Work Package 1, D1.2

Project Name:	Disc4All 955735		
Date:	12 / 12 / 2021	**Release:**	Final
WP Leader (WPL):	INSILICOTRIALS		
WP Co-leader (WPCL):	AQUAS		
Reviewer 1	Marc-Antonio Bisotti		
Reviewer 2	Salas Fernandez, Tomas,		
Document Number:	D 1.2		

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
12 / 22 / 2021	N / A		N
1` / 12 / 2021	12 / 22 / 2021	Marc-Antonio Bisotti	Y
1 / 17 / 2021	12 / 22 / 2021	Salas Fernandez, Tomas	Y

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

Work Package Authorisation	
Title	WP 1 Leader/ESR Supervisor
Person Authorised[1]	Marc-Antonio Bisotti
Date[2]	22.12.2021

Description & Deliverables

(A description of the work to be done)

Techniques, Processes and Procedures

(Any techniques, tools, standards, processes or procedures to be used in the creation of the specialist products)

Problem Handling and Escalation

(This refers to the procedure for raising issues and risks)

1 The name of the WPL

2 The date of the agreement between the Coordinator and the WPL/person authorised

Approval method

(The person, role or group who will approve the completed products within the Work Package, and how the Coordinator is to be advised of completion of the deliverables and Work Package)

Work Package Acceptance	
Person Accepting[3]	
Date[4]	
Assessment and feedback	

3 The Coordinator or other person accepting the work package on the Coordinator's behalf

4 The date of acceptance

Disc4All Data Governance Framework

Table of Contents

Abstract

Data is a critical asset Disc4All has, and it affects the decision-making processes of the project. Different organizations have designed different ways to deal with the different challenges that data brings about such as governance programs. Researchers in most fields first review how the people understand the data and various definitions of data governance, mission, vision and goals, change and issue management and regulatory compliance. The main objective of this document is to use a similar approach to come up with a framework that can be used by Disc4All researchers to maximize the value from data through improved data management practices which aid in data intensive decision making and strategic planning.

Introduction

Data governance is a collection of processes, roles, policies, standards, and metrics that facilitate the effective and efficient use of information enabling the organisation to achieve its goals [1]. The data governance operation will be an internal function to support decision-making by partners at all levels within the consortium. It will be applicable to all processes and systems that collect, analyse, disseminate, and store data; and includes anything that affects the consortium's ability to perform these functions. The ability of Disc4All to use data for decision-making is reliant on the availability, usability, integrity, and security of the data.

Disc4All mainly utilizes primary data from Northern Finland Birth Cohorts and Twins UK data infrastructures after signing a data transfer agreement. The Northern Finland Birth Cohort 1966 Study was started in the year 1965 on expectant mothers. Data on the individuals born into this cohort was collected from the 10th to the 16th gestational week as well as their mothers and, to a lesser extent, fathers. The cohort included 12055 mothers and they had 12068 deliveries (13 women delivered twice). The data was also collected at the ages of 1, 14, 31 and 46 using postal questionnaires, hospital records and national register data as shown in the image below [2].

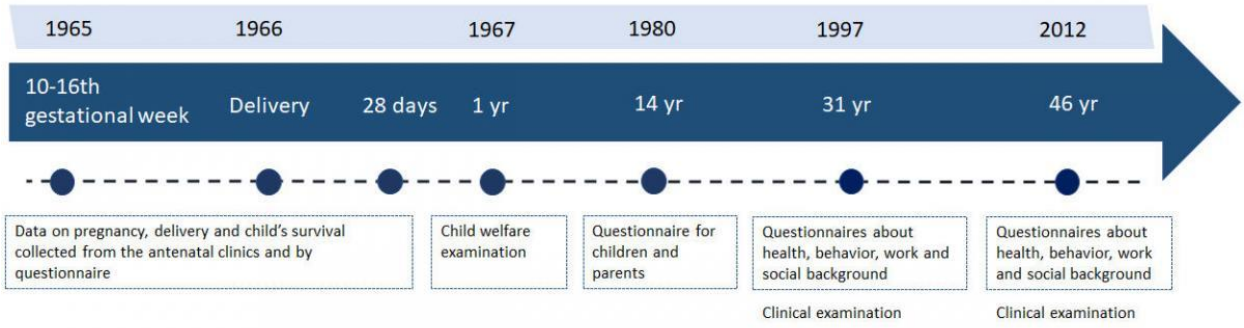

Figure 1 NFBC Data Collection Timeline

Twins UK is an extensive clinical, physiological, and behavioural and lifestyle data, including biochemical and genetic data, available to researchers after a lengthy data transfer agreement. Many data types have been collected at multiple longitudinal time points. Available sample types include: DNA, cell lines, serum, plasma, stool and urine. All samples have been genotyped using the Infinium assay (Illumina, San

