BioData.pt | ELIXIR PT Ethics and Legal Policy

Historic of versions:
Version 2 - upon addition of INESC-ID Direction's recommendations, on the 30th of September 2020

1. Considerations

1.1 The BioData.pt | ELIXIR PT founding documents place special emphasis on the development of an "ELIXIR Ethics Policy" to support the sharing of data underlying specific regulatory requirements, especially Personal Data including Sensitive Data.

BioData.pt | ELIXIR PT Services do not produce or own personal data and are not involved in getting informed consent from research participants, for example - so their role centres around aspects of safekeeping and provision of data for secondary use via repositories.

1.2 Some BioData.pt | ELIXIR PT Services manage, however, data from human research participants, which are used in the context of clinical and health research. Gaining and deserving the trust of patients, study participants and donors concerning the proper handling of their data is of utmost importance for research to proceed and generate benefits for society.

1.3 The purpose of this Ethics and Legal Policy is to support making scientific data available in the context of BioData.pt | ELIXIR PT in an ethically and legally sound manner, consolidating requirements shared across all BioData.pt | ELIXIR PT Members and Services, including those arising from the BioData.pt | ELIXIR PT founding documents.

1.4 BioData.pt | ELIXIR PT recognises that while data and knowledge provided by BioData.pt | ELIXIR PT Services will be accessible this does not mean that the use of data is unencumbered: restrictions on the use of data may arise due to legal (e.g. data protection requirements, copyright protection, or license restrictions) or ethical considerations. Copyright, intellectual property or licensing considerations are not covered in this policy.

1.5 BioData.pt | ELIXIR PT recognises that the purpose of many BioData.pt | ELIXIR PTServices is to facilitate the open sharing of research data; they do not assume the

ownership of the data but provide a platform where Data Controllers/Providers can share their data with the community.

1.6 Every BioData.pt | ELIXIR PT Service (i.e. Node-funded Services included in Service Delivery Plans) involving Personal Data including Sensitive Data must have a regulatory framework ensuring that these data are made available for research in a way that is compliant with all relevant (e.g. EU-level, national and local or internal) legal and ethical requirements.

1.7 The BioData.pt | ELIXIR PT Nodes are responsible for the implementation of the requirements of the Policy with respect to the provision of BioData.pt | ELIXIR PT Services. The Policy does not prescribe how the specific requirements are met; this is up to the Node.

1.8 BioData.pt | ELIXIR PT Services make data available for research on the basis of scientific best practice and conventions and using state of the art technology. Via mechanisms for knowledge exchange and capacity building across its Nodes, BioData.pt | ELIXIR PT ensures excellence in the delivery of BioData.pt | ELIXIR PT Services.

1.9 This Policy provides evidence that an adequate level of protection of Personal Data including Sensitive Data is in place throughout BioData.pt | ELIXIR PT, which increases the acceptance of clauses in Consent forms concerning data deposition with BioData.pt | ELIXIR PT Services. This is especially relevant with respect to gaining approval of ethics committees or other competent oversight bodies, which are established on the basis of a variety of laws and regulations and in very different ways both with respect to their composition as well as the scope and granularity of ethical reviews.

1.10 This Policy is intended to provide the required basis to satisfy the ethics requirements of funders, such as for example those of the European Commission's Horizon 2020 framework and the Foundation for Science and Technology (FCT).

1.11 BioData.pt | ELIXIR PT Services participate in a multitude of research projects in both national and international settings that are governed by project-specific policies and codes. Such policies may impose additional requirements on BioData.pt | ELIXIR PT Services that go beyond the scope of this policy.

1.12 The Data Protection Officer (DPO) of INESC-ID, the leader of the ELIXIR PT Consortium, is responsible for ensuring the processing of data in compliance with the applicable data protection rules (email for contact: dpo@inesc-id.pt).

1.13 The appointed responsible for each of the Biodata.pt | ELIXIR PT Node services is the appointed Data Controller (DC) for the service (check the Node Services page on the biodata.pt site to identify the person in charge of each service).

