal data that has been shared for longer than the time required to achieve the agreed objectives****.* ***As an exception*** *to that established above, the* ***Parties may continue to retain shared personal data*** *for the retention periods provided for by law".*

The sharing of data and their long-term use is extremely useful for scientific development, especially in the biomedical field.
Nevertheless, the scientific importance of data sharing must be balanced against other potentially conflicting rights and interests.
Among these, specific protection is foreseen for the rights of research participants with regard both to their willingness to participate in research and to the processing of their data.
The European data protection framework derives from several specific sources (see below Annex 1), which may concern:

- data protection in general
- data protection in the research context
- the regulation of some specific fields, such as, for instance, in the case of the ENLIGHTENme project, the biomedical field and biological samples.

These instruments may have different nature and legal value at different levels, and namely:

[1] Project Beneficiaries (hereinafter PBs).

- International, such as charters of fundamental rights or documents containing ethical principles for the biomedical field.
- European and therefore binding on member states to the point of direct applicability in the case of EU regulations. At the European level, it should be remembered that the protection of personal data is provided for as a fundamental right by the Charter of Fundamental Rights of the European Union (which since the entry into force of the Lisbon Treaty has the same legal force as the Treaties). Moreover, the GDPR provides specific rules on the use of data for scientific research purposes and some principles relevant to the long-term use of data.
- National.

From this point of view, multinational projects such as ENLIGHTENme represent an asset on a scientific level but require an appropriate balance between relevant principles and regulatory levels.
For these reasons, the definition of a shared policy among all PBs is essential, as well as their commitment to be compliant with the relevant international, European and national regulations.

As outlined by the EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (EDPB Guidelines 03/2020), the use of health data for the purpose of scientific research can be either:

1. Primary, i.e., the use of data directly collected for the purpose of scientific research.
2. Secondary, i.e., the further use of data initially collected for a different purpose.

Secondary uses of personal (health) data are permitted, provided that:

- this is **in line with the original consent** given by the research participants.
- and **appropriate safeguards** are in place to protect the fundamental rights of the research participants.

Moreover:

- **Dynamic consent models** supported by seamless and transparent communication enable the participants to adjust their preferences *vis-à-vis* proposed further uses of their data.
- **This is especially sensitive for countries where reconsent for further use is always a legal requirement, as in Italy, unless the national authority (garante) gave specific permission to proceed with further uses.**
- This should be **embedded in appropriate governance and oversight mechanisms**, with a specific body (e.g., an access committee) with the mission to **ensure that secondary uses comply with applicable regulations and the fundamental rights of the participants are respected**.

3. Aims of the policy

This document aims to:

- Identify the relevant ethical and legal principles to guide the long-term exploitation of the biomaterials and data collected within the ENLIGHTENme project ensuring sustainability plans
- Safeguard research participants' rights and interests while enabling the ethical secondary use of bio-samples and data for scientific research.
- Ensure and promote ethical best practice in the collection, storage, sharing and long-term exploitation of the biomaterials and data collected within the ENLIGHTENm in compliance with the international, European and national relevant regulations, including the upcoming Health Data Space that may impact this guidelines once enforced.

Since the principles applicable to data processing and the protection of research participants (also intended as data subjects) have already been clarified in other deliverables, this policy will only recall them and focus on the additional guidance related to the secondary use of data.

4. Application of the policy

The **main legal and ethical issues** addressed by this policy 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. Health data collected within the scope of monitoring health variations in relation to lighting.

This policy therefore concerns WP3 activities and **must be implemented by the PBs involved, namely UNIBO, AUSL, UTARTU, VUA, C@W, SURREY, LSE.**

5. Collection, storage and use of biosamples and data in the ENLIGHTENme project

This policy addresses individual health and well-being data coming from biomedical research activities.

The PBs have undertaken to collaborate on the research project "ENLIGHTENme", in relation to which they shall jointly determine the purposes and means of the following processing activities:

- Participants' recruitment and data and biological (saliva) samples collection;
- Saliva samples exchange and extraction of total DNA for nuclear and mitochondrial DNA analysis;
- DNA aliquots transfer for specific nuclear and mitochondrial DNA analysis;
- Genotyping of DNA samples (nuclear and mitochondrial DNA);
- Saliva samples exchange and melatonin analysis;
- Actigraph/light sensors distribution and related data collection;
- Data analysis and elaboration with regard to the objectives of ENLIGHTENme;
- Data gathered through questionnaires.