Diego, USA). They also hold gene expression data (fat, LCL, skin). Genetic data available include GWAS Illumina, gene expression, sequence data and metabolic data [3]. Before processing of any of the above sources, users have to sign a data processing agreement. See template attached.

1.0 Readiness Assessment

To gauge the level of maturity of the current level of the data governance operation, a data maturity assessment will be done by the data controller. The Data Maturity Model is a set of tools for planning and sustaining a strategic programme such as the data governance program. It tracks the state of a program over time consistently. Because the implementation and full maturation of a data governance program is a multiyear effort, the intermediate maturity states can be used to construct a program roadmap [4].

The governance maturity assessment should be focused on 6 areas i.e. policy, standards & strategy, data quality, compliance, integration, data warehousing / business intelligence and management support [5]. The contents of the focus areas should be based on 11 data governance dimensions, with a customized set of questions that capture each dimension's characterizing elements. The 11 data governance dimensions are:

1. Data Risk Management and Compliance. A method by which risks are identified, qualified, quantified, avoided, accepted, mitigated, or transferred out;
2. Value Creation. A process by which data assets are qual-ified and quantified to enable the business to maximize the value created by data assets;
3. Organizational Structures and Awareness. The level of mutual responsibility between business and IT, and the recognition of fiduciary responsibility to govern data at different levels of management;
4. Stewardship. A quality-control discipline designed to ensure the custodial care of data for asset enhancement, risk mitigation, and organizational control;
5. Policy. The written articulation of desired organizational behavior;
6. Data Quality Management. The methods used to mea-sure, improve, and certify the quality and integrity of pro-duction, test, and archival data;
7. Information Lifecycle Management. A systematic policy-based approach for

information collection, use, reten-tion, and deletion;

8. Information Security and Privacy. The policies, practices, and controls used by an organization to mitigate risk and protect data assets;
9. Data Architecture. The architectural design of struc-tured and unstructured data systems and applications that makes data available to appropriate users;
10. Classification and Metadata. The methods and tools used to create common semantic definitions for business and IT terms, data models, and repositories;
11. Audit Information Logging and Reporting. The organizational processes for monitoring and measuring data value and risks as well as the effectiveness of data governance.

The response scale of each question comprises of five possible answers (1) Performed, (2) Managed, (3) Defined, (4) Measured or (5) Optimized. Once the results have been submitted, the cumulative score should be obtained by averaging the score of all questions [5].

1.1 Mission, Vision and Goals

Mission: To ensure that the highest quality data is collected, analysed, and made available to key stakeholders through coordinated efforts for the purposes of improving efficiency, protecting privacy, and enabling better decision-making.

Vision: To govern and protect all Disc4All data and information wherever it resides supporting the needs of the consortium and its members as well as needs of the partners we collaborate with.

Goals: Must be met in the near-term to position the consortium to meet its mission. These goals will be the data governance program's initial focus and all effort and resources will be directed toward their successful completion. They include:

- **Data Privacy.** Protecting the privacy of data. Identifying and labelling all data elements that contain personally identifiable information and creating efficient and effective policies around data access, data use, and data release.
- **Data Accessibility.** Providing appropriate access to data across Disc4All. Creating policies and procedures that give Disc4All researchers appropriate access to data based on job function, while maintaining compliance.

