HEALTHYCLOUD
Health Research & Innovation Cloud

D2.2 Framework of modular contract clauses for HRICs

Document Information

Contract Number	965345
Project Website	http://www.healthycloud.eu/
Contractual Deadline	M18, August 2022
Dissemination Level	PU-Public
Nature	R-Report
Author(s)	Adrian Thorogood (UNILU, WP2)
Contributor(s)	Regina Becker (UNILU, WP2) Irene Schlünder (BBMRI-ERIC/TMF, WP2), Christian Ohmann (ECRIN, WP2) Linda Ebermann (UNILU, WP2)
Reviewer(s)	Carlos Luis Parra Calderón (SAS) Ramón Launa Garcés (IACS) Alexander Degelsegger-Márquez (GÖG)
Keywords	Legal framework, data access agreement, data processing agreement, organisational safeguards, cloud, usage, hosting, privacy by design

Notice: *The HealthyCloud project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement №965345*

Table of contents

DOCUMENT INFORMATION ... 1

TABLE OF CONTENTS ... 1

EXECUTIVE SUMMARY ... 2

1 INTRODUCTION ... 2

1.1 BACKGROUND ... 2
1.2 METHOD ... 3
1.3 CONTEXT, TERMINOLOGY AND DEFINITIONS ... 3
1.4 PROPOSED STRUCTURE AND IMPLEMENTATION OF MODULAR CLAUSES ... 4
1.5 INTERSECTIONS WITH OTHER HEALTHYCLOUD DELIVERABLES ... 4

2 GDPR REQUIREMENTS FOR DATA SHARING CONTRACTS ... 5

2.1 GDPR REQUIREMENTS FOR JOINT CONTROLLER AGREEMENTS (ART 26) ... 6
2.2 GDPR REQUIREMENTS FOR DATA PROCESSING AGREEMENTS (ART 28) ... 7
2.3 TRANSFERS BETWEEN CONTROLLERS ... 8

3 DATA ACCESS AGREEMENTS – MODULAR CLAUSES ... 8

3.1 INTRODUCTION ... 8
3.2 LIST OF EXAMPLES/TEMPLATES REVIEWED ... 9
3.3 MODULAR CLAUSES ... 10

4 DATA SUBMISSION AGREEMENTS – MODULAR CLAUSES ... 14

4.1 INTRODUCTION ... 14
4.2 LIST OF EXAMPLES/TEMPLATES REVIEWED ... 15
4.3 MODULAR CLAUSES FOR A DATA SUBMISSION AGREEMENT ... 15

5 DATA HOSTING AGREEMENTS ... 19

5.1 LIST OF EXAMPLES/TEMPLATES REVIEWED ... 19
5.2 DATA HOSTING – CONTROLLER-PROCESSOR [C-P] ... 19
5.2.1 DATA HOSTING – JOINT CONTROLLERSHIP [JC] ... 20
5.2.2 DATA HOSTING – CONTROLLER-TO-CONTROLLER TRASNFER [C-C] ... 22

6 AGREEMENTS GOVERNING DATA ANALYSIS IN SECURE PROCESSING ENVIRONMENTS ... 23

6.1 LIST OF EXAMPLES/TEMPLATES REVIEWED ... 23
6.2 MODULAR CLAUSES ... 23

7 CONCLUSION: OPPORTUNITIES AND CHALLENGES TO ADOPTING HARMONIZED AGREEMENTS ... 24

Executive Summary

This deliverable provides a list of modular contractual clauses that can be integrated into data sharing agreements that support the implementation of a Healthy Research and Innovation Cloud (HRIC) in the EU. The document reviews common clauses found in the following categories of data sharing agreements:

1. Data Access Agreements (between Data Providers/Data Hubs and Data Users, where access to data is granted for research purposes),
2. Data Submission Agreements (between Data Providers and Data Hubs where data are submitted to a Data Hub to be curated and stored to facilitate access by prospective Data Users),
3. Data Hosting Agreements (between Data Providers and Data Hubs, outlining conditions and processes of data access), and
4. Data Analysis Agreements (between Data Users and Data Hubs which provide a Secure Processing Environment for the analysis of data).

The focus of this document is on addressing data protection requirements. This requires assumptions to be made about the context in which these agreements are used, as well as the resulting GDPR roles and relationships. The deliverable outlines the GDPR sub-components of these agreements depending on the applicable relationships (e.g., GDPR data processing agreements, joint controller agreements, data transfer agreements), and outlines the clauses commonly needed in these agreements to satisfy GDPR compliance. For Data Access Agreements specifically, a broader set of common clauses are described relating to intellectual property rights (IPR), publication policies etc. .

The primary aim of this deliverable is to provide a checklist of clauses for data sharing agreements in an HRIC. This will assist drafters with ensuring agreements cover essential matters. Use of this deliverable can also support greater standardization of the content of such agreements, which can improve the consistency of clauses, reduce time spent drafting and negotiating agreements, as well as increase the connectability of resources. The clauses are not intended, however, to be standard or harmonized agreement templates, as drafters retain the flexibility to include (or not) certain clauses suitable to their context, or to select between different options relating to a particular theme.

1 Introduction

1.1 Background

Task 2.2 of Healthy Cloud describes the goal of developing ELSI compliant contract templates for data access and resource usage.

Task 2.2. ELSI compliance of the governance of the future HRIC decentralized platform (Lead: UNILU – Participants: IACS, BBMRI-ERIC, TMF, GOG, BSC, SAS) (M01-M30): "Based on already existing data hosting and data use contracts, this task will generate templates that can be used by data providers, data hubs and compute infrastructure providers at the institutional level to provide the tools for a GDPR compliant implementation of Art. 26 and Art. 28 (where applicable). In addition, researcher-specific templates will be generated to delineate the rights and obligations of end users of data consistent with the HRIC-wide framework of data handling responsibilities."

1.2 Method

The method used to develop this deliverable consisted primarily of a review of data access agreements, templates, and standard models (including those from data resources, data hubs, and computing environments surveyed by WPs 3-5). The deliverable was also informed by a review of relevant legislation (e.g., GDPR), guidelines, and literature.

1.3 Context, Terminology and Definitions

This Deliverable should be read in the context of data sharing in an HRIC. The parties involved, their relationships, and the types of agreements that connect them are helpfully described in the Data Governance Model proposed in D2.1. This Deliverable relies on terms selected and defined in the HealthyCloud Glossary, most importantly the following terms:

Data Provider: "Any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as European Union institutions, bodies, offices and agencies who has the right or obligation, or the ability to make available, including to register, provide, restrict access or exchange certain data."