As to datasets

With reference to the data processing activities of the project and the categories of vulnerable data subjects concerned (Elderly: over 65 years), PBs working in WP3 (UNIBO, AUSL, UTARTU, VUA, SURREY, C@W and LSE):

- **pseudonymize** personal data they collect or generate
- and store them into shared platforms/repositories and use the data provided by other PBs through the platform for carrying out the project-related activities foreseen in WP3.

  In this case, each PB (UNIBO, AUSL, UTARTU, VUA, SURREY, C@W and LSE) qualifies as joint controller for the personal data processing that is done by storing and disclosing information to these platforms/repositories (WP3 of the project). However, each PB is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

As to saliva samples

The collected saliva samples will be:

- **pseudonymised**
- and sent to be analysed for the study in Estonia (at the Institute of Genomics University of Tartu), in the Netherlands (at Chrono@Work, which is a spin-off of the University of Groningen, and in Italy (at the IRCCS Istituto delle Scienze Neurologiche in Bologna). They will be **stored in the related biobanks**.

The results of the analyses are **pseudonymised** as well and will be used for the purposes of the project only.

6. Data protection and participants' rights 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). They also must fulfill as appropriate, specific national derogation or specific rules.

The full text can be found here and a summary of the definitions and basic principles in Annex n. 3 below.

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

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

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

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

Three deliverables have been submitted and shared with all PBs on this topic to ensure internal guidance on data protection compliance.

The main content of these deliverable is reported below **to facilitate the guiding role of the principles, guidelines and policies that PBs shall respect in their activities.**

Deliverable 8.1

The deliverable addresses the following ethical and legal requirements the ENLIGHTENme project must comply with: • The procedures and criteria that will be used to identify/recruit research participants • The informed consent procedures that will be implemented for the participation of humans • Templates of the informed consent forms and information sheets including personal data protection (in language and terms intelligible to the participants) • Assurance that households with children will be excluded from the study in WP3. • Measures to protect vulnerable groups/individuals and description of how to minimise the risk of their stigmatisation. This must be submitted as a deliverable. • Details on an incidental findings policy • A risk assessment regarding the potentially deleterious effects of the interventions on the participants health.

Deliverable 8.1 also includes copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans must be submitted as a deliverable.
For the basic principles on consent see Annex 2 (tables, A, B and C).

Deliverable D 8.6, which includes:

- **Statements of the DPO each PB** involved in the processing of personal data. Each statement declares that the **PB is compliant with the respective national legal framework**; that a DPO 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; that the PB has a legal basis for the data processing and that appropriate technical and organisational measures are in place to safeguard the rights of the data subjects. The statement contains as well the evaluation of the ethics risks related to the data processing activities and the DPO opinion on the DPIA.
- Explanation of how all of the data the PBs intend to process is relevant and limited to the purposes of the research project (in accordance with the **'data minimisation 'principle**). According to the deliverable, **each ENLIGHTENme PB intends to process only personal data relevant and limited to the purposes of the research project in compliance with the applicable European and national regulations.**
- A description of the **technical and organisational measures** that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable. It must be stressed 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** (the related rules and principles have been submitted and shared with all PBs as deliverable: see D.8.1).
- A description of the **security measures** that will be implemented to prevent unauthorised access to personal data or the equipment used for processing. **Each PBs is responsible for the compliance with the relevant regulations.**
- Description of the **anonymisation/pseudonymisation techniques** that will be implemented must be submitted as a deliverable. **Each PBs is responsible for the compliance with the relevant regulations.**
- Evaluation of the ethics risks related to the data processing activities of the project. **The DPOs of the PBs conducting WP3 research and acting as joint controllers have thoroughly discussed the need for DPIA.**

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

This document offers guidance for the collection and the use of data in WP activities and contains:

- Key definitions
- Key individuals, roles, and responsibilities
- Basic principles for the processing of personal data
- Focus on the rights of the data subject
- Principles related to new data (informed consent, data privacy, further ethical principles)
- Principles related to data already collected in previous initiatives or projects
- Technical and organisational measures to safeguard the rights and freedoms of data subjects/research participants
- Security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing
- Third-party access to personal data
- Open Access
- Secondary use
- Breach of personal data

Moreover:

- ENLIGHTENme PBs have all committed to full compliance with the relevant national regulations.
- WP3 PBs will sign a joint controllership agreement which regulates all these issues.

7. Legal and ethical framework for secondary use: basic principles

As a rule, Article 5 (1) (b) of the GDPR requires data to be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". This is known as the **purpose limitation principle.**

Article 5 (1) (b) of the GDPR also foresees a "compatibility presumption".
According to this presumption "further processing for […] scientific research purposes […] shall, in accordance with Article 89 (1), **not be considered to be incompatible with the initial purposes**".