- **Data Content.** Understanding all the data collected and used by Disc4All. Each research area should gain a better understanding of its respective data through the process of documentation.
- **Application Use.** Increasing capacity for extracting data from existing applications. Research units should understand the functionality of the applications they use to collect data. This includes gaining the ability to extract data from those applications for the purposes of producing reports.
- **Data Manipulation.** Increase Disc4All's capacity to manipulate data. Provide training to Disc4All researchers in order to expand the ability to query, sort, filter, organize and present data that meets the needs of stakeholders.
- **Data Definitions.** Define every data element collected by Disc4All. Create a consistent format for data definitions and create a definition for every data element collected by Disc4All that is clear and consistent with the chosen format.
- **Data and IT Strategic Plan.** Create a data and IT Strategic Plan and communicate it across the consortium. Executive leadership should create a clear and strategic plan that clearly outlines the goals for and path toward improving Disc4All's data and IT initiatives.
- **Resource Management.** Prioritize and increase transparency around the use of IT resources. Develop consistent processes for initiating new projects and enhancements and for governing data collection and dissemination. Include all Disc4All researchers in these processes in order to properly track resources and create transparency around their use.
- **Research Rules.** Establish research rules that ensure all of Disc4All's data conforms to identified standards of quality, consistency and shareability. Develop, document, publish and implement research rules that clearly outline actions and constraints around creating, updating, deleting, and distributing data.

1.2 Governance Strategy and Model

To get the most value out of data, we will adopt a Federated approach to support a centralized strategy to processes and systems for data creation, storage, maintenance, and disposal where one data governance organization will co-ordinate with multiple research units to maintain consistent definitions and standards, but with decentralized execution. This will be the basic structure of responsibility for master data management, while data governance policies define the people, processes, and technologies for managing data [6].