Data User: "A natural or legal person/organisation who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes."

Health Data Hub (or simply Data Hub): "Minimal inclusion criteria: 1. A digital technical infrastructure with the core mission of enabling health data sharing 2. It provides health data from different sources 3. It allows discovery of health datasets 4. It has a metadata discovery service 5. It has a data accessibility mechanism in accordance with existing regulation 6. It has an authorization functionality, provided by the same Data Hub or by an external institution."

Secure Processing Environment: "The physical or virtual environment and organisational means to provide the opportunity to re-use data in a manner that allows for the operator of the secure processing environment to determine and supervise all data processing actions, including to display, storage, download, export of the data and calculation of derivative data through computational algorithms."

In addition, this Deliverable introduces the following terms, which may be included in subsequent versions of the Glossary.

Data Access Agreement (i.e., data use agreement, data transfer and use agreement): An agreement for a Data Provider (and/or a Data Hub) granting a Data User access to data to be employed in the Data User's research project. The GDPR relationship between the entity providing access and the Data User is typically controller-to-controller.

Data Submission Agreement (i.e., data submission and processing agreement, data transfer agreement, data deposition agreement): An agreement for a Data Provider submitting data to a Data Hub that provides services to curate, manage, and store the data, so as to facilitate making data available to prospective Data Users. The GDPR relationship between the Data Provider and Data Hub is typically controller-to-processor. A Data Submission Agreement typically comprises a service-level agreement as well as a GDPR data processing agreement.

Data Hosting Agreement (i.e., data access policy): An agreement for a Data Provider and a Data Hub outlining the conditions and processes for granting prospective Data Users access to data. The GDPR relationship between the Data Provider and Data Hub is context-dependent, and may be controller-to-processor, joint controllership, or controller-to-controller. The type of GDPR agreement required will depend on the relationship.

Data Analysis Agreement (Data processing agreement; terms of use**)**: An agreement for a Data User conducting a research analysis within a Secure Processing Environment provided by a Data Hub (or other cloud platform). The GDPR relationship between the Data User and the Data Hub is typically controller-processor, and will include a GDPR data processing agreement.

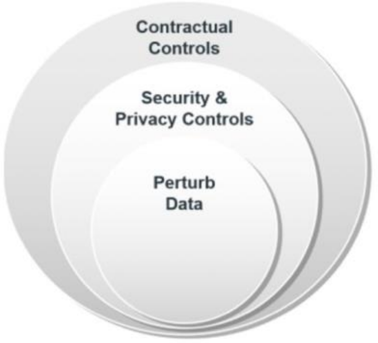
Note: these agreements are not just one-to-one agreements, but can also be many-to-one, one-to-many, or many-to-many.

1.4 Proposed Structure and Implementation of Modular Clauses

The modular clauses are framed as a checklist of elements to inform the drafting of data sharing agreements (or templates). These elements can help to draft an agreement or template by ensuring that relevant issues have been covered in the document. In some cases we have suggested a DEFAULT clause, with alternatives provided (indicated by an OR). Clauses described as OPTIONAL are to be included at the discretion of the parties drafting the agreement. These clauses could in the future be implemented into contractual drafting IT tools. An additional potential goal of the modular clauses is to promote standardisation of data sharing agreements. The modular clauses can contribute to consistent use of standard content in data sharing agreements. Where optionality exists, the modular clauses can accelerate negotiations by presenting default choices and a bounded range of alternatives.

1.5 Intersections with Other HealthyCloud Deliverables

This deliverable on modular contractual clauses complements and is informed by **D2.1. First draft on legal framework for technical safeguards with a focus on cloud usage** (Responsible: BBMRI-ERIC) (M15). D2.1 outlines minimal data security standards for agreements involving the provision of data access to a user on a cloud platform. Contractual controls complement other forms of security and privacy controls to reduce risks (see Figure below). These two deliverables should therefore be read together.



[1]

This deliverable is also informed by **D4.1 Recommendations for integration in HealthyCloud, including an analysis of Data Hub patterns of governance.** This survey was used as a source to identify examples/templates of data use/processing agreements used by existing Data Hubs.

The HealthyCloud survey of Data Hubs included questions about "Data Access Agreements" and "Data Processing Agreements" (we refer to the latter as Data Submission Agreements in this deliverable). The survey provided a valuable resource of links to existing agreements incorporated into this deliverable. The survey also highlighted the degree to which Data Hubs are willing to negotiate the contents of these agreements.

In the HealthyCloud survey of Data Hubs, some had non-negotiable Data Access Agreements, whereas others had negotiable ones. 55,26% (21) of the 38 interviewed data hubs' answers provide a Data Access Agreement, 23,68% of the 38 answers do not provide a Data Access Agreement, and 21,05% of the 38 answers selected "Other" e.g., depends on the specific resource queried, only employees can access the data directly. 52,38% of the 21 with Data Access Agreement use a non-negotiable form, and 47,62% of the 21 with Data Access Agreements provide a template that may be modified under the agreement.

In the HealthyCloud survey of Data Hubs, in terms of a Data Processing Agreement [Data Submission Agreement] to be signed with the Data Providers, 53,12% (17/32) answers provide a Data Processing Agreement. 25,00% do not provide a Data Processing Agreement, and 21,87% selected other (to be further analysed). 41,18% of the 17 with Data Processing Agreement use a non-negotiable form, and 58,82% of the 17 with Data Processing Agreements provide a template which may be modified under the agreement.

2 GDPR Requirements for Data Sharing Contracts

Forms of data protection responsibility between parties in health research data sharing are described in the following table (adapted from D2.1). The type of agreement usually applicable in each context is also described in the table, and the following sub-sections clarify GDPR requirements relating to the content of these agreements.

