EXCELERATE Deliverable 12.1

Project Title:	ELIXIR-EXCELERATE: Fast-track ELIXIR implementation and drive early user exploitation across the life sciences	
Project Acronym:	ELIXIR-EXCELERATE	
Grant agreement no.:	676559	
	H2020-INFRADEV-2014-2015/H2020-INFRADEV-1-2015-1	
Deliverable title:	ELIXIR Ethics Policy	
WP No.	12	
Lead Beneficiary:	EMBL (ELIXIR Hub)	
WP Title	Excellence in ELIXIR Management and Operations	
Contractual delivery date:	31 August 2016	
Actual delivery date:	31 August 2016	
WP leader:	Niklas Blomberg	1: EMBL
Partner(s) contributing to this deliverable:	n/a	

Authors and contributors: Niklas Blomberg, Stephanie Suhr, ELIXIR SAB and partners

Table of contents

1. Executive Summary

The purpose of many ELIXIR Services is to facilitate the open sharing of research data. While data and knowledge provided by ELIXIR Services will be accessible to researchers, 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. Especially for ELIXIR Services managing data from human research participants that 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. The ELIXIR Ethics Policy provides evidence that an adequate level of protection of personal data including sensitive data is in place throughout ELIXIR - including across national borders - which increases the acceptance of clauses in consent forms concerning data deposition with ELIXIR Services.

ELIXIR Services are formally defined and must meet specific criteria based on the ELIXIR founding documents. Every ELIXIR Service involving personal 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. At the same time, ELIXIR is a distributed infrastructure and its Nodes are independent organisations. The Node providing an ELIXIR Service is responsible for the implementation of the requirements of the ELIXIR Ethics Policy. Consequently, the Policy does not prescribe how the specific requirements are met; this is up to the Node.

The Ethics Policy, which is a specific requirement of the ELIXIR founding documents, consolidates requirements that are shared across all ELIXIR Members and Services. It imposes no additional constraints on the use of data contributed to ELIXIR Services than those provided by the Data Controller/Provider or existing legal and ethical requirements.

ELIXIR Services do not assume the ownership of the data they hold, but provide a platform where data controllers/data providers can share their data with the community. One of the major achievements made during the development of the ELIXIR Ethics Policy is the clear definition of responsibilities with respect to the provision of data underlying regulatory requirements into those to be met by the individual researcher or investigator or body of researchers or investigators that submits data for access and use in the context of an ELIXIR Service (the “data provider”), the ELIXIR Service, and the individual researcher or investigator or group of researchers or investigators that accesses and/or uses data made available as part of an ELIXIR Service (the “data user”).

The ELIXIR Ethics Policy is accompanied by a document providing background and context for the requirements of the policy (Annex 2). The background document will be updated continually and expanded to include more in-depth explanations of the requirements included in the policy, where they originate, how they can be implemented, and a clarification of how the policy relates to guidance provided by other relevant initiatives (such as the GA4GH, among others).

To facilitate and support implementation in the ELIXIR Nodes, once it has been approved by the ELIXIR Board as required by the ELIXIR founding documents, the policy will be accompanied by the following supporting materials:

- **operational procedures** addressing specific issues in more detail and providing recommendations on the implementation of the Policy, which will be developed together with Node technical personnel based on specific needs and to address relevant use cases (e.g. local EGA instances) and which will address the capacity

building requirements of the ELIXIR Consortium Agreement concerning the ethics policy
- a draft, lightweight, **compliance check procedure** that will tie into procedures already under development (Service Delivery Plans, Node reviews, etc.)

Both activities will be covered by EXCELERATE Subtask 12.2.4: Establish ELIXIR's internal processes for ELSI, for which a milestone is due in project month 24 (August 2017).

2. Project objectives

This deliverable fulfils one of the Ethics requirements of EXCELERATE.

With this deliverable, the project has reached or the deliverable has contributed to the following objectives:

No.	Objective	Yes	No
1	Coordinate ELIXIR-EXCELERATE project management with risk assessment and quality control to ensure successful and on-time completion of the project deliverables		x
2	Conclude the implementation of ELIXIR coordination and operational structure and collect defined procedures into ELIXIR Handbook of Operations to be available online for all partners	x	
3	Review the suitability of ELIXIR's legal framework, as recommended by ESFRI, and provide conclusions and options to the ELIXIR Board		x
4	Analyse emerging technical data and experiences gained from Nodes to update the long-term strategy for the sustainability of data management, which will advise future funding strategy and the ELIXIR Programme		x

3. Delivery and schedule

The delivery is delayed: ☐Yes ☑ No

4. Adjustments made

No adjustments were made.

5. Background information

Background information on this WP as originally indicated in the description of action (DoA) is included here for reference.

Work package number	12	Start date or starting event:	month 1
Work package title	**Excellence in ELIXIR Management and Operations**		

Lead	Niklas Blomberg (ELIXIR Director)

Participant number and person months per participant

1 – EMBL (120 PM), 6 - NBIC (3.6 PM), 43 - UEDIN (2.4 PM)

Objectives

- Coordinate ELIXIR-EXCELERATE project management with risk assessment and quality control to ensure successful and on-time completion of the project deliverables. (Task 12.1)
- Conclude the implementation of ELIXIR coordination and operational structure and collect defined procedures into ELIXIR Handbook of Operations to be available online for all partners. (Task 12.2)
- Review the suitability of ELIXIR's legal framework, as recommended by ESFRI, and provide conclusions and options to the ELIXIR Board. (Task 12.3)
- Analyse emerging technical data and experiences gained from Nodes to update the long-term strategy for the sustainability of data management, which will advise future funding strategy and the ELIXIR Programme. (Task 12.4)

Description of work and role of partners

The purpose of this Work Package is to:

- Run the overall project management function ELIXIR-EXCELERATE; and
- Deliver value to Member States by completing the ELIXIR Management and Operational processes so that ELIXIR Hub and Nodes - operates as a world-class distributed infrastructure to its users.