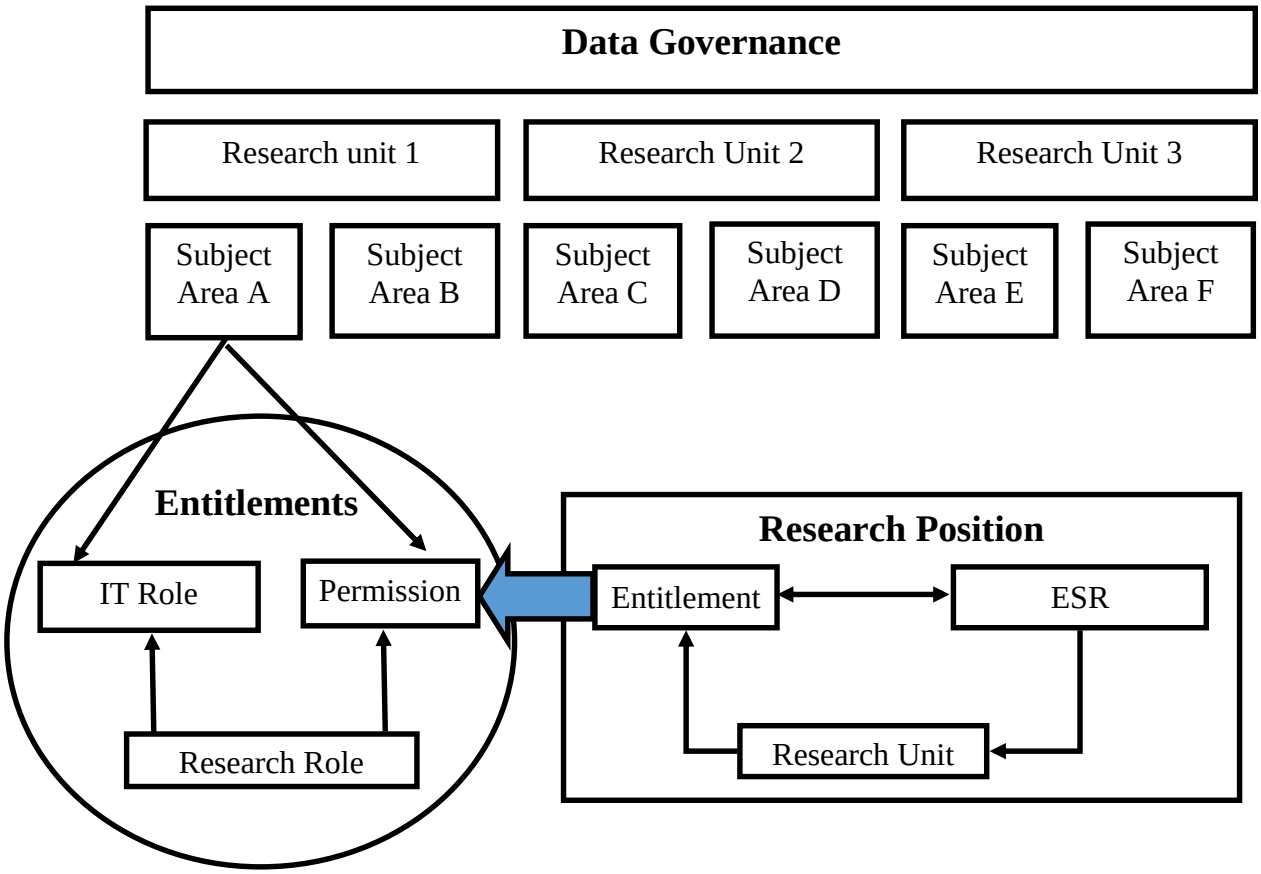

Figure 2 Disc4All Federated Data Governance Strategy

This data governance model will have activities at different levels within the organization as well as a separation of governance responsibilities within organizational functions and between technical and research areas. The figure below illustrates how the various areas work together to carry out data governance.

Element Definition

Key Roles definition

a) The Chief Data officer is responsible for developing and governing data and information strategy to drive research decisions and growth. He/she will develop data procedures and policies, and work closely with various consortium partners to collect, prepare, organize, protect, and analyse data assets while ensuring that the consortium meets industry best practices.

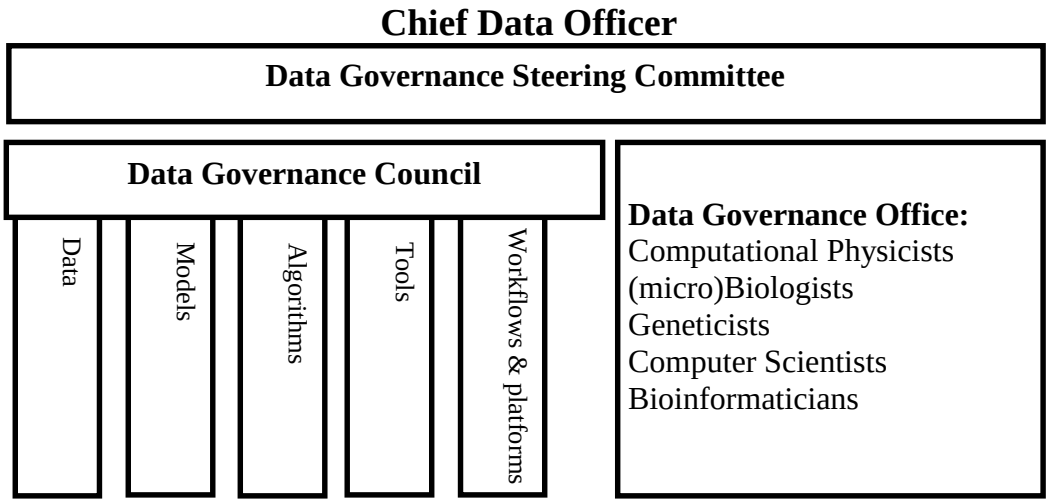

Figure 3 Disc4All Data Governance Model

b) Data Governance Steering Committee is the primary and highest authority organization for data governance in Disc4All, responsible for oversight, support of data governance activities.

b) Data Governance Council (DGC): Manages data governance initiatives (e.g., development of policies or metrics), issues, and escalations. Consists of executive according to the operating model used.

c) Data Governance Office (DGO): Ongoing focus on enterprise-level data definitions and data management standards across all Knowledge Areas. Consists of coordinating roles that are labelled as data stewards or custodians, modelers, analysts, architects, and data owners.

1.3 Operating Framework

While ultimate authority and responsibility lie with the Project Co-ordinator, data governance decisions involve many people.

- Input is received from consortium partners and the chief data officer according to the consortium's agenda as needed and channelled to the Data Governance office through the Data Governance Steering Committee.
- Data Governance Office convenes as needed to trouble shoot and find potential solutions for data issues, determining necessary changes for compliance with standards and regulations and make detailed recommendations to the data governance council.
- The Data Governance Council then review the solutions suggested solutions and give a go ahead for data development of these solutions to be implemented and once ready they manage the process of moving the solutions to production first by conducting pre-tests and performance tests to make sure nothing will be affected.
- The Data Governance steering committee give the permissions for the Disc4All platform to be changed or updated. They receive requests for moving solutions to production from the Data Governance Council and they are responsible for provisioning needed rights and accesses to the platform.
- The Chief data officer then updates the Project Co-ordinator on the platform status and gives any needed official communication.