Controller to Processor	**Joint Controllership**	**Controller to controller** **(Separate responsibility)**
Art. 28 GDPR	**Art. 26 GDPR**	**Normal case**
Basic dependence on instructions Decision-making power of the person accepting the instructions possible for the TOMs (Art. 32 GDPR)	Equality: i.e. joint decision-making Joint influence on the personal data processing	Contractual requirements for the handling of the transferred data possible, e.g. limitation of the permitted processing purposes.
The person commissioning the data processing[?] decides on the purpose and means of data processing	Means and purpose of the data processing are jointly determined	Each responsible person shall determine its purposes and means
E.g., Data Submission Agreement (between Data Provider and Data Hub); **Data Analysis Agreement** (between Data User and Data Hub providing a Secure Processing Environment (SPE))	**E.g., Data Hosting Agreement** (between Data Provider and Data Hub acting as an access intermediary)	**E.g., Data Access Agreement** (between Data Provider/Data Hub and Data User)

2.1 GDPR Requirements for Joint Controller Agreements (Art 26)

GDPR Art 26 (1)Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
(2) The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
(3) Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

“In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities." (EDPB 07/2020)

"Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data." (EDPB 07/2020)

"The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract. … The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement." (EDPB 07/2020)

"Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle." (EDPB 07/2020)

"The obligations do not need to be equally distributed among the joint controllers. … However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools. … Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers." (EDPB 07/2020)

2.2 GDPR Requirements for Data Processing Agreements (Art 28)

The GDPR requires that processing of personal data shall be governed by a binding contract addressing a range of substantive matters (Art 28(3)), including the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. Obligations of the processor include the following:

- process only on documented instructions from the controller,
- ensure persons authorised to process have committed themselves to confidentiality,
- provide sufficient guarantees to implement appropriate technical and organisational measures,
- ensure security, and
- assist the controller to respond to requests for exercising the data subject's rights,
- assist controller to fulfill security, breach reporting, and accountability obligations,

- at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies,
- assist with demonstrating compliance,
- allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller,
- when engaging a sub-processor, the processor shall not engage another processor without prior specific or general written authorisation of the controller:
    - in the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes,
    - sub-processing shall be governed by a binding contract (extending the same obligations as above),
- if the processor considers that any of the instructions received infringes the GDPR or any other data protection provisions of the Union or the Member States, he/she shall immediately inform the controller.

2.3 Transfers Between Controllers

Technically speaking, contractual agreements are not required for controller to controller transfers, as both controllers have full statutory responsibility under the GDPR for their own processing. However, agreements can be established in these cases as an accountability tool to clarify the respective obligations of the parties. See also EDPB Guidelines 04/2019: “The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.”

3 Data Access Agreements – Modular Clauses

3.1 Introduction

A Data Access Agreement is a contract that describes what data are being shared by a Data Provider to a Data User, “for what purpose, for how long, and any access restrictions or security protocols that must be followed by the recipient of the data.”[2] The arrangement is often complicated by the involvement of a Data Hub, in which case the Data Access Agreement will be between the Data Provider and/or Data Hub on one side (depending on the nature of their Data Hosting relationship – see below), and the Data User on the other side. For simplicity, we will refer simply to the Data Provider throughout this section.

Often these types of contracts are structured as a generic set of terms and conditions governing data use, combined with some project-specific information describing the party or parties requesting access, the datasets or fields requested, etc.. Project-specific information is often entered into a data access request form and then incorporated into the agreement. Where a Data Hub provides access to multiple datasets from multiple sources, the agreement may also incorporate dataset-specific information or conditions (e.g., the duration of a particular publication embargo, or the details of how to acknowledge a particular source in the agreement).

[2] (Vilhuber n.d.)

The assignment of GDPR roles to the Data Provider(s) and Data User(s) will affect the respective data protection responsibilities of the parties, and in turn the nature and content of the agreement between the parties. By default we consider a Data Access Agreement to be a Controller to Controller agreement (transmission). This is because in most secondary use contexts, the Data User pursues an own research project, and the Data Provider merely provides data access.[3] As controllership is assigned to specific phases of processing, not to the data itself, the Data Provider would be the upstream controller for the primary purpose (e.g., initial healthcare or research project), and the Data User would be the downstream controller for the research project. Again, this relationship may be complicated in many scenarios by the involvement of a Data Hub. In such cases, the Data Provider and/or Data Hub may be considered the upstream Controller (or joint controllers), and the Data User will be the downstream controller. Again, for simplicity in this section we refer to Data Provider as the upstream controller. The subsequent section of Data Hosting Agreements will explore different potential relationships between Data Providers and Data Hubs.

In theory, no contract or specific clauses are required by the GDPR in a controller-to-controller context (assuming both controllers are based in a EU/EEA country), as both controllers have full statutory responsibilities. However, in practice, a contract will in any case be needed to cover matters beyond data protection (e.g., IP, publication). And data sharing agreements can function as a helpful accountability tool clarifying the responsibilities of both parties and can be seen as an accountability tool under the GDPR of the disclosing controller.

Data sharing agreements within the context of joint collaborations are outside the scope of this deliverable. Where the Data Provider and Data User are actively collaborating on the project, they will be joint controllers for the project – they will have a collaboration agreement and a joint controller agreement. Some of the Data Access Agreements reviewed here are structured as joint controllership agreements (e.g., SPHN), reflecting the particular collaboration context.

An important trend is that the contractual protections of Data Access Agreements are increasingly complemented by requirements that access to data are provided to Data Users within Secure Processing Environments (SPEs). SPEs may be managed by Data Hubs or on-premise by Data Providers. There are different implementations, e.g., direct v.s. indirect remote access to data. In a federated analysis, the Data User may submit an analysis routine to a coordinating body, which then sends the routine to multiple different SPEs (hosted by different Data Hubs or Data Providers) to run on local data. Contractual clauses in a Data Access Agreement that may be relevant to all or some SPE contexts are mentioned as [SPE].

3.2 List of Examples/Templates Reviewed

A range of examples and templates were reviewed, reflecting a range of different contexts.

- European Genome-Phenome Archive, Data Access Agreement template (no date)
- Swiss Personalised Medicine Network, Data Transfer and Use Agreement (01.06.2021)
- Germany Medical Informatics Initiative, Germany Medical Informatics Initiative, Contract on the use of patient data, biomaterials, analysis methods and routines within

the framework of the medical Informatics Initiative (v1.3 06.10.2020) [translated from German]
  - +Annex to the contract of use: General Terms and Conditions of Use and Contract for the provision and use of patient data, biomaterials and analysis methods and routines within the framework of the medical informatics initiative (v1.3)
- ELIXIR-Luxembourg, Data Use Agreement-ELIXIR (v1.5 07.2022)
- EU Stands4PM, Harmonised Data Access Agreement (hDAA) for Controlled Access Data (v 1.0)
- Instituto Aragonés de Ciencias de la Salud, Agreement for the Transfer of Human Biological Samples and/or Associated Clinical Data for Biomedical Research (internal)

3.3 Modular Clauses

Context
- Parties to the Agreement (e.g., Data Provider, Data User (principal investigator and affiliated institution)).
- Purpose /Project (usually described in an Appendix – incorporated from the Data Access Request form).
- Justification of the need for access to personal data or pseudonymised data (because the research includes follow-up of patients or updating of data of the cohort under study).
- Data (usually data sets and/or data fields/types are described in an Appendix – incorporated from the Data Access Request form).
- Duration of Data Access
  - DEFAULT: Project-specific duration specified by requestor – incorporated into the Data Access Agreement from the Data Access Request form. Potentially subject to a maximum duration (e.g., 5 years). Process for requesting extensions.
  - [OR: Standard duration of access (e.g., 1 year). Process for requesting extension].