2. Scope

This Policy applies to BioData.pt | ELIXIR PT Services that make data underlying specific regulatory requirements available.

The Policy applies solely to BioData.pt | ELIXIR PT Services as defined by the BioData.pt | ELIXIR PT founding documents, i.e. Node-funded Services provided in the context of Node Collaboration Agreements and on the basis of Service Delivery Plans. It does not apply to any other services or research activities provided by the institute(s) constituting or affiliated with the BioData.pt | ELIXIR PT Node.

The vast majority of data made available for research via BioData.pt | ELIXIR PT Services is freely available and open for use by the scientific community. For data subject to regulatory requirements, this Policy provides the framework to ensure that provision of data through BioData.pt | ELIXIR PT Services is consistent with the relevant laws and regulations, good scientific practice and ethical principles as they are agreed within the research community.

The Policy does not cover the handling of data that are not processed within, or made available for research by, an BioData.pt | ELIXIR PT Service.

3. Legal Basis

As set forth in clause 7th, nr2, line f of the ELIXIR Portugal Consortium Contract, the Head of Node is responsible for the implementation, monitorization, control and compliance with the Ethics Policy of ELIXIR that is in line with relevant laws and regulations and that considers best practices.

This Policy is designed to be inter alia compliant with national laws and relevant international regulations:

- Universal Declaration of Human Rights, 10 December 1948
- Article 8 of the European Convention on Human Rights
- Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (convention 108)
- Charter of Fundamental Rights of the European Union 2010/C 83/0215
- Directive 95/46/EC of the European Parliament of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Nagoya Protocol on access to genetic resources and the fair and equitable sharing of benefits arising from their utilization to the convention on biological diversity, 29 October 2010
- European Convention for the Protection of Vertebrate Animals used for Experimental and Other Scientific Purposes, Strasbourg, 18 March 1986

4. Basic Ethical Principles

4.1 Human dignity and autonomy

The principle of human autonomy and self-determination is acknowledged by respecting the preferences of the Data Subject as expressed in their statement of Consent and by exercising diligence in the management of Personal Data in order to ensure the security of such data. Persons who are not in a position to make decisions freely and independently (people incapable of giving Consent) are covered by provisions of special protection.

4.2 Non-discrimination

Protection against discrimination requires equal treatment and respect for all persons whose data are used in research. The interests and needs of every person must be respected without bias regardless of its age, ethnicity, gender and/or race; every person must be protected from harm and treated with care impartially.
Stigmatisation of subsets of the population via certain data analyses is to be avoided even if it may be induced unintentionally.

4.3 Good scientific practice

Good scientific practice includes scientific honesty and diligence (professionalism, forthrightness, transparency) in the stewardship of data, samples, and research results. It is subverted by scientific dishonesty (deception, fraud, illegitimate use of knowledge from other sources).

4.4 Public benefit

Biomedical research serves the greater well-being of all humankind. Its benefit to society consists in achieving greater insight into the foundations of biology as well as in integrating its findings into clinical care. For the sake of realising societal benefit, it is necessary to ensure the broadest participation, which includes the general public, in sharing the benefits of scientific advancement.

5. Definition of terms

The definitions below shall be considered only for the purpose of this Policy. Some definitions from the General Data Protection Regulation have been adapted for the purpose of this Policy.

Anonymous (or Anonymised) Data is data that does not relate to an identified or identifiable natural person or to data that was personal data at the time it was collected but which, using best practices, has been rendered anonymous in such a manner that the data subject is no longer identifiable.

Consent means any freely given, specific, informed and unambiguous indication of their wishes by which the Data Subject, either by a statement or by a clear affirmative action (such as a signed document), signifies agreement to Personal Data relating to them being processed.

Data Access Committee (DAC) means a designated group of individuals who are made responsible for reviewing applications and granting permission for access to access-controlled datasets. Decisions to grant access are made based on whether the request conforms to the conditions under which data is made available by the Service.

Data Protection Officer (DPO) means a designated person within an organisation that audits Personal Data; he/she acts independently and is responsible for making sure that the organisation complies with data protection law.