The WP addresses quality management, risk management, and service sustainability and aims to ensure the delivery of long-term, mission-critical services of high quality. It also includes activities that ensure ELIXIR takes part in future EU grants as a single entity. It delivers the activities that directly addresses the ESFRI recommendations for ELIXIR: 1) strengthen the central coordination role of the ELIXIR Hub, 2) evaluate the appropriateness of the ELIXIR legal framework, 3) enhance ELIXIR operational processes to support the full deployment of the service streams, 4) develop data access and ELSI procedures, and 5) develop common procurement and recruitment procedures. The two remaining recommendations on industry engagement and expansion of ELIXIR's membership are addressed in WP13. This WP further addresses the long-term bottleneck in implementation identified in the Assessment Expert Group review: sustainable funding models for critical, core, data resources that bring together national and international stakeholders.

Task 12.1: Coordinate ELIXIR-EXCELERATE project management (78PM) (M1-M48)

Subtask 12.1.1: Day-to-day management, reporting, quality control and risk management (40PM)

The ELIXIR Hub will lead the project management and coordination of ELIXIR-EXCELERATE. This will, as far as possible, make use of established ELIXIR structures and will be complemented by additional resources (where relevant) to ensure appropriate project management practice and completion of all reporting requirements. Time in regular ELIXIR advisory body meetings will be dedicated to discuss ELIXIR-EXCELERATE; however, due to the size and complexity of the implementation project, additional meetings for Heads of Nodes and other permanent ELIXIR working groups will

be required. This task covers all the necessary Project Management, KPI tracking, reporting and risk management activities necessary for a large, distributed project and embeds these activities in the ELIXIR Hub project management unit. Further, in this task the quality control procedures on milestones, deliverables and other project results will be established (e.g. internal peer review, HoN review and acceptance for milestones). This will ensure that deliverables adhere to some quality principles (such as completeness, relevance, uniformity in presentation, etc.), which is important both for internal and external communication and reporting to the EC. In order to bring together ELIXIR's users and operators, an international conference: "Landmark in Bioinformatics Services" will be organised during the second year of the project. This meeting includes breakout sessions and hackathons for ELIXIR users, in addition to keynote talks by external experts. The meeting invitation will be extended to related infrastructures with the expectation that participants pay for the meeting registration and for their own travel.

Subtask 12.1.2: Develop and maintain a high-class intranet for project partners, committees and governance bodies (38 PM)

Information flow within the project is ensured through an intranet that will be developed and maintained by the ELIXIR Hub. This is a critical task for a large, distributed project with multiple partners. It will help the ELIXIR Hub to manage documents, assign tasks, report project outcomes, follow up KPIs, manage risks and find people involved in ELIXIR. The intranet will be aligned to the ELIXIR website so information can easily flow from the private area to the public area. The ELIXIR Hub will also develop and maintain system for exposing ELIXIR events, news, vacancies and shared information across the ELIXIR Hub and Nodes website. The ELIXIR Hub will adapt the emerging iAnn standard to federate this content and provide a solution to facilitate exchange of announcements like news and events across ELIXIR Nodes, ELIXIR participants' institutions as well as other relevant organisations in the life sciences domain. Partners: EMBL-ELIXIR

Task 12.2: Conclude the implementation of ELIXIR coordination and operational structure (28PM) (M1- M48)

Subtask 12.2.1: Develop ELIXIR operations framework and processes (23PM)

In order to ensure pan-ELIXIR coherency in the delivery of high quality and mission-critical services, ELIXIR has established permanent working groups on technical and training services: Technical Coordinators Group (TCG) and Training Coordinator Group (TrCG) were formed in 2014. In 2015, upon recruitment of ELIXIR's Data Coordinator, a Data Coordinator Group (DCG) will be established. The coordinator groups constituted by Node Technical, Training and Data coordinators and led by the respective ELIXIR coordinator, coordinate service objectives and action lines within ELIXIR. In this project they have a key role to bring coherence across the Work Packages, in particular the four Use Cases (WP6 to 9) and ensure that solutions are made available nationally and to other communities. They are also responsible for maintaining a long-term view of their respective area. The aim of this task is to drive the technical, data and people coordination within ELIXIR by strengthening the ELIXIR permanent working groups (DCG, TCG, TrCG). To strengthen the harmonisation of processes across the whole infrastructure (the ELIXIR Hub and the Nodes, as well as external interactions), ELIXIR procedures, recommendations and guidelines will be collected into a living document: the ELIXIR Handbook of Operations. This will be made available through the ELIXIR intranet. The handbook will encompass all ELIXIR operations, e.g. the ELSI guidelines, communication plan, international strategy, diversity and equal opportunities, common procurement and recruitment procedures, and will also link to the Handbook for Nodes (delivered by WP10). The handbook is updated annually and final version released at the end of this project. According to the ELIXIR governance, any infrastructure-wide policies

will need to be decided by the ELIXIR Board and therefore, the Handbook of Operations will feed into the development of the next ELIXIR Scientific Programme for 2019-2023, which the Board will approve in the spring 2018. Progress on the Handbook development will be regularly reported to the ELIXIR Board.