Note: a process should be foreseen for substantial amendments to these main elements of the project.

General Obligations

- Data Provider commits to provide the Data User access to data for the duration of the project, and permission/license to use the data for the project. *Note: this clause will be more important where data are accessed in a SPE controlled by the Data Provider*.
  - Data Provider will provide the data in optimal research conditions and follow applicable quality standards, including metadata that enables compliance with FAIR principles in as much depth as possible. *Note: this does not constitute a warranty*.
  - Data User commits to only use the data for the project.
- Fees to be paid for services from the Data Provider (where applicable).
  - DEFAULT: data are provided for free and fees are limited to cost recovery and specified in an Appendix of the DUA.
  - [SPE] Fees to be paid for Secure Data Processing Services provided along with the data.
  - [SPE] Data Provider shall be granted a right of use to the analysis methods and routines.

Privacy/Confidentiality

- Data Provider will ensure the data are appropriately anonymised, or where justified, appropriately pseudonymised/coded or identified data.
- Data User obligations:
    - shall only use data for the authorized purpose/project [see Essential Clauses above].
    - shall not attempt to re-identify or re-contact data subjects.
    - shall not attempt to link datasets at the individual level.
    - shall keep all (personal) data received confidential.
        - shall ensure all staff with access to data are bound by a duty of confidentiality.
        - unless data are publicly known, or must be disclosed by law.
    - shall ensure only aggregate/anonymous data are released in publications. [*Note: where data are processed in an SPE, the Data User shall only be allowed to export aggregate/anonymous data. The Data Provider may retain the right to review the results before export.]*
    - shall report a personal data breach to the Data Provider in a timely manner and assist with mitigation.
- General prohibition on onward transmission/provision of access.
    - [OPTIONAL EXCEPTION] other authorized Data Users.
    - [OPTIONAL EXCEPTION] data processors approved by the Data Provider.

Note: see the Warranties section for Data Provider statements about upstream data protection compliance

International Transfer (to a Data User in a third country)

- general prohibition on International Transfers to parties in third countries outside the EU/EEA or to international organisations.
    - [OPTIONAL EXCEPTION] subject to conditions of onward international transfer by User.
- [OR] standard contractual clauses may be incorporated as an Appendix.

Security

- DEFAULT Data User must adopt reasonable technical and administrative measures to prevent unauthorized or unlawful access or use.
- [OR] Minimum security requirements established by the Data Provider.
- [OR] Minimum security commitments are detailed by the Data User (usually in an Appendix).
- [OR] Data User must only process data in a Secure Processing Environment (SPE) designated by the Data Provider.
- [OR] Data User must only process data in a certified SPE. [*Note: clauses for security in the SPE are addressed below]*.
- Data User has the obligation to report security incidents to the Data Provider.
- [OPTIONAL (where applicable)] Data Provider will have the right to audit the Data User's security, under certain conditions (e.g., time periods; on premises and/or virtual).

Data subject rights, accountability

- any requests to exercise data subject rights submitted to the Data User will be directed to the Data Provider.

- Data User shall assist the Data Provider with the exercise of data subject rights.
- in particular, the Data User will delete all copies of a data subject's data upon request of the Data Provider in response to a withdrawal of consent or an objection to processing (unless these rights are not applicable, or exceptions apply).
- Data User shall provide the Data Provider with information necessary to allow it to fulfill its accountability obligations.

Publication (Acknowledgement, Reporting, and Review)

- Data User will acknowledge Data Provider(s) in any scientific publication (form of acknowledgement typically specified in the agreement).
- [OPTIONAL] Data User will acknowledge an infrastructure provider (e.g., Data Hub) in any scientific publication (form of acknowledgement typically specified in the agreement).
- Data User shall respect applicable publication embargos (typically specified in the agreement).
- Data User shall state the User is fully responsible as author for the contents of the publication.
- Data Provider has the right to publish information about the completed project and its outcomes.
  - [OPTIONAL] Data User is required to report reference citation upon publication to the Data Provider.
  - [OPTIONAL] Data User is required to report on study completion to the Data Provider (may be confidential).
- [OPTIONAL] Data User shall provide a draft of all manuscripts X days before submission for review by the Data Provider. The Data Provider shall review the manuscript to ensure purpose limitation was respected (research on an approved area), includes appropriate acknowledgement and does not include personal data.

Scientific Integrity and Reproducibility

These clauses clarify the expectations of the scientific community. In addition, EDPB suggests that to fall under "scientific research" in the GDPR, a research project must be "set up in accordance with relevant sector-related methodological and ethical standards" [EDPB Guidelines 05/2020] In some cases these clauses will be drafted as recommendations. In others these will be drafted as binding contractual obligations.

- Data User is expected to carry out the research project following the state-of-the-art in terms of scientific practice.
- Data User is expected to publish or publicly report results.
- Data User is expected to include a reproducibility statement in any publication allowing others to repeat the study.
- Data Provider is expected to ensure the ongoing availability of any original or derived data used in the study, including metadata for compliance with FAIR principles.

Commercialisation and Intellectual Property (Data)

- Data Provider retains any ownership and IP rights in the primary data.
- Data User is prohibited from making IP claims on the primary data.
- Data User is prohibited from selling or otherwise commercialising the primary data.

Intellectual Property (Results)

- [DEFAULT] Data User is permitted to pursue commercialisation.
    - Data User owns any IP rights that may arise from the project, but these must not obstruct further exploitation of the data by other parties.
- [OR] The Data User agrees to provide a non-exclusive license any IP in the results back to the Data Provider.
- [OR] Agreement to negotiate in good faith.
- [SPE] Data User retains IP rights in any data analysis tools used or created.

<u>Confidentiality (towards other party)</u>

- Each party agrees not to disclose any scientific information or techniques belonging to the other party without permission of that party or unless its already in the public domain.
- [OPTIONAL] terms of the Data Access Agreement are confidential and cannot be announced without approval of the other party.