Data Controller (DC) means the natural or legal person who has the legal and actual ability to determine the purposes and means of the Processing of Personal Data.

Data Provider means the individual researcher or investigator or body of researchers or investigators that makes data available or submits data for access and use in the context of an ELIXIR Service.

Data Subject refers to an identified or identifiable natural person (individual) whose data are accessed (e.g. patients, donors or study participants).

Data Transfer Agreement (DTA) means an agreement or contract made between a Data Provider and a Service Provider (i.e. when data is submitted to an BioData.pt | ELIXIR PT Service – “data in”) or a Service Provider and a Service user (i.e. when an BioData.pt | ELIXIR PT Service makes data available to researchers – “data out”) that governs the conditions under which the data is transferred and defines the rights of the contracting parties regarding future data usage. The DTA can take the form of general terms of service or terms of use.

Data User means the individual researcher or investigator or group of researchers or investigators that accesses and/or uses data made available as part of an BioData.pt | ELIXIR PT Service.

BioData.pt | ELIXIR PT Service(s) refers to BioData.pt | ELIXIR PT Services as defined in the Node Collaboration Agreements, i.e. Node-funded Services.
Ethics Review means a process, carried out by an Ethics Committee or other competent body, resulting in ethical approval for a study (or systematic data collection, e.g. biobank) which has collected data that will be subsequently made available by the Data Provider within an BioData.pt | ELIXIR PT Service.

Genetic Data means data relating to the genetic characteristics of an organism that have been inherited or acquired and which may provide unique information about the physiology or the health of that organism or individual.

Incidental Findings are findings concerning an individual discovered in the course of research using data offered in the context of an BioData.pt | ELIXIR PT Service that are beyond the original aims of the research.

Personal Data means any information relating to an identifiable natural person (Data Subject); an identifiable natural person is someone who can be identified with reasonable efforts, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Genetic Data may be considered non-Personal as long as it does not fulfill the criteria of Personal Data.

Processing means any operation that is performed with Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available (including use or making available for research purposes), alignment or combination, restriction, erasure or destruction.

Pseudonymised Data (also known as ‘coded’ or ‘linked’ data) is data that can only be connected to the Data Subject by using additional, separately kept information (a ‘key’) that would allow certain authorised individuals (e.g. the clinical team who collected the data) to link them back to the identifiable Data Subject.

Sensitive Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.
Service Provider refers to the Node providing an BioData.pt | ELIXIR PT Service.
Supervisory Authority means an independent public authority established in order to supervise and decide critical issues in a specific area.

6. Human Personal Data

General Requirements

6.1 Preferability of Processing anonymised data

Anonymous or Anonymised Data can be Processed without data protection constraints. Wherever possible with regard to the purpose of the BioData.pt | ELIXIR PT Service, data Processing shall only take place with Anonymous or Anonymised Data.
Whether Pseudonymised Data can be considered Anonymous Data for everybody who has no access to the key (linkage code, cipher), or who has no means to trace back the Data Subject via additional information (concept of relative anonymisation), is not unambiguously clarified on the EU level and depends on the relevant jurisdiction. An Ethics Review should be conducted and/or the Data Protection Officer or Supervisory Authority should be consulted in cases of doubt.

Anonymisation should be achieved using state of the art techniques that are used in practice. It is sufficient that the data is *de facto* anonymised, i.e. individuals cannot be re-identified by the use of reasonable means. When assessing re-identification risks all factors have to be considered, including for example context knowledge that is available to the data users, access control systems that ensure data is only used for biomedical research purposes in order to reduce available context knowledge, sensitivity of the data, etc.

6.2 Processing of Personal Data

Personal Data can only be processed if

- the Data Subject has given their Consent for the purpose of the Processing and according to 1.3, or

- the Processing is compliant with an applicable legal authorization,

and the use for biomedical research has been reviewed following an established Ethics Review process according to para. 1.9.