Subtask 12.2.2: Develop the ELIXIR equal opportunities policy (1PM)

Gender balance and equal opportunities have already been considered within ELIXIR when setting up the ELIXIR governance structure with requirements on e.g. advisory boards. In addition, each ELIXIR Node has their own employment policies in place. However, there is not yet a developed ELIXIR-wide equal opportunities policy. Within this project, the equal opportunity recommendations in access to training and services will be reviewed throughout ELIXIR, along with developing the Charter and Code of Access to research infrastructures. This task will draw on the diversity work across BMS research infrastructures planned within the CORBEL cluster project. In addition, collaborations with the emerging NIH BD2K Biomedical Data Science Training Coordination Centre will be sought, not only on bioinformatics training and shared infrastructure but also on gender/diversity issues. Based on these a good practise recommendation for ELIXIR on diversity issues will be completed to be included into the ELIXIR Handbook of Operations.

Subtask 12.2.3: Investigate and recommend options for common procurement across Nodes (2PM)

ESFRI recommends ELIXIR to develop common procurement and recruitment procedures. To gain understanding in the processes, we will investigate how commercial partners work with data intensive partners in the life science. A feasibility analysis will assess options on compute and storage services with ELIXIR datasets and explore joint procurement for commercial cloud services, e.g. AWS, Google Cloud, and Azure. This analysis will include access for SMEs and will be performed together with WP4 and partners from the EMBL-EBI, Finnish and Czech Nodes, who are experts in technical services. The ELIXIR Hub will implement the strategy and include it into the ELIXIR Handbook of Operations.

Subtask 12.2.4: Establish ELIXIR's internal processes for ELSI (1PM)

Within Europe, BBMRI-ERIC has already established Common Service ELSI (http://bbmri-eric.eu/common- services). Although their work is focussing on the biobanking community, the Common Service ELSI provides a very useful framework for ELIXIR. We are currently developing a Memorandum of Understanding with BBMRI-ERIC with the intent of establishing a long-term relationship for ELSI Services that maximise infrastructure synergies. The aim of this task is to establish ELIXIR's internal processes for ELSI by bringing together the planned work within CORBEL (see section 1.3.2) and ELIXIR Nodes' national ELSI processes and ensure that ELIXIR's roles, policies and responsibilities are clear and transparent – the foundation for effective partnership. Once established, the ELSI processes will be included into the ELIXIR Handbook of Operations.

Subtask 12.2.5: Review ELIXIR Node Collaboration Agreements to streamline participation on grants (1PM)

There is a clear need to review and assess the suitability of ELIXIR Nodes' legal structures in the context of EU grant applications, where the intention is for ELIXIR to participate in future grants with as fewer numbers of separate beneficiaries as possible. ELIXIR-EXCELERATE shows that ELIXIR Nodes - and their various legal forms - are very heterogeneous and in many cases don't yet allow for participation by a single entity. Options such as Joint Research Units and Linked Third Parties will be encouraged.

Partners: EMBL-ELIXIR, NL, UK

Task 12.3: Assess the suitability of ELIXIR's legal framework (14PM) (M18- M36)

The legal framework of ELIXIR is based on the ELIXIR Consortium Agreement (ECA), which has been concluded among the Member States and EMBL and officially entered into force on 12 January 2014. The ECA covers ELIXIR's mission, membership, obligations of the Members and the ELIXIR Hub, the governance structure of the ELIXIR Hub and relationship to the ELIXIR Nodes. Based on the ECA, EMBL carries out activities on behalf of and as mandated by the ELIXIR Consortium that require EMBL's legal personality. ESFRI recommends that under the ELIXIREXCELERATE project, ELIXIR would "consider the long term sufficiency of the present legal framework as EMBL special project". Therefore, this task will: 1) Arrange a workshop with ELIXIR members to agree on a scope of the legal framework review and develop a request for tender document, 2) tender for an external expert to review and compare different legal frameworks, and 3) arrange a workshop to conclude recommendations for ELIXIR's future legal framework based on the consultant review. This task will require the ELIXIR Board administrative delegates and legal experts from ELIXIR Member States. As the Board members are not from partner institutes, their travel costs are budgeted within this task. The tender evaluation committee will be appointed by the ELIXIR Board.

Partners: EMBL-ELIXIR Additional resources required: Procurement (external consultant) €60,000

Task 12.4: Ensuring long-term strategy for the sustainability of data management (6PM) (M1-M36)

The long-term sustainability of Europe's public data resources is of paramount importance. Indeed, ELIXIR is recognized as Europe's attempt to coordinate, integrate and facilitate the long-term sustainability of these critical resources. The aim of this task is to evaluate the relevance of the previous work in this area and present an updated, forward-looking strategy to feed into the long-term funding strategy and ELIXIR Programme for 2019-2023. This task is a direct response to the recommendations of both ESFRI and the Assessment Expert Group, and will bring together senior policy makers, technical experts and resource owners from ELIXIR Nodes. This task will build on other activities within ELIXIR-EXCELERATE. A permanent working group, already created within ELIXIR, will work within ELIXIR-EXCELERATE and monitor the emerging technical data from WP3 (development of metrics around core resources) and WP5 (interoperability requirements) and the experiences from WP10 (increased capability from Nodes). The WG will consolidate the collected data into a high-level strategy that informs the Programme. In addition, institutional good practises will be defined and rolled out via the Node Handbook (WP10). The WG members are ELIXIR Board administrative delegates and scientific experts from ELIXIR Member States. As the WG members are not from partner institutes, their travel costs are budgeted within this task.