<u>Return of Analysis Results / Derived Data / Associated Scripts</u>

- [DEFAULT] Data User shall provide the Data Provider with a copy of analysis results, derived data, and/or associated scripts (expected products are usually specified in the access request form / appendix of the agreement).
- Data User provides the Data Provider with a license to re-use and share the derived data subject to the same conditions as the primary data.

<u>Research Ethics</u>

- [DEFAULT] the project has been reviewed and approved by a competent Research Ethics Committee (REC), where required by local norms.
- [OR] the project has been reviewed and approved by a competent Research Ethics Committee (REC)
- [OR – OMIT may not be required depending on the context].

<u>Handling of individual findings of clinical relevance</u>

This issue is not addressed here as it is very context specific. In some cases Data Providers may impose a particular policy stating that Data Users MUST, SHOULD, MAY, or MUST NOT report findings of clinical relevance to data subjects or their families, as well as defining criteria for reportable results. Data Provider policy will depend on many factors including having obtained consent. The Data Users may be required by their research ethics committees to anticipate if their project has the potential to generate (new) research results or incidental findings of clinical significance, though the possibility of return will always be dependent on the Data Provider.

<u>Data Provider warranties, waivers, limitations of liability</u>

- warranty the Data Provider is entitled to supply the data in compliance with applicable laws, approvals, consents.
    - [OPTIONAL] warranties, attestations, or documentation about specific obligations, e.g., data protection obligations to have lawfully collected the data.
- no warranties for data quality, utility, accuracy, completeness, suitability.
- [SPE] no warranties for data availability.
- no warranties of infringement of third party IP rights.
- No liability for damages resulting from use of the data, as recipient is sole controller.
- no liability for data unavailability.

Data User warranties, waivers, limitation of liability

- warranty that Data User has resources and expertise to conduct the project.
- warranty that the project is in compliance with applicable laws and approvals.
- [SPE] warranty the analysis methods have been reviewed for security flaws [and have documented any deficiencies or risks].
- [SPE] no warranty for the non-existence of third party IP rights in the analysis routines provided. Data User accepts liability for a breach of such rights in connection to the data use.
- [SPE] Data User shall be liable for damage caused to Data Providers caused by the performance of analyses by way of analysis methods and routines provided.
- [For Derived Data] no warranty of or liability for the data quality, utility, accuracy, completeness, suitability.

Term and Termination

- agreement enters into force upon final signatures.
- agreement may be terminated: upon completion of the project, by mutual agreement, dissolution of one the parties, or by breach of obligations.
- notice period for termination of the agreement.
- conditions under which the parties may terminate the agreement.
- consequences
    - Data User obligation to delete/return of data.
    - [SPE] immediate termination of access.
- surviving clauses - rights/obligations (such as confidentiality, acknowledgement, return/destruction) shall not cease.

Miscellaneous

- Changes/Amendments
- Dispute Resolution
    - Parties agree to resolve disputes that may arise from implementation of the agreement amicably.
    - [DEFAULT] Parties agree to only submit disputes to the competent court in the jurisdiction of the Data Provider.
    - [OR] ...of a specified neutral jurisdiction.
- Applicable Law
    - [DEFAULT] Parties agree that the agreement will be governed by the law of [the jurisdiction of the Data Provider].
    - [OR]: Parties agree that the agreement will be governed by the law of [the jurisdiction of the Data User].
- Signature Page

4 Data Submission Agreements – Modular Clauses

4.1 Introduction

A Data Submission Agreement is established between a Data Provider and a Data Hub and governs the deposit, transformation and storage of data in a repository so that the data can be more easily made accessible in the future to prospective Data Users. In GDPR terms, the

Data Provider is typically the Data Controller, whereas the Data Hub is typically a Processor. A Data Deposition Agreement often is constituted by a Service Agreement, which is generally combined with a separate Data Processing Agreement to enable the processing of personal data necessary to fulfil the service contract. The Data Hub may also establish a Privacy Policy describing how it processes the administrative or operational personal data (e.g., name, contact details, login details) about the Data Provider as well as information collected for invoicing, security, service quality, etc., for which the Data Hub may act as a Controller.

4.2 List of Examples/Templates Reviewed

- European Genome-Phenome Archive (EGA), Data Processing Agreement (v 1.1 March 2021) BBMRI-ERIC, Data Transfer Agreement (v 28 September 2018).
- University of Luxembourg / ELIXIR-LU, Hosting and Processing Agreement ("General Terms of Services") (v 2.2 October 2020).
- Swiss Personal Health Network (SPHN), BIOMEDIT Infrastructure Data Transfer and Processing Agreement (V3 01 June 2021).
- Aragon, Acuerdo de Encargado del Tratamiento (8 August 2019).
- EOSC Life, COVID-19 Repository Data Sharing Policy (20 September 2021).

4.3 Modular Clauses for a Data Submission Agreement

Given the wide diversity of Data Hubs and associated services, clauses describing the services provided by the Data Hub will vary widely. We provide a brief introduction to these services to provide context for our discussion of modular clauses relating to data protection, often found in a GDPR data processing agreement that comprises part of the Data Submission Agreement.

Description of the services

- purpose.
- overall description.
- further specification.
- user support.
- service availability requirements (e.g., guarantees of service levels).
- error response times and procedures (e.g., responding to critical errors).
- the associated fees that will be charged (where applicable).
- Data Provider requirements to ensure software necessary to enable connection to the infrastructure.
- backups.

General service-related obligations (may overlap to some extent with data protection clauses)

- general confidentiality / non-disclosure obligations (not specific to data protection/personal data but as a general duty of the Data Hub as a service provider).
    - Duty must be extended to staff.
    - Duty must be extended to subcontractors.
- security obligations (e.g., generally accepted in the industry) to ensure confidentiality, prevent unauthorised access, and to protect against unwanted modification or erasure of data, and against software viruses affecting the Data Provider's IT environment. E.g.,
    - ISO/IEC 27001 "Information Security Management" certification.
    - Logical separation of the Data Provider's data from any third party data.
    - Access by Data Hubs's employees only where necessary to provide the services.

- right of the service provider to use subcontractors, if any, e.g., and any conditions relation to notification periods and extending obligations to subcontractors.
- term and termination of the service agreement.
- applicable standard (ISO IEC 20000 “Information technology — Service management”).
- applicable law (including law based on extraterritorial jurisdiction applicable to the service provider).
- competent courts.
- dispute resolution.
- limitation of liability e.g.,
  - no Data Hub liability for any loss or damage resulting from the Data Provider’s use of the Services.
  - no Data Hub liability for third party IP rights in software.