The Data Controller overseeing the provision of Personal Data in the context of an BioData.pt | ELIXIR PT Service has to ensure that the intended Processing is lawful (e.g. through a Data Access Committee). Where an BioData.pt | ELIXIR PT Service makes patient data or data from donors of biomaterial or Genetic Data available, prime consideration should be given as to whether the Data Provider has given sufficient evidence (e.g. in the context of a DTA) that the available Consent allows this.

Novel ways of combining data or datasets in the context of BioData.pt | ELIXIR PT can proceed as long as the data is Anonymised or Pseudonymised and approval has been granted following an Ethics Review, or by a Supervisory Authority or equivalent where required. Where there is doubt that Consent provisions adequately cover the combination of datasets, an Ethics Review should clarify or the opinion of a Supervisory Authority or equivalent should be sought as to whether additional participant Consent is required. This should normally happen within the context of the research project seeking to combine the datasets using the BioData.pt | ELIXIR PT infrastructure and attested through DTAs.

No further Consent will need to be sought where pre-collected Consent by the Data Subject adequately covers the provision of data in the context of the BioData.pt | ELIXIR PT Service.

Where adequate Consent has not been obtained, or where there is doubt, the Data Provider should seek approval via an Ethics Review and, where relevant legal (e.g. national) requirements dictate, from a relevant regulatory body or Supervisory Authority, before the data can be deposited. An example for this may be pre-collected data where Consent or approval was not broad enough to include the provision of the data in the context of an BioData.pt | ELIXIR PT Service. Re-Consent might not be necessary if approval is granted following an Ethics Review or by a relevant Supervisory Authority confirming that the benefit of providing the data in the context of BioData.pt | ELIXIR PT outweighs any risk to the Data Subject, and where local, regional or national or other relevant regulations allow this decision to be made by relevant Supervisory Authorities or via Ethics Reviews.

Even with Consent or a legal basis for Processing Personal Data, the principle of data minimisation has to be taken into account: Data should be de-identified if the research objectives can still be achieved with a de-identified data set.

6.3 Non-discrimination of vulnerable groups

Certain data analyses may confer non-intentional stigmatisation of subsets of the population involved. Consequently, any data analysis using BioData.pt | ELIXIR PT Services that may have the potential to cause stigmatisation must be carefully considered and discussed in the context of an Ethics Review in order to obtain further guidance prior to the analyses being undertaken. The responsibility to ensure appropriate Consent and approval based on an Ethics Review or from a national authority lies exclusively with the Data Provider and must be in place before data is made available in the context of BioData.pt | ELIXIR PT Services.

Requirements to be met by the Service Provider

6.4 Data Transfer Agreements (DTAs)

Any Transfer of Personal Data should be based on formal agreements such as DTAs. The Service Provider must conclude two types of DTAs: one with the Data Provider

before data is submitted to the BioData.pt | ELIXIR PT Service and one with the Data User before data is made available for research. These DTAs can be implemented as Terms of Use or Terms of Service.

At the point of data submission ("data in") and where applicable, any such agreement must reflect that the Data Provider is submitting the data to the Service only after having secured the necessary Informed Consent by the Data Subject and/or taking into account any other limitations, such as for example deriving from ethics reviews or relevant law, or the requirement to feedback Incidental Findings. It is advisable that the DTA also include a provision for the Data Provider to inform the Service Provider should the need to remove Personal Data arise for example when Consent is withdrawn.

At the point of data use ("data out"), in the case of data requiring Consent by the Data Subject, it is advisable that the DTA between the Service Provider and the Data User exclude any further data transfer from the side of the Data User or, where such transfer is intended, include a requirement for the Data User to document any such data transfer in case Consent for Personal Data is withdrawn in order to be able to comply commensurately with a revocation of Consent. The Service Provider might also consider referring to the BioData.pt | ELIXIR PT ELSI Policy in this DTA.

For the avoidance of doubt, the responsibility for meeting any applicable requirements around Consent, Ethics Reviews and Incidental Findings remains with the Data Provider.

6.5 Physical Security

Adequate measures based on current and continuously updated best practice, which may include formal certification, should be implemented to guarantee the physical security of data during the Processing within the context of an ELIXIR Service.

6.6 Controlled Access to Data

Controlled access to Personal Data should be implemented unless the available consent or other considerations allow fully unrestricted open access.

The Service Provider is responsible for ensuring levels of data security appropriate for the type of data held.

The access procedure should be transparent to ensure fair access. The principles governing the use of data after access has been granted should be outlined in a DTA (see para 4).

Controlled access to data is provided on the basis of an appropriate data security plan that is based on current and continuously updated best practice and which may include formal certification.

Additional restrictions may be imposed by the ELIXIR Service home organisation's IT requirements and policies, e.g. regarding server, network, and application security.

6.7 Third Party-Managed IT resources

Increasingly, IT services are moving from local servers and hardware managed by the organisation's own staff to systems owned and managed by third party providers. Transfer and storage of controlled access data on third party systems require additional considerations.

Thus, it is advisable that institutions validate that they are partnering with a reputable third party provider and develop appropriate security plans and service agreements before data is migrated to third party providers. Migration of person-related data to servers located in other countries also require consideration of relevant data protection regulation (e.g. in the case of non-EU cloud services, it should be ensured that it is legally allowed, for example because the foreign country has been declared a “safe” country by the EU Commission or the Consent of the Data Subject explicitly allows the transfer).

Requirements to be met by the Data Provider

6.8 Informed Consent

a) Requirements

Drafting Consent forms and obtaining and managing Consent for data collections is entirely the responsibility of the researcher collecting the data deposited in BioData.pt | ELIXIR PT Services (who may or may not be the same as the Data Provider). The responsibility to ensure that appropriate Consent and/or Ethics Committee or other Supervisory Authority approval is in place before data is deposited and/or made available in the context of the BioData.pt | ELIXIR PT Service lies exclusively with the Data Provider. The Data Provider remains responsible for managing the Consent.

Consent must be documented. It is advisable that the Service Provider ensures that the Data Provider’s responsibility for obtaining Consent is clearly stated in the DTA between the Data Provider and the Service Provider.

Consent forms should be drafted to adequately cover the use in the context of an BioData.pt | ELIXIR PT Service concerning:

- access to and linkage of data that is stored in an electronic database
- sharing of data with other researchers within and outside of the country
- any decisions made regarding the management and communication of findings of individual clinical significance (Incidental Findings), including any obligations data consumers may have to communicate findings, and any pre-set time-limits for the feeding back of results
- the possibility of the data being used in a commercial context.

b) Withdrawal of Consent

Personal Data are to be destroyed upon withdrawal of Consent except in cases where the relevant law allows or requires data retention. The Data Provider is responsible for

informing the Service Provider should any such need arise, and it is advisable that this responsibility is clearly stated in the DTA between the Data Provider and the Service Provider.

6.9 Ethics Review and regulatory approvals

The Data Provider must ensure that an Ethics Review as required by all relevant law and internationally agreed standards has been completed. An Ethics Review is always required where the Consent form indicates that Consent has been given on the condition that such review is conducted before data is processed (i.e. used for a given research project). The ethics review must cover the secondary use of data e.g. through submission and managed access through an BioData.pt | ELIXIR PT Service.

In cases where the DAC considers an Ethics Review necessary but where this is not already available, it can build an ad hoc ethics committee or equivalent body to conduct the appropriate review.

Data protection authority approval must be obtained if required by relevant law.

6.10 Incidental Findings

Where there is a requirement to return Incidental Findings to Data Subjects, the responsibility to ensure that appropriate Consent and mechanisms of feedback, which must have been Consented to by the Data Subject and agreed in an Ethics Review or by a Supervisory Authority, lies exclusively with the Data Provider and must be in place before data is deposited and/or made available in the context of ELIXIR Services. Requirements to be met by the Data User

Besides meeting the requirements as laid out in the DTA between the Service Provider and Data User (which can take the form of Terms of Use or Terms of Service), the Data User must adhere to the Basic Principles described in this policy concerning Human Dignity and Authority, Non-Discrimination, Good Scientific Practice and Public Benefit.