Partners: EMBL-ELIXIR

Annex 1: ELIXIR Ethics Policy

Annex 2: Background to the ELIXIR Ethics Policy

Background to the ELIXIR Ethics Policy

Table of contents

1. Introduction

This document accompanies the ELIXIR Ethics Policy, which is required according to Article 11 of the ELIXIR Consortium Agreement. The Policy has been developed in consultation with or feedback and input from Node technical personnel, Heads of Nodes, Ethics Experts on the ELIXIR Scientific Advisory Board, technical staff and external experts.

The purpose of this document is to support the development, interpretation and application of the ELIXIR Ethics Policy by providing background and context. This document does not set out any binding requirements over and above the ELIXIR Ethics Policy, which remains the authoritative source for resolving any potential issues.

In order to facilitate its interpretation and application, and to avoid possible confusion, the Policy is divided into two sections: one concerning human personal data and one concerning non-human and animal data.

To facilitate and support implementation in the ELIXIR Nodes, once adopted the policy will be accompanied by the following:

- **Operational procedures** addressing specific issues in more detail and providing recommendations on the implementation of the Policy, which will be developed together with Node technical personnel based on specific needs and to address relevant use cases (e.g. local EGA instances) and which will address the capacity building requirements of the ELIXIR Consortium Agreement concerning the ethics policy
- A **compliance check procedure** that will tie into procedures already under development (Service Delivery Plans, Node reviews, etc.)

In addition, this background document will be updated continually and expanded to include more in-depth explanations of the requirements included in the policy, where they originate,

how they can be implemented, and a clarification of how the policy relates to guidance provided by other relevant initiatives (such as the GA4GH, among others).

2. Why the policy?

ELIXIR founding documents stipulate the need for an ELIXIR Ethics policy (see also Figure 1):

ELIXIR Consortium Agreement

Article 11

The ELIXIR Board shall

[…] establish an ethics policy that is in line with relevant laws and regulations and that considers best practices.

[…] put in place measures to ensure that activities […] shall be in line with this ethics policy.

[…] implement mechanisms to ensure that ELIXIR Nodes as well as all other collaboration partners […] are made aware of their 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.

Node Collaboration Agreements

10.1.2 'Role and tasks of the Head of Node'

[...] The tasks of the Head of Node include, but are not limited to the following:

a. Ensure the compliance of the Node [and all involved national research institutes] with the ELIXIR Ethics Policy, national regulations and international best practices; [...]

e. Provide evidence to the Ethics Advisory Committee in carrying out a review of the ethical measures in place at the ELIXIR Node

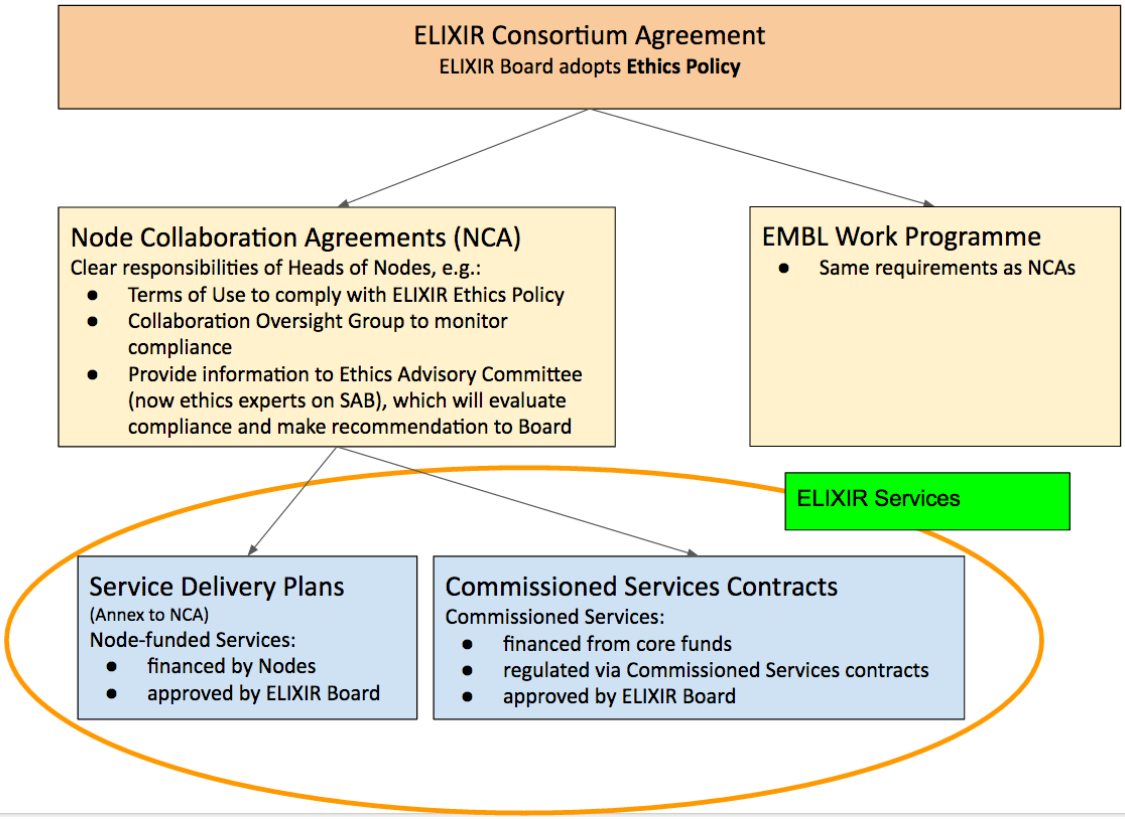

Figure 1 Basis for the Ethics policy as per the ELIXIR legal framework

3.