<u>Scientific, commercial, and/or business relationship between the Data Provider and Data Hub</u>

- no ownership of Data Provider data is transferred to Data Hub. Data Provider grants Data Hub a license to process in order to provide the services.
- Data Provider must protect confidential business information of the Data Hub.
  - E.g., confidential security documents provided by Data Hub to Data Provider.

<u>General context of GDPR data processing agreement</u>

- This is a GDPR data processing agreement that authorizes the Data Hub to process personal data on behalf of the Data Provider as necessary to provide the Services (specified in the Service Agreement).
- [OPTIONAL] general description of the overall mandate of Data Hub (e.g., to provide an environment for researchers to be able to securely manage and provide access to data; to securely analyse data).
- [OPTIONAL] specific description of the personal data processing operations that will be provided (often selected from a generic checklist).
- for the performance of the services, the Data Provider makes the following data available to the Data Hub (often specified in an Appendix to the DPA).
- the Duration of processing (typically the same as the duration of the Service Agreement).

<u>Obligations of the Data Provider (as controller)</u>

- Deliver to the Data Hub the data referred to in clause 2 of this document.
- Carry out the corresponding prior consultations.
- Ensure, prior to and throughout the processing, that the Data Hub complies with the GDPR.
- Supervise the processing, including, where appropriate, carrying out inspections and audits.
- [OPTIONAL] Data Provider must protect the Data Hub’s confidential security documentation that is provided by the Data Hub to the Data Provider.

<u>Data Hub duty to follow instructions</u>

- Data Hub duty to only process data according to the Data Provider’s Instructions [and never for another purpose or the Data Hub’s own purpose].
  - Exception in the case of a Data Hub processing data in order to fulfill a legal obligation (with an obligation to notify the Data Provider about the processing to the degree legally permitted).

- Obligation to notify Data Provider if instructions conflict with applicable laws.

Data Hub duty of confidentiality

- Binding on Employees and others who are authorized to process personal data.
- Guarantee that its employees, as well as the persons authorised to process personal data, undertake expressly and in writing to respect confidentiality and to comply with the corresponding security measures, of which they must be duly informed. [or are required by law].
- Documenting compliance of this.
- Guarantee the necessary training.

Data Hub data security obligations

- [DEFAULT] Data Hub shall take appropriate Technical and Organisational Measures...
- [AND/OR] Data Hub shall take the following minimum security measures, including:
    - pseudonymise, encrypt data,
    - restore availability after incident,
    - user authentication, logging,
    - limiting # and access of system admins, and
    - monitor effectiveness; penetration testing; conduct (regularly updated) risk analysis.
  - [OPTIONAL] Data Hub adherence to code of conduct or certification mechanism.
  - [OPTIONAL] Data Hub freedom to adopt alternative security measures (that meet or exceed commitments).
- Data Hub must document its security policy and risk assessments, and make this information available to Data Provider on request [overlaps with assistance obligations below].
- Data Hub must report security incidents in a timely fashion (and no later than 72 hours), to the appropriate contact point,
  - together with all relevant information for the documentation and communication of the incident, including:
    - nature of the breach (e.g., categories and # of affected data subjects/records),
    - possible consequences, and
    - measures taken or proposed to be taken to remedy the breach / mitigate negative effects.
  - [OPTIONAL] Data Hub must have/document a contingency/continuity plan in case of serious security breach, and provide to Data Provider on request.
  - Data Hub must assist the Data Provider to fulfill its responsibility to communicate to supervisory authority and data subjects.
- Security audits
  - Data Hub will regularly implement security audits.
  - Data Hub will document the audits and make them available to Data Provider.
  - Data Provider may perform a security audit on the Data Hub's system/facilities, or request an independent third-party audit (appointed by one or both of the parties).
  - Each party will cover its own costs associated with audits.

Data Hub obligation to return or delete data

- obligation to destroy the data:

- on request of the Data Provider, or
- once the service has been provided / agreement terminated / [30 days after] end of specified retention date.

- obligation to notify the Data Provider of upcoming deletion date.
- obligation to document deletion.
- obligation to certify destruction to the Data Provider in writing.
- [OPTIONAL] however, the Data Hub may keep a copy, with the data duly blocked, for as long as liability may arise from the performance of the service.
- Survival of obligation to return/delete data after termination of agreement.

Data Hub obligations when engaging a sub-processor.

- [DEFAULT] outsourcing of the processing of personal data by the processor shall not be permitted without prior approval of the Data Provider.
- [OR] Data Provider generally authorizes the Data Hub to use a sub-processor.
  - ...record-keeping and obligation to notify, following a notice period, the Data Provider of any changes [often there is a web link provided listing subcontractors].
  - the sub-processor must be subject to a written agreement extending all obligations of the processor.
  - the Data Hub will be responsible to verify sub-processor compliance.

Data Hub obligations when transferring personal data to third countries or international organisations

- [DEFAULT] Data Hub shall not transfer any personal data to third countries, except under instructions of the Data Provider.
- [OR] Data Hub shall guarantee that tan adequate level of protection of privacy are in place in accordance with the applicable personal data regulations, including that there is a lawful transfer mechanism and that that the necessary additional technical, organisational and/or legal measures have been implemented.

Assistance w/ data subject rights

- Data Hub shall assist to respond to data subject requests to exercise rights:
  - any requests directed to Data Hub must be immediately (within 1 working day) communicated to the Data Provider (contact point usually provided in text or appendix), along with information relevant for resolving the request.
  - duty is applicable only to the extent possible and appropriate considering the nature and scope of the processing.

Accountability / record-keeping / duties to assist

- Data Hub obligation to assist with accountability.
- Data Hub must keep a written register of all categories of processing activities carried out on behalf of the Data Provider.
- it shall collaborate with the Data Provider for the identification of the information to be included in its register of processing activities.
- Support the Data Provider in carrying out data protection impact assessments, where appropriate.

Miscellaneous

- Data Hub prohibition to Link/Re-identify/ reverse the pseudonymisation procedure.

- Data Hub's obligation to provide its Data Protection Officer's contact details.
    - Designate a data protection officer in the cases provided for in Article 37 of the GDPR and communicate his/her identity and contact details to the data controller.