7. Non-Human Data including Animal Data

7.1 Rules

Where animal data is made available for research via an BioData.pt | ELIXIR PT Service, the Data Provider must ensure that relevant guidelines and laws for the animals' welfare and care during collection of the data are followed.

Where non-human genome data is made available, use and provision in the context of an BioData.pt | ELIXIR PT Service must be compliant with the relevant national implementation of the Nagoya Protocol.

As described under section F. Human Personal Data (para 4), these rules can be implemented in a Data Transfer Agreement, for example as Terms of Use or Terms of Service, taking the different perspectives described above (Data Provider, Service Provider, Data User) into account.

8. Approval, implementation, monitoring and development of this Policy

8.1 Approval

The responsibility for the approval of this Policy lies with the BioData.pt | ELIXIR PT Board.

The BioData.pt | ELIXIR PT Head of Node is responsible for ensuring that the Policy is routinely reviewed by the BioData.pt | ELIXIR PT Scientific Advisory Board in order to improve it and to keep it continuously up-to-date with new advances in basic research and bioinformatics as well as developments concerning ethical and legal requirements.

Feedback from the Heads of BioData.pt | ELIXIR PT Consortium Members and key expert groups or persons will also be sought regularly.

8.2 Implementation and compliance

As per Art. 10.1.2g of the Node Collaboration Agreements, the BioData.pt | ELIXIR PT Head of Node is responsible for ensuring compliance with this Policy for the BioData.pt | ELIXIR PT Services offered by the Node to ELIXIR. In turn, Coordinators of BioData.pt | ELIXIR PT Nodes are responsible for ensuring compliance with this Policy for the BioData.pt | ELIXIR PT Services offered by the respective Node.

Each BioData.pt | ELIXIR PT Node is responsible to implement its own policies in order to ensure that the Services provided within BioData.pt | ELIXIR PT comply with the BioData.pt | ELIXIR PT ELSI Policy and national rules and regulations as well as international standards of best practice.

8.3 Information

The Head of Node of BioData.pt | ELIXIR PT shall remind the ELIXIR Node of its obligation to ensure compliance of all relevant laws and regulations (and, where applicable, local ethical guidelines) when handling, storing, or processing personally identifiable data resulting from biomedical research.

8.4 Monitoring

The Collaboration Oversight Group, which is established by the Parties to the Node Collaboration Agreement and comprises the Head of Node, the Node Coordinator and other individuals appointed by them, shall monitor the compliance of BioData.pt | ELIXIR PT Services provided by the Node in question*.

In collaboration with the BioData.pt | ELIXIR PT Scientific Advisory Board and supported by the Node in question, data concerning BioData.pt | ELIXIR PT Service compliance with this Policy will be gathered by the Board of Directors and submitted to the BioData.pt | ELIXIR PT Scientific Advisory Board in the context of regular BioData.pt | ELIXIR PT Service reviews.

Upon recommendation of the BioData.pt | ELIXIR PT Scientific Advisory Board (including Ethics Experts), the BioData.pt | ELIXIR PT Board shall decide whether it wishes to renew or terminate (in whole or in part) the Agreement with the BioData.pt | ELIXIR PT Node.

This Policy has been adopted by the BioData.pt | ELIXIR PT Executive Board on the 19th of June 2020.

* It should be noted that the Collaboration Oversight Group works as a flexible structure to facilitate communication, but the rights and obligations of the BioData.pt | ELIXIR PT Director and the Head of Node remain unaffected.

BioData.pt elixir PORTUGAL
Co-financiado por:
CRESC ALGARVE 2020 Lisb@20[20] PORTUGAL 2020 UNIÃO EUROPEIA Fundos Europeus Estruturais e de Investimento

Annex 1

Sensitive Data Typologies

BioData.pt | ELIXIR PT repositories hold the following types of sensitive data:

1. Clinical and Health Data
2. Genomics Data