1.4 Data Governance Meeting Schedule

Project co-ordinator and chief data officer:

Governance items will appear on the chief data officer's agenda as determined by the project co-ordinator.

Data Governance Steering Committee:

The Data Governance steering committee will meet at the request of the chief data officer's request, based on the number of items on his agenda.

Data Governance Council:

The Data Governance Council meets monthly. Meetings are facilitated by the data governance coordinator.

Data Governance office:

The Data Stewards Workgroups and External Advisory Committees meet on an ad hoc basis. Meetings are organized and facilitated by the data governance coordinator.

2.0 Regulatory Compliance (Legal framework)

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros [6].

With the GDPR, Europe is signalling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence. The regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized research units [6] . The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) [7].

To provide assurance that privacy and data protection have been highly upheld, a data protection impact assessment (DPIA) is imminent. By providing a structured way of thinking about the risks to data subjects and how to mitigate them, DPIAs help organisations to comply with the requirement of 'data protection by design' [8].
The assessment contains:

a) a systematic description of the envisaged processing operations and the purposes of the processing;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 of Article 39 of the Regulation 2018/1725; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. Data Processing Agreement Template

Where necessary, the data controller shall carry out a review to assess if the data processing is being performed in accordance with the data protection impact assessment, at least when there is a change of the risk represented by processing operations [8]. According to the GDPR, most important are the rights of the data subject where they have a right to erasure, right of access, right to rectification, right to object, right to restrict processing, among many more. [9]

The data controller will be using a GDPR checklist with several recommendations for securing the project, protecting subject data, and avoiding costly fines for non-compliance [10].

a) **Lawful basis and transparency:** The data controller will conduct an information audit to determine what information the project processes and who has access to it, have a legal justification for having provided clear information about the project's data processing and legal justification in the privacy policy [12].
b) **Data security:** The data controller shall take data protection into account at all times, from the moment they begin developing a product to each time they process data. Encrypt, pseudonymize, or anonymize personal data wherever possible. Create an internal security policy for your team members, and build awareness about data protection. Know when to conduct a data protection impact assessment, and have a process in place to carry it out. Have a process in place to notify the authorities and your data subjects in the event of a data breach [12].
c) **Accountability and Governance:**
   The Data controller shall be responsible for ensuring GDPR compliance across your organization, shall sign a data processing agreement between the project and any third parties that process personal data on the project's behalf.

If you process data relating to people in one particular member state, you need to appoint a representative in that country who can communicate on your behalf with data protection authorities. The GDPR and its official supporting documents do not give guidance for situations where processing affects EU individuals across multiple member states. Until this requirement is interpreted, it may be prudent to designate a representative in a member state that uses your language. Some organizations, like public bodies, are not required to appoint a representative in the EU [12].

d) **Privacy rights:** The data control shall make it easy for the data subjects to request and receive all the information the project has about them, correct or update inaccurate or incomplete information, request to have their personal data deleted, ask you to stop processing their data, receive a copy of their personal data in a format that can be easily transferred to another company and object to you processing their data [11]

3.0 Data Standard Recommendations

Data standards are the guidelines that define the approach and practices for developing, approving and instituting compliance for data representation, data access and data distribution standards [9]. Standards should be explicitly described, be aligned with existing and provisional standards proposed by national and international bodies, should be able to be easily used [10].

According to a health data user and custodian surveys carried out by Health Data Research UK's (HDR UK), the majority (64%) of health data users said they have basic or no data standards expertise, with much greater stated expertise among the industry users compared with the academic researchers.

- 85% of users were in support of a core set of data standards to enable health data research
- Both users and custodians highlighted the importance of open standards and clinical terminologies

- Currently data users are using a wide range of data standards, with greatest alignment around Clinical Data Interchange Standards Consortium (CDISC), Observational Medical Outcomes Partnership (OMOP)
- Data custodians also currently support a wide range of data standards, with OMOP and HL7 FHIR the most frequently supported [11].

After putting all the above into consideration, they recommended that for organisations considering establishing standards such as data models and messaging standards for research purposes, the use of OMOP and/or HL7 FHIRv4 as standards/specifications for research which can be adopted most widely by both users and custodians for a range of purposes. [11].

However, for organisations already using different standards or models HDR UK recognises that there are resourcing and cost implications for each organisation and potential information loss associated with transition to OMOP and HL7 FHIRv4. Ultimately, the appropriate standards should be selected to support the specific use cases and capabilities.