<u>(Disclaimer of) warranties and (limitation of) liability</u>

- Data Provider - legal compliance (data protection).
- Data Provider – responsibility to have consent/legal basis/ethics approval.
- Data Provider – anonymisation/pseudonymisation.
- Data Provider – encryption at rest/in transit.
- Data Provider – responsibility to verify Data Hub's technical and organisational measures.

<u>Term and termination</u>

- term (e.g., last signature on the Service Agreement).
- termination: e.g., as long as the data processor manages personal data on behalf of the data controller pursuant to the service agreement (which will have clauses on voluntary termination without cause with notice, and termination with cause including breach of data processing agreement).
- survival of clauses after termination.
    - e.g., duty of confidentiality.

5 Data Hosting Agreements

In the Data Submission Agreements section above, we considered a Data Hub (data processor) that provides repository services to a Data Provider (data controller). In addition to repository services, Data Hubs can act as data access intermediaries, and play a valuable role in streamlining data access processes across a network consisting of many Data Providers and many Data Users. The Data Hub may for example establish a common access policy, centralize data access requests and reviews, and/or implement a single Data Access Agreement even where data is accessed from multiple Data Providers. The Data Hub acting as an access intermediary may also be in charge of monitoring or reporting about data access and use. In this section, we focus on different types of relationships and agreements between Data Providers and Data Hubs, who play different respective roles with regards to granting data access to Data Users.

5.1 List of Examples/Templates Reviewed

- BBMRI, Data Access Policy
- BBMRI-ERIC, Data Protection Policy – Colorectal Cohort
- ELIXIR-Luxembourg, Hosting and Processing Agreement ("General Terms of Services") (v 2.2 October 2020)
- European Platform for Neurodegenerative Diseases (EPND), Material and Data Transfer Agreement Template (MDTA)
- EOSC Life, COVID-19 Repository Data Sharing Policy (20 September 2021).

5.2 Data Hosting – Controller-Processor [C-P]

<u>Description</u>

The Data Provider has full control over whether or not to grant access to a particular Data User. The Data Hub only grants access to a particular Data User for a particular research project upon the instruction of the Data Provider or the Data Provider's designated Data Access Committee.

- Data Provider = controller for granting access; Data Hub = processor for granting access.
- The Data Submission Agreement (and GDPR data processing agreement) above can essentially be extended to include clauses describing the service of granting access to Data Users on instruction from the Data Provider.
- E.g., European Genome-Phenome Archive.

Modular Clauses

- Data Hub only grants access to data on the instruction of the Data Provider.
- Data Provider's Data Access Committee makes decisions to grant access.
- Data Provider must establish a Data Access Agreement template, and must execute the agreement directly with the Data User.
- Data Provider is responsible to monitor Data Users under its Data Access Agreement.

5.2.1 Data Hosting – Joint Controllership [JC]

Description

The Data Provider provides clear criteria to the Data Hub describing the conditions under which access may be granted. The Data Hub (or its Data Access Committee) and the Data Provider can influence the decision to grant access to a particular Data User for a particular project if it determines that the criteria are met.

- the Data Provider and the Data Hub participate jointly in data governance = joint controllers.
- they establish a Data Hosting Agreement (including a joint controllership agreement).
- e.g., Luxembourg Data Hub; EOSC-LIFE COVID-19 Repository.

Note: The Data Hub is typically also the entity providing the general repository services to the Data Provider as a processor. So the Data Provider and Data Hub will typically establish a Data Submission agreement for those services (where the Data Provider = controller, Data Hub = processor). A different GDPR relationship and agreement will to apply for granting data access and associated processing.

Data Hosting Agreement - Clauses

- Data Provider is responsible for defining and ensuring compliance with the access policy, including:
    - a description of the permitted purposes/types of research projects,
    - criteria about what types of researchers/research organizations can access data, and
    - the means of access by approved users (e.g., data download, access in an SPE).
- Data Hub and Data Provider are jointly responsible for establishing a Data Access Committee according to defined Standard Operating Procedures (detailed in an Appendix to the Data Hosting Agreement).
- [DEFAULT] Data Hub is responsible to review data access requests to determine compliance of the requests with the data access policy established by the Data Provider.
- [OR] Data Hub makes a preliminary recommendation to grant access that is communicated to the Data Provider(s), who may veto the decision with a given time frame [e.g. 10 days].

  - The Data Provider(s) will provide a justification for overturning the Data Hub's decision.
- Data Hub is responsible to establish a standard Data Access Agreement template and to execute an agreement with approved Data Users as a condition of access.
  - [where applicable] The Data Provider is responsible to report any data-specific data use conditions as part of the Access Policy.
- Data Hub is responsible to monitor data users and to report to the Data Provider (or public) about access decisions and the results of research uses.

<u>Joint Controllership Agreement</u>

- the joint aim of the parties is to make data available / to provide access to data according to the Data Hosting Agreement.
- through this agreement, the parties seek to clarify their respective data protection responsibilities.
- except where this agreement allocates responsibility for compliance with obligations under data protection law only to one Party, both parties will comply with their respective obligations under applicable data protection law.

<u>Legal Basis / Purpose Limitation</u>

- The Data Hub shall process personal data solely for the joint purpose of providing access according to the Data Hosting Agreement and will not process otherwise without written consent of the Data Provider.
- Both parties warrant they have a valid legal basis for processing personal data under this agreement [the legal basis of each party must be specified in text or in an Appendix].
- [Where consent is the legal basis] the Data Provider shall notify the Data Hub without undue delay if a Data Subject withdraws consent on which the processing is based.

Considering that the Data Hub does not have a direct relationship with the relevant Data Subjects whose Personal Data are Processed hereunder, the Data Provider agrees to take on responsibility for the following obligations under applicable Data Protection Legislation:

- the Data Provider is responsible to ensure the data subjects are notified according to GDPR Arts 13/14.
- the Data Provider shall be the principal point of contact for enquiries from Data Subjects and handling rights.
- Data Provider is responsible for any legally required notifications to the affected Data Subjects as a result of a Personal Data Breach.
- Rights the Data Provider is responsible for addressing Data Subject Rights.

Considering that only the Data Hub actually processes the Personal Data, or directly oversees this processing, the Data Hub agrees to take on responsibility for the following obligations under applicable Data Protection Legislation:

- Security:
  - [DEFAULT] the Data Hub is primarily responsible to ensure appropriate GDPR security requirements are met when providing access.
  - [OR] Data Provider may establish specific requirements.
- Use of processors:
  - [DEFAULT] the Data Hub is primarily responsible for the choice of processor.
  - [OR] Data Provider may prohibit the use of processors, or insist on providing specific authorization for engaging processors.
  - Data Hub shall ensure (sub)processors only process data based on its instructions.