4. Who are the stakeholders?

Aspects covered by this policy will be relevant to/required by a large variety of stakeholders.
External stakeholders include:

- ethics committees and ethics advisory boards (e.g. of large projects)
- funders, e.g. European Commission (--> see EXCELERATE ethics review)
- data providers (researchers that want to submit data to ELIXIR Services)
- data users (researchers that want to use data offered in the context of ELIXIR Services)
- patients/patient groups

ELIXIR-internal stakeholders are:

- ELIXIR Members/the Board (ELIXIR Consortium Agreement)
- Nodes: Heads of Nodes, technical staff
- ELIXIR SAB/Ethics experts

5. What does the policy do?

The ELIXIR ethics policy provides guidance to ELIXIR Nodes/institutes forming the ELIXIR Nodes that provide personally identifiable or Sensitive Data within the distributed ELIXIR infrastructure.

The policy:

- identifies the potential risks concerning legal/ethical aspects of sharing research personal data and in particular sensitive data
- provides first guidance and high level principles concerning how these risks can be addressed (this can, and normally will, be refined by internal Node policies that build on ELIXIR "best practices")
- describes the roles and responsibilities concerning implementation of ELSI within ELIXIR

6. What does the policy not do?

ELIXIR is a distributed infrastructure with organisationally independent Nodes. The ELIXIR Services are delivered by institutes associated with the Nodes in ELIXIR's Member countries, and the legal basis for ELIXIR requires that each Service has its own functioning ethics and regulatory oversight in place. In addition, the complexity and diversity of regulations around data underlying regulatory requirements - which can vary significantly between countries or even individual states within countries, and/or organisations - demands that the necessary knowledge and expertise concerning these requirements sits locally with the Service provider.

Consequently, *the policy does not*:

- dictate the processes at individual institutes that make up an ELIXIR Node
- replace or supercede local policy and compliance requirements and procedures at the ELIXIR Nodes and Node institutes
- impose additional compliance monitoring processes that interfere with existing measures, either at the operational level or in the context of relevant ELIXIR procedures (Service Delivery Plans, Node review)
- impose additional requirements that go beyond existing legal requirements and ethics principles
- require Non-EU member states to adopt EU legislation or directives

7. What does the policy cover?

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

The specific requirements of the policy apply only to data underlying legal/regulatory requirements. It is the Node's responsibility to ascertain that the ELIXIR Services they provide have mechanisms in place that make data submitters and data controllers aware of any relevant ethical and legal requirements, in particular requirements for sensitive data.

It should be noted that the legal and ethical requirements regarding use and storage of sensitive data stem from the applicable laws and regulations and not from the ELIXIR founding documents or the ELIXIR Ethics Policy. The role of the Policy is to clarify and describe how and by whom the existing legal and ethical requirements are met in the context of ELIXIR, and to make this visible to external stakeholders such as funders where required (e.g. in the context of grant funding).

8. What are the critical ELSI issues addressed in the policy?

Anonymisation of genetic data. Genetic data can be clearly non-personal data (not rich enough to single out an individual), or there can be uncertainty regarding the status of anonymity. The distinction between the two cases and the evaluating of the status of anonymity of genetic data will be addressed in a best practice document to be developed.

Definition of terms. The policy provides definitions of terms that will be used in the context of ELSI and data sharing within ELIXIR (e.g. anonymisation, linked data, data controller) to provide clarity and a basis for detailed policies.

Informed consent. Even broad consent may not be “broad enough” (see Rec. 25aa GDPR). Limited consent must be managed.

Ethics Review. The ethics committee landscape is very fragmented in Europe, and there is no clear rule concerning where ethics committee reviews are needed. Consequently, it is necessary that a competent DAC decides on data use of sensitive data according to local law and or applicable ELIXIR best practice.

9. What does the policy leave open?

In some cases it may be unclear whether data held by a specific Service is sensitive. Such “legacy data” may be data that was submitted to the Service longer ago and for which a DTA was not concluded as it did not qualify as sensitive data at the time of submission (e.g. due to lack of legislation or procedures around informed consent at the time the data was generated). There is currently no legal solution to this challenge, so the Policy does not address this.

A possible solution for the Service provider may be to require the user to make a statement (e.g. by acknowledging Terms of Use) such as "I understand that this data entered the ELIXIR Service without a DTA. I certify that I have duly executed a DTA to obtain this data, and will use it consistent with the regulations of my funder, home institution, and current scientific best practices." However, any possible approach should always be discussed with ethical and legal experts familiar with the specific requirements to be met by the Service.

10. Who is responsible for what?

The Policy must be implemented solely to ELIXIR Services as defined by the ELIXIR founding documents, i.e. Node-funded Services provided in the context of Node Collaboration Agreements and on the basis of Service Delivery Plans, and Commissioned Services provided on the basis of Commissioned Services contracts. It does not apply to any

other services or research activities provided by the institute constituting or affiliated with the ELIXIR Node.