The scope of such a presumption is, however, not entirely clear, particularly its impact on the legal basis required for the further use of the data. To date, this issue still requires regulatory clarification. The planned EDPB guidelines on the processing of health data for the purpose of scientific research will consider this topic in more detail. In any event, also considering the sensitive nature of health data, **it is advisable to ensure that the further use of data for research is supported by an appropriate legal basis and, particularly, the explicit consent of the research participant.**

In this regard, GDPR Recital 33 suggests **the use of a broad consent** from data subjects to facilitate secondary uses of personal data for research "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or research projects to the extent allowed by the intended purpose" (GDPR, Recital 33).

On the other hand, the EDPB Guidelines 05/2020 on consent under Regulation 2016/679 stated that: "**Recital 33 does not disapply the obligations with regard to the requirement of specific consent**. This means that, **in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose**. **For the cases where purposes for data processing within a scientific research project cannot be specified at the outset**, Recital 33 **allows as an exception** that **the purpose may be described at a more general level**.

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, Article 29 Working Party (WP29)[2] notes that **when special categories of data are processed on the basis of explicit consent** (as it is the case for the ENLIGHTENme project – see deliverable D.8.6 and D.5.3 mentioned above), applying the flexible approach of Recital 33 will be subject to **a stricter interpretation and requires a high degree of scrutiny**.
According to WP 29 "when regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked" [3].
More precisely "When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research

[2] WP29 "is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR)": https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en
[3] WP29, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018.

advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research"[4].

Against this backdrop, the EDPS Preliminary Opinion on data protection and scientific research (EDPS Preliminary Opinion) stated that "innovative forms of consent in research activities, like tiered and **dynamic consent** […] are promising practices that should be further encouraged and developed".
This is because they are "means for giving individuals more control and choice and thereby for upholding society's trust in science".
For these consent mechanisms to be effective, an **ongoing communication with the research participants on potential further uses of data for research should also be ensured**.
In particular, as recommended by the EDPB, "in case of further use for a different purpose, **the participants must be informed before further processing takes place, even if the purpose is compatible**".

Furthermore, Article 5 (1) (b) of the GDPR requires **compliance with Article 89 (1) of the GDPR**. This latter stipulates that the further use of data for research is subject to "**appropriate safeguards**". Such "safeguards shall ensure that **technical and organizational measures** are in place in particular in order to ensure respect for the **principle of data minimisation**. Those measures may include **pseudonymisation** provided that those purposes can be fulfilled in that manner.
Moreover "where those 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" (i.e, **anonymisation**).

In this connection, considering the sensitive nature of health data and the risks when re-using health data for the purpose of scientific research, the EDPB Guidelines 03/2020 advise that "strong measures must be taken in order to ensure an appropriate level of security as required by Article 32 (1) GDPR", and that the **safeguards should at least include encryption, non-disclosure agreements and strict access role distribution, access role restrictions, and access logs**. The EDPS Preliminary Opinion also specified that "even where consent is not appropriate as a legal basis under GDPR, informed consent as a human research participant could still serve as an 'appropriate safeguard' of the rights of the data subject" as empowering the participant to exert more control over their own data.

Finally, additional safeguards can be identified in international instruments on health data sharing for research. These point to the importance not only of informed consent, but also of ethics review of the research project underlying the data secondary use, transparent and accountable and oversight mechanisms. In sum, data sharing for research should be subject

[4] Ibid.

to effective and publicly accessible governance procedures that clearly allocate duties and responsibilities. A mechanism increasingly used for such purposes of the adoption of an access committee screening data access requests by researchers.

To complement the above-mentioned principles (**lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability)**, the secondary use of the health data and bio-samples collected by the ENLIGHTENme project must comply with the following principles and **each PBs is responsible for being compliant with them.**

Legitimacy. It means that the secondary use of health data and bio-samples must be compliant with all applicable European and national regulations.

Respect for research participants and informed consent.
Since the secondary use of health data and bio-samples may have implications for participants and at times their families, researchers must respect their views, including the right to self-determination and the right to integrity, as well as, if applicable, the views of their families.
Informed consent is the ethical and legal tool to protect participant's rights.

Privacy and data protection. The secondary use of health data and bio-samples must respect the participants' privacy, confidentiality and data protection. Since the right to the protection of personal data, as well as the right to privacy and family life are fundamental rights (e.g., the European Charter of Fundamental Rights of the European Union; GDPR) any limitation must be necessary, limited, proportionate, accountable, and transparent with safeguards in place to continue to protect the essential core of the participants' rights. With reference to data protection and related safeguards see Annex 3.