- Third country transfers:
  - [DEFAULT] the Data Provider may prohibit third country transfers, or may require specific authorisation, and/or may impose conditions e.g., the applicable legal mechanism.
  - [OR] the Data Hub is responsible for ensuring any third country transfers comply with the GDPR.
- Data Subject Rights:
  - Data Hub shall notify Data Provider immediately of any enquiries made by Data Subjects directly to the Data Hub and shall not directly respond unless required by law or authorized by the Data Provider.
  - Data Hub will have procedures for assisting the Data Provider in response to queries from Data Subjects, and shall provide all information necessary to respond to any inquiry.
- Data Breach Notification Obligation:
  - Data Hub shall notify the Data Provider of a breach.

Responsibilities of both Parties:

- Accountability:
  - to consult with a Data Protection Officer (DPO) and to conduct a Data Protection Impact Assessment (DPIA) where required.
  - to maintain a record of all categories of Processing activities. The parties shall make their record available to each other for the purposes of demonstrating compliance and to the Supervisory Authority on request.
  - to be responsible for any legally required notifications to the competent supervisory authority/ies as a result of a Personal Data Breach. Each Party shall inform the other in advance of making any notification to the supervisory authority/ies where it is reasonably practicable to do so and it is consistent with their legal duties.

Applicable Law:

- National law of the Data Hub.
- OR National law of the Data Provider.

5.2.2 Data Hosting – Controller-to-Controller Transfer [C-C]

Description

A Data Provider transfers data to a Data Hub, who independently pursues the aim of making data available to Data Users for research projects.

- Data Provider = upstream controller for primary purpose. Data Hub = independent, downstream controller for hosting and providing access to data.
- The parties establish a data transfer agreement (controller to controller agreement).
- E.g., under European Health Data Space legislation proposal would establish Data Access Bodies with legislative authority to make independent access decisions for data held by multiple Data Holders. The US NIH dbGaP also functions in analogous way.

Modular Clauses

- The Data Hub establishes Data Access Policy. The Data Provider(s) warrants data can be made available according to the access policy in compliance with applicable laws, approvals, and consents.
- The Data Hub's Data Access Committee makes decisions to grant access, subject to any regulatory restrictions established by the Data Provider in the Data Transfer Agreement.

- The Data Hub must establish a Data Access Agreement template and must execute the agreement directly with the Data User.
- The Data Hub is responsible to monitor Data Users under its Data Access Agreement.

6 Agreements Governing Data Analysis in Secure Processing Environments

A final scenario to consider is where a Data Hub provides a SPE in which a Data User remotely accesses data, and conducts an analysis on data for a research project. We focus on the default use case where a Data Hub collocates repository services and SPE services. Note that SPE services may also be provided by an external cloud platform, or by the Data Provider itself (an on-premise SPE). We address only a default use case in which a Data User (or several) enter into an agreement with an (external) Data Hub to allow the Data User to analyze data within an SPE as part of a research project. In this use case, the Data User (or several) is the controller for the research project, and the Data Hub providing the SPE services is a processor acting on behalf of the Data User (or Users). Therefore the agreements between these parties will typically comprise a terms of use (for the SPE), and a data processing agreement between the Data User and the Data Hub.

Notably, in our use case, the Data Provider is not a party to the agreements, though the Data Provider is typically the source of the requirement that the the Data User access data in a SPE (by requiring this in the Data Access Agreement). In other use cases the Data Provider may host an on-premise SPE, and thus will replace the Data Hub. This section also assumes that neither the parties providing data nor the parties providing analysis environments are joint collaborators on the research project (supporting the interpretation of the controller-processor relationship).

Such analysis may also be scaled across multiple SPEs — hosted by different cloud platforms, Data Hubs, or Data Providers — in the case of a federated network. In a federated network, an additional coordinating body may be needed to distribute the Data User’s analysis workflow to different Data Hubs or Data Providers, and to assemble the local results from each site for the user (e.g., Germany’s Medical Informatics Initiative). In such a case, the coordinating body may act as a processor, with the Data Hubs/Providers acting as sub-processors for the analysis.

6.1 List of Examples/Templates Reviewed

- de.NBI-Cloud:
  - Terms of use.
  - Joint controllership agreement (between all de.NBI-Cloud sites; for identifying user data only, as they need to be shared between the de.NBI-Cloud main office in Bielefeld and the processing de.NBI-Cloud site).
  - Data Processing Agreement (individual for each de.NBI-Cloud site, between processing de.NBI-Cloud site and external cloud user, mainly for sensitive project/research data).
  - Portal Privacy Policy (de.NBI-Cloud main office in Bielefeld).
  - Cloud Privacy Policy (identical for all sites).

6.2 Modular Clauses

The clauses of the Terms of Use between the Data User and the Data Hub providing the SPE are beyond the scope of this deliverable. The clauses of the accompanying data processing agreement between the Data User and the Data Hub will be similar to those found in the Data Hosting Agreement section above.

7 Conclusion: Opportunities and challenges to adopting harmonized agreements

Many projects have highlighted the value of standardising or harmonising contracts, to provide clarity, certainty and predictability, and to facilitate negotiations. In practice, however, institutions and their legal departments typically insist on using their own templates or developing their own agreements, sometimes on a case-by-case basis. Many of the challenges of achieving harmonisation have to do with different data sharing contexts: different data types, types of actors (e.g., academic v industry v healthcare institutions), jurisdictions involved (and applicable laws), different relationships between the parties, different sectoral norms (proprietary vs open science). This challenge is especially relevant in the case of analyses on data federation between different data providers and countries of the union, as it multiplies the complexity of the legal and organisational contexts.

While the GDPR has been in force for several years, given its relative novelty, it remains a disruptive force in terms of contractual fragmentation. There are still competing GDPR interpretations (e.g., assignment of controllership, legal basis, identifiably) that impact on data sharing agreements. The GDPR has also significantly increased the due diligence surrounding contract execution – before (due diligence, negotiation, signing), and after (monitoring of obligations).

Specially for data sharing agreements from a data protection perspective, these agreements (or more specifically the data sharing clauses) may not always be looked at as purely contractual. Data sharing agreements between independent controllers are often more a form of accountability tool – clarifying the processing flows, the statutory obligations and demonstrating compliance – than a privative contract. Of course these data protection agreements or clauses may always be combined with other agreements or clauses that are indeed of a contractual nature.