The policy clearly defines the following roles in the context of data provision via ELIXIR Services:

Data Provider	means the individual researcher or investigator or body of researchers or investigators that submits data for access and use in the context of an ELIXIR Service
Service Provider	refers to the Node providing an ELIXIR Service
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 ELIXIR Service

Each of these has different, clearly defined responsibilities:

General rules (apply to data provider, service provider and data user):

- Preferability of Processing anonymised Data
- Processing of Personal Data
- Non-discrimination of vulnerable groups

Rules to be met by the **Service Provider**:

- Data Transfer Agreements
- Physical Security
- Controlled Access Data
- Third-Party-Managed IT Resources

Rules to be met by the **Data Provider**:

- Informed Consent
- Ethics vote and regulatory approvals
- Incidental Findings

Requirements to be met by the **Data User**:

- Adhere to basic ethical principles and conditions of any relevant DTA(s)

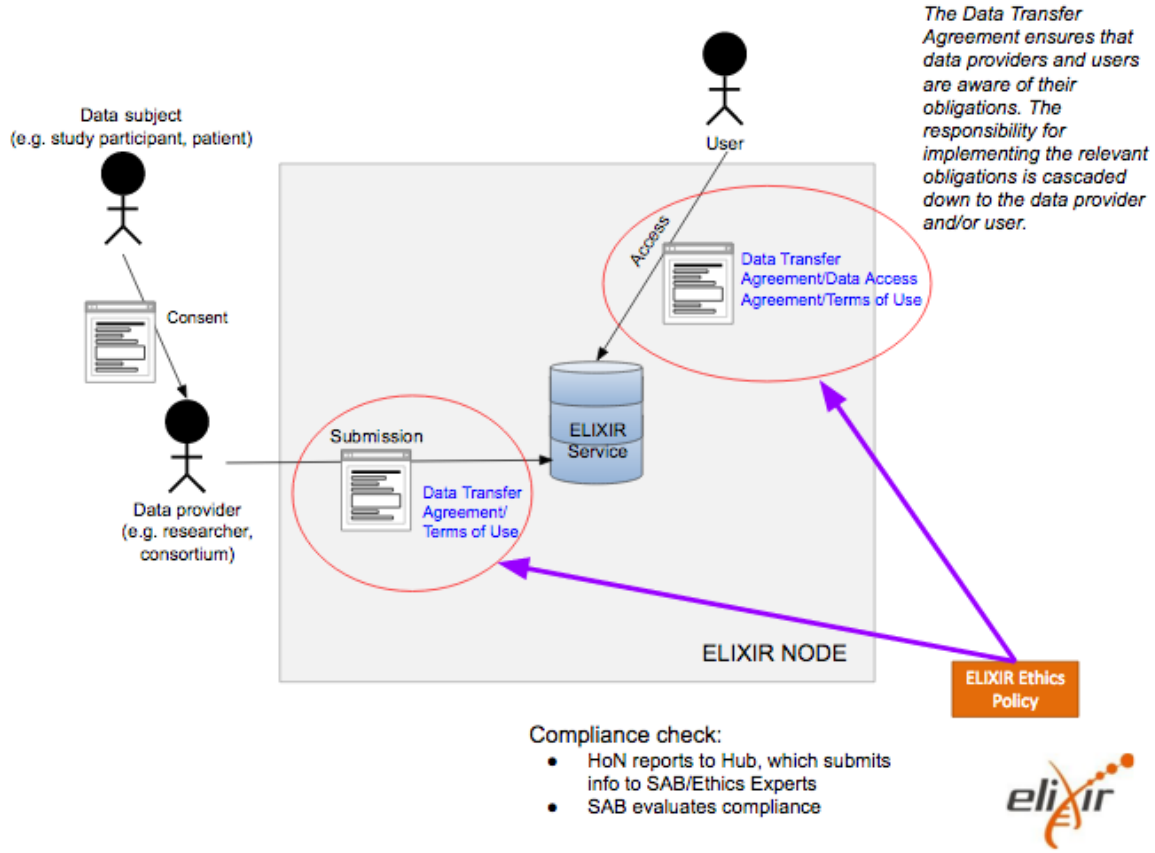

Figure 2 An ELIXIR Service (e.g. an archive) providing data for research. When implemented the Ethics policy only influences the DTAs (e.g. as "Terms of Use" or "Terms of Service) at the "data in" (submission) and "data out" (use) ends; the Node retains full responsibility for having a suitable ELSI framework in place for the ELIXIR Service in question

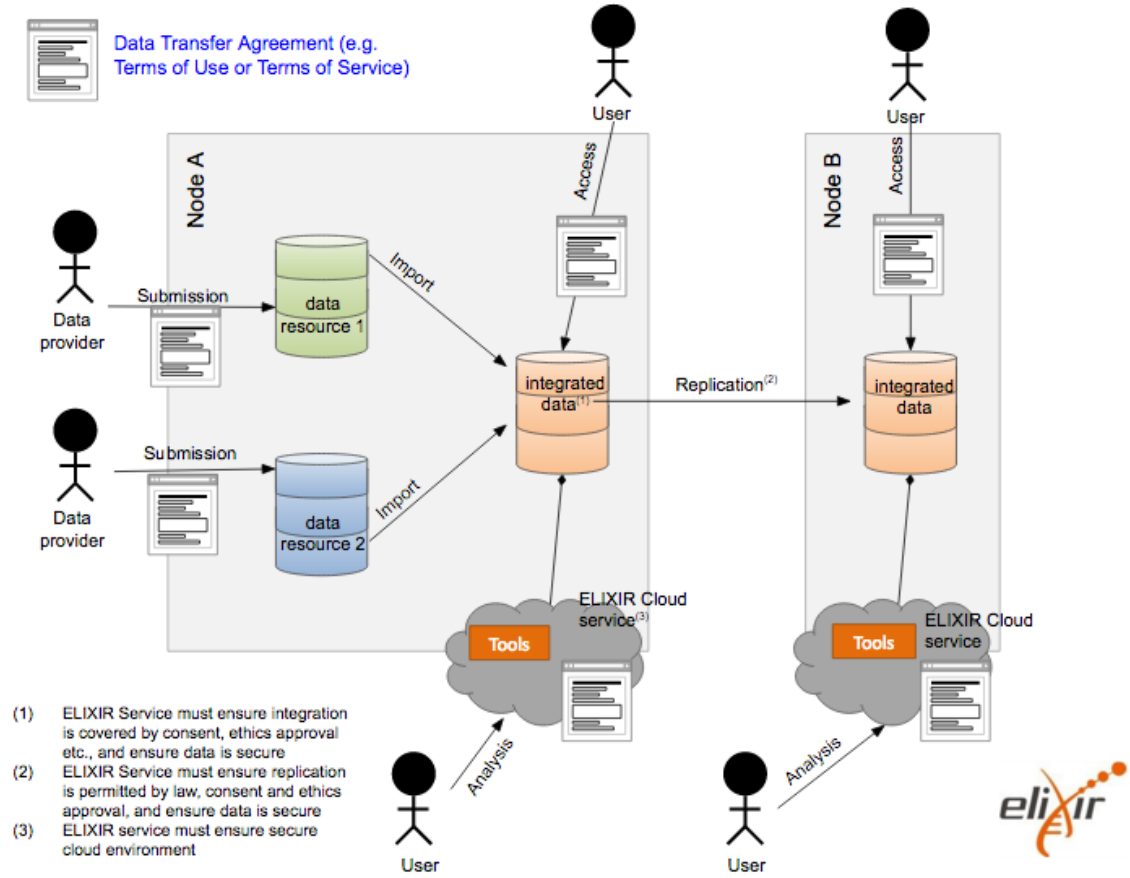

Figure 3 ELIXIR Service integrating and/or replicating existing data resources, resulting in a new resource with different functionality compared to the data sources. As a result, the ELIXIR Service should examine their role with respect to the Ethics policy

11. What are the definitions of terms based on?

While a small number of terms have been defined specifically to clarify roles in the provision of ELIXIR Services, most definitions of terms are based on several sources, including the Global Alliance for Genomics and Health Data Sharing Lexicon and definitions from the European General Data Protection Regulation. In several cases, the definitions include some level of clarification of the term in the context of providing data for scientific research as part of an ELIXIR Services[1].

Term	Definition	References
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	Refer to Recital 26 GDPR; includes considerations on implementation
Consent	means any freely given, specific, informed and unambiguous indication of their wishes by which the Data	GDPR Article 4 (Definitions)

[1] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679

	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	GA4GH Lexicon (includes additional clarification on the conditions for data access)
Data Protection Officer	means a designated person within an organisation that collects Personal Data; he/she acts independently and is responsible for making sure that the organisation complies with data protection law	Refer to Article 37, 38, 39 GDPR
Data Controller	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	Refer to GDPR Article 4 (Definitions)
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	ELIXIR Ethics Policy
Data Subject	refers to an identified or identifiable natural person (individual) whose data are accessed (e.g. patients, donors or study participants)	Refer to GDPR
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 ELIXIR Service – “data in”) or a Service Provider and a Service user (i.e. when an ELIXIR 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	Contractual agreement on data provision in the context of ELIXIR Services; ELIXIR Ethics Policy
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 ELIXIR Service	ELIXIR Ethics Policy
ELIXIR Service(s)	refers to ELIXIR Services as defined in the Node Collaboration Agreements, i.e. Node-funded Services or Commissioned Services.	ELIXIR Node Collaboration Agreement
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 ELIXIR Service	ELIXIR Ethics Policy
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	Refer to GDPR Article 4 (Definitions)
Incidental Findings	are findings concerning an individual discovered in the course of research using data offered in the context of an ELIXIR Service that are beyond the original aims of the	GA4GH Data sharing lexicon

	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	GDPR Article 4 (Definitions)
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	GDPR Article 4 (Definitions)
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	Refer to GDPR Article 4 (Definitions)
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	GDPR Article 9 (except for biometric data as such data, where relevant, would be covered under data concerning health)
Service Provider	refers to the Node providing an ELIXIR Service	ELIXIR Ethics policy
Supervisory Authority	means an independent public authority established in order to supervise and decide critical issues in a specific area	

ELIXIR ETHICS POLICY

Author of the paper

ELIXIR Director

Purpose of the paper

To present the proposed ELIXIR Ethics Policy to the ELIXIR Board

Action required

The Board is asked to review and approve the policy presented

Voting requirements

Decision by simple majority is required by application of ECA Art. 6.2.4.bb (TBC)

ELIXIR ETHICS POLICY

1. Considerations

i. The ELIXIR founding documents place special emphasis on the development of an ELIXIR Ethics Policy in order to support the sharing of data underlying specific regulatory requirements, especially Personal Data including Sensitive Data. The Policy is established and approved by the ELIXIR Board as set forth in Art. 11 of the ELIXIR Consortium Agreement and provides the basis for the implementation of the requirements arising from the Node Collaboration Agreements.

ii. Some ELIXIR Services manage data from human research participants and 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.

iii. The purpose of this Policy is to support the process of making scientific data available in the context of ELIXIR in an ethically and legally sound manner by consolidating requirements that are shared across all ELIXIR Members and Services, including those arising from the ELIXIR founding documents. This Policy imposes no additional constraints on the use of data contributed to ELIXIR Services than those provided by the Data Controller/Provider or existing legal and ethical requirements.

iv. ELIXIR recognises that while data and knowledge provided by ELIXIR 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 license considerations are not covered in this policy.

v. ELIXIR recognises that the purpose of many ELIXIR Services 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.

vi. Every ELIXIR Service (i.e. Node-funded Services included in Service Delivery Plans and Commissioned Services - either Implementation Studies or Infrastructure Services) 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.

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

viii. ELIXIR 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, ELIXIR ensures excellence in the delivery of ELIXIR Services.

ix. The ELIXIR Ethics Policy provides evidence that an adequate level of protection of Personal Data including Sensitive Data is in place throughout ELIXIR - including across national borders - which increases the acceptance of clauses in Consent forms concerning data deposition with ELIXIR 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. Since research projects are reviewed on the basis of relevant legal and ethical standards, many ethics committees are reluctant to approve data sharing beyond borders when there is no cross-border standard of data sharing policies in place. This Policy provides that standard.

x. 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.

xi. ELIXIR 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 ELIXIR Services that go beyond the scope of this policy.

2. Scope

This Policy applies to ELIXIR Services that make data underlying specific regulatory requirements available.

The Policy applies solely to ELIXIR Services as defined by the ELIXIR founding documents[1], i.e. Node-funded Services provided in the context of Node Collaboration Agreements and on the basis of Service Delivery Plans, and Commissioned Services provided on the basis of Commissioned Services contracts. It does not apply to any

[1] see ELIXIR founding documents: ELIXIR Consortium Agreement and Node Collaboration Agreement

other services or research activities provided by the institute(s) constituting or affiliated with the ELIXIR Node.

The vast majority of data made available for research via ELIXIR 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 ELIXIR 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 ELIXIR Service.

3. Legal Basis

As set forth in Art 11. of the ELIXIR Consortium Agreement, the ELIXIR Board shall establish an Ethics Policy 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.III.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; 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 means a designated person within an organisation that collects Personal Data; he/she acts independently and is responsible for making sure that the organisation complies with data protection law.

Data Controller 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 ELIXIR Service – “data in”) or a Service Provider and a Service user (i.e. when an ELIXIR 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 ELIXIR Service.

ELIXIR Service(s) refers to ELIXIR Services as defined in the Node Collaboration Agreements, i.e. Node-funded Services or Commissioned 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 para. 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. 9.

The Data Controller overseeing the provision of Personal Data in the context of an ELIXIR Service has to ensure that the intended Processing is lawful (e.g. through a Data Access Committee). Where an ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ELIXIR Ethics 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 ELIXIR 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 ELIXIR 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 ELIXIR 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 ethicsreview must cover the secondary use of data e.g. through submission and managed access through an ELIXIR 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 ELIXIR Service, the Data Provider must ensure that relevant guidelines and laws for the animals' welfare and care during collection of the data were followed.

Where non-human genome data is made available, use and provision in the context of an ELIXIR 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 the ELIXIR Ethics Policy lies with the ELIXIR Board.

The ELIXIR Director is responsible for ensuring that the Policy is routinely reviewed by the ELIXIR 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

Nodes Committee and via the Collaboration Oversight Groups for individual Nodes will also be sought regularly.

8.2 Implementation and compliance

As per Art. 10.1.2g of the Node Collaboration Agreements, the ELIXIR Heads of Nodes are responsible for ensuring compliance with this Policy for the ELIXIR Services offered by the respective Node.

For the sake of clarity, and as indicated in Art. 14 of the Node Collaboration Agreement, each ELIXIR Node is responsible to implement its own policies in order to ensure that the Services provided within ELIXIR comply with the ELIXIR Ethics Policy and national rules and regulations as well as international standards of best practice.

8.3 Information

As per Art. 14 of the Node Collaboration Agreement, the ELIXIR Hub 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 ELIXIR Director, the Head of Node and other individuals appointed by them, shall monitor the compliance of ELIXIR Services provided by the Node in question[2].

In collaboration with the ELIXIR Scientific Advisory Board and supported by the Node in question, data concerning ELIXIR Service compliance with the ELIXIR Ethics Policy will be gathered by the Hub and submitted to the ELIXIR Scientific Advisory Board in the context of regular ELIXIR Service reviews.

In accordance with Art. 11.2 of the Node Collaboration Agreement, upon recommendation of the ELIXIR Scientific Advisory Board (including Ethics Experts and replacing the Ethics Advisory Committee as per the ELIXIR Board decision DD/MM/YYYY), the ELIXIR Board shall decide whether it wishes to renew or terminate (in whole or in part) the Agreement with the ELIXIR Node.

This Policy has been adopted by the ELIXIR Board on November, .. 2016.

[2] It should be noted that the Collaboration Oversight Group works as a flexible structure to facilitate communication, but the rights and obligations of the ELIXIR Director and the Head of Node remain unaffected as stated in Art. 10.2.2 of the ELIXIR Collaboration Agreement.