Data custodianship: a valuable and sustainable secondary use of the health data and bio-samples collected during the ENLIGHTENme project depends on the data being **secure, accessible, good quality,** with **clear procedures** in place to provide access to the data for further research based on robust ethical, legal and scientific principles. **Trustworthiness** is linked to this principle since both the use and re-use of health data and bio-samples must be done in a manner that promotes trust and trustworthiness amongst participants, as well as the scientific community.
To ensure trust, the decision process on secondary use must be guided by the following principles: **Transparency, Consistency, Accountability.**
It means that:

- The process to decide on access for the secondary use of health data and bio samples must be transparent, in line with the principle of informed consent;
- Decisions on use and re-use of health data and bio-samples must follow clear and transparent criteria and procedures, that must be uniformly applied. Exceptions must be justified.

- The PBs, which are custodians of the health data and bio-samples must be accessible to respond to participants and those seeking access to the secondary use of the collected data. They are responsible for compliance with the relevant European and national regulations.

8. Implementing the legal and ethical framework for secondary use in the ENLIGHTENme project

8.1 Informed consent

Further use of the health data and bio-samples collected by the ENLIGHTENme project shall be **in line with the original consent** obtained by research participants.

At the time of the informed consent procedure PBs did inform participants of the possibility to consent to the secondary use of their health data and bio-samples. This consent clause was separated from the consent to participate in the research and to the related data processing. Participants has been informed:

- that they can consent to the processing of data for the ENLIGHTENme project but refuse to consent to their secondary use.
- that and how they can withdraw their consent for secondary use
- where the data will be held
- how they will be informed about the future use of their data
- about the governance process for the secondary use of their data and bio-samples.

PBs gave to research participants the possibility to provide their consent to be re-contacted to give their consent for secondary use of their health data and bio-samples, based on the explanation of the new purpose of their use.

Consent templates for the ENLIGHTENme project (**as approved by the ethics committee of each PB**) contained the following information:

- Once the project is over, the saliva samples will be destroyed.
- They will not be destroyed only if the participants decided with his/her **specific informed consent** that they will be kept at the biobank for sample storage **for the time and purpose expressed in the consent.**
- **If there are specific national derogation made clear at the time of consent**

8.2 Withdrawal of consent and ongoing information to the research participants

All participants have the right to amend and/or withdraw their consent to secondary use of their data and bio-samples at any time. The informed consent procedure must include this information.

Research participants shall be made aware that data that has already been used may need to be maintained to ensure scientific integrity.
Ongoing communication with the research participants on potential further uses of their health data and bio-samples for further research should also be ensured. This is based on the participants' **consent to be re-contacted** to obtain their consent for secondary use when the research purpose is known.
For this purpose, seamless and transparent communication shall be used by PBs to build **dynamic content models**, which ensure the participants to adjust their preferences *vis-à-vis* proposed further uses of their data.

8.3 Incidental findings

With reference to biomedical and clinical research, incidental findings cannot be excluded although the risk is very limited due to the type of analysis that will be carried out. The PBs involved in biomedical and clinical research have addressed the possibility of discovering incidental findings and the issue whether to communicate them to participants (see deliverable 8.1).
The results of the ENLIGHTENme are not findings with diagnostic value. Since further use of the health data and bio-samples collected must be in line with the original content and purpose, in case of unexpected findings deriving from secondary use, this information will have to be verified by further examinations according to a specific pathway aiming at a diagnosis.
Therefore, unexpected or incidental findings will only be provided if the participant agrees to be contacted again. In addition, in the event that variants associated with genetic diseases emerge, the participant will receive a genetic counselling with a specialised doctor from whom the participant and his/her family can seek clarification and further information.
The types of possible incidental findings and the conditions of their disclosure are expressly stated in the information sheet and in the consent form.

8.4 Compliance with Article 89 (1) of the GDPR: appropriate safeguards

Accordingly, PBs shall ensure:

- that the required **technical and organizational measures** are in place
- the **principle of data minimization**
- **pseudonymisation** of datasets and bio-samples, provided that those purposes can be fulfilled in that manner. In any case, where the 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 (i.e, **anonymisation**).

See Annex 3 and Deliverable 8.6 and 5.3.

8.5 Data security

As stated by the above- mentioned regulations and guidelines, security measures shall at least include:

- **Encryption**
- **non-disclosure agreements**
- **strict access role distribution,**
- **access role restrictions**
- **access logs**.

Each PB has declared the technical, organizational and security measures in place in deliverables no. 8.6 and in the Data Management Plan. Internal guidance has been given in deliverable D.5.3.
Each PB is responsible for maintaining the same security levels guaranteed during the ENLIGHTENme project (as defined in D8.6, D. 5.3 and in the Data Management Plan) for possible long-term use of the data and bio-samples.
If this is not possible, it must arrange for the data and samples to be stored in another institution that guarantees adequate security standards.
For each secondary use of the collected data, an adequate risk assessment and thus a DPIA must be foreseen in compliance with the relevant European and national regulations.

8.6 Assessment: independent body

The secondary use of health data and bio-samples **must be embedded in appropriate governance and oversight mechanisms based on the advice of an independent institutional body.**

Each PBs is responsible for:

- compliance with the applicable European and national regulations, and
- obtaining a favorable advice from the independent body which, according to the applicable national legislation, is competent to give it.

8.7 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.

9 Attachements

Annex 1 Main legal instruments[5]

Instrument	Publishing body and year	Applicable to
GDPR	European Union – 2016 (Directly applicable on 25 May 2018)	Any company/entity, which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data are processed; or a company established outside the EU offering goods/services or monitoring the behaviour of individuals in the EU

[5] Taken – with some modifications – from Staunton C, Slokenberga S, Mascalzoni D. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. Eur J Hum Genet. 2019 Aug;27(8):1159-1167. doi: 10.1038/s41431-019-0386-5. Epub 2019 Apr 17. PMID: 30996335; PMCID: PMC6777499, in particular Table 1 and 2.

Charter of Fundamental Rights and Freedoms of the European Union	European Union – 2000 (Binding value starting from the Lisbon Treaty, 2007)	EU Member States
European Convention on Human Rights	Council of Europe (CoE) – 1953	Member States of the CoE
Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention)	CoE – 1997	States that have signed and ratified the Convention (some states have signed but not ratified – for them the Oviedo Convention has a persuasive value)
Convention for the protection of individuals with regard to the processing of personal data	CoE 1980 (revised 2018)	States that have signed and ratified the Convention
Declaration of Helsinki	World Medical Association (WMA)- The 2013 edition	Doctors (but persuasive for all health researchers)
Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks	WMA - 2002 (revised 2016)	Doctors (but persuasive for all health researchers)

Annex 2 INFORMED CONSENT – BASIC PRINCIPLES AND PROCEDURES

Table A

INFORMED CONSENT TO PARTICIPATE IN THE RESEARCH
In all WPs involving research participants, the purpose of the research and information relating to participation are **explained orally and through an appropriate information sheet** (both the paper information sheet and the electronic one on the website, app, etc.), containing: • a **clear description of the aims, methods/assessment procedures, duration, and implication of the participation** of the subject in the research; • the **nature of the participation** (why the participant has been selected) and **any effects** (benefits, risks or discomfort) that might be involved; • **confidentiality issues** and **how the research group will deal with the data**, who will be using the data (national and foreign universities) and the **measures used to secure pseudo-anonymisation** handling and **analysis of the data** (e.g., means and duration of storage, and measures used to protect the data stored; persons having the access to the data files; how the data will be treated after the completion of the research); • that **publicatio**n (including publication on the internet) **of the data of the research does not lead** (either directly or indirectly) **to a breach of agreed confidentiality and anonymity** and **no identifying information on the participant will appear**;

• a statement that **participation is voluntary,** and they **have the option of not participating at all, or not respond to any specific question/item** which they do not want to respond, or **withdraw** from the survey, groups, forums, etc. within a specified time limit, **without stating a reason and without any negative consequences** (e.g., sanction, adverse criticism, loss of privileges) for the withdrawing person or their organization/Institution. This includes the specification of **the right to have the data of the person permanently deleted from the files in case of withdrawal**. The time limit of withdrawal will be set up according to the timing of the research: in any case prior to the destruction of personal data; • information of the procedure that the Consortium has defined to manage unexpected incidental findings; • information about the **Institution that is in charge of the research, funders, project website, the contact details** (name, address, phone number, e-mail) of the person to be approached for any question of concern on the research and rights and the person in charge of the use of data

Table B

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.

Table C

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.**

Annex 3 DEFINITION OF TERMS AND BASIC PRINCIPLES ON DATA PROTECTION (GDPR)

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	Processing is subject to **appropriate safeguards for the rights and freedoms of the data subject**. Those safeguards:

HISTORICAL RESEARCH (ART. 89 GDPR)	- 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.