Disc4All however is in a unique position because of the research angle we are undertaking. Putting this into consideration, FHIR does not adequately structure all the data types we are intending to work with and does not have mechanisms for storing results. It however has the best data model for the primary data. I therefore recommend the use an imaging research platform XNAT for the extra features but with the FHIR data model to store primary data to be worked on and for extra structures for AI/ ML/ M&S and privacy (data location, anonymization/ pseudonymization) features.

Conclusion

This document outlines a set of rules that define how data is processed across the organization to ensure privacy, compliance and maximum utilization of data. The first step involves doing a data maturity assessment to assess the level of data governance in the organization. This can be done periodically to see which measures

need to be taken to improve or degrade the state.

The second step is a feedback loop, where the data protection officer receives issues from the consortium and channels it to the data governance office through a meeting with the data governance steering committee. The data governance office then finds solutions for the data issues and makes detailed recommendations to the data governance council for approval, after which they implement and deploy the solutions.

The third and last step is conducting a data protection impact assessment to ensure regulatory compliance of data processing operations. The three steps above will enable the project to get maximum value from the data it holds. Check the Data Protection Impact Assessment linked.

References

[1] "The Definitive Guide to Data Governance," [Online]. Available: https://info.talend.com/rs/talend/images/WP_EN_DG_Talend_DefinitiveGuide_DataGovernance.pdf?mkt_tok=MzQ3LUlBVC02NzcAAAGCBGwSxZEUNSMRauQbf66Dbh-9DCaRVXVllc9VO1ni5A74BAse8NXTCMwDNmX6kdT2Nsfrk06TzyssfQr8XMb3Wt-6HzuZYsreUuvmXgCQtR7CjTP8.

[2] "NFBC 1966 data collection," University of Oulu, [Online]. Available: https://www.oulu.fi/nfbc/node/19663.

[3] "TwinsUK Resources for Researchers," Department of Twin Research & Genetic Epidemiology, King's College London, [Online]. Available: https://twinsuk.ac.uk/resources-for-researchers/our-data/.

[4] "DATA GOVERNANCE MATURITY MODEL," [Online]. Available: https://hnu.edu/wp-content/uploads/2020/03/Data-Governance-Maturity-Model.pdf.

[5] G. Thomas, "The Data Governance Framework," The Data Governance Institute.

[6] B. Wolford, "What is GDPR, the EU's new data protection law?," [Online]. Available: https://gdpr.eu/what-is-gdpr/.

[7] GOV.UK, "Data protection," [Online]. Available: https://www.gov.uk/data-protection.

[8] "Data Protection Impact Assessment (DPIA)," EUROPEAN DATA PROTECTION SUPERVISOR, [Online]. Available: https://edps.europa.eu/data-protection-impact-assessment-dpia_en.

[9] "Data Standards," [Online]. Available: https://www.usgs.gov/data-management/data-standards.

[10] "Principles for Data Standards," [Online]. Available: https://www.hdruk.ac.uk/wp-content/uploads/2020/06/200630-Data-Standards-Principles-FINAL.pdf.

[11] "HDR UK – Recommendations for Data Standards," [Online]. Available: https://www.hdruk.ac.uk/wp-content/uploads/2020/06/200630-Data-Standards-Principles-FINAL.pdf.

[12] B. Wolford, "Data Processing Agreement (Template)," [Online]. Available: https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf.

[13] "Data Protection Impact Assessment (DPIA)," [Online]. Available: https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

APPENDIX

1.0 Data Processing Agreement Template [12]

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between

_____

_____

And (the “Institution”)

_____

_____

(the “Data Processor”)
(together as the “Parties”)

WHEREAS

(A) The Company acts as a Data Controller.
(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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).
(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Sub processor;

Data Processing Agreement — Your Institution

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the_____ services the Company provides.

1.1.10 "Sub processor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

Data Processing Agreement — Your Company

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub processor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably

understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws

inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Processor shall provide written certification to Company that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

Data Processing Agreement — Your Institution

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of _____.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Institution	**Processor Institution**
Signature	Signature
_____	_____
Name:	Name:
_____	_____
Title:	Title:
_____	_____
Date Signed:	Date Signed:
_____	_____

1.1 Data Protection Impact Assessment Template [13]

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA