SAGE DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is between Sage Bionetworks (“**Sage**”) and [Institution full name, trading name (if different), official registration number (if any)] (“**Institution**”) and is supplemental to the Sage Terms of Service [add link] [and Self-Managed Plan Agreement or DCC], collectively referred to herein as (the “**Agreement**”). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

| Sage [To be pre-signed] | Institution: |
| --- | --- |
| Name: | Name: |
| Job title, contact details including email address: | Job title, contact details including email address: |
| Address:  2901 Third Ave, Suite 330  Seattle, WA 98121,  United States | Address: |
| Signature: | Signature: |
| Date: | Date: |

**Signature instructions.** This DPA has been pre-signed by Sage. To enter into this DPA, Institution must:

1. complete the table above with signatory information;
2. sign the DPA by [please briefly explain the signatory process that Sage wants to implement, e.g., submit the completed and signed DPA to Sage via email to: [privacyofficer@sagebase.org]].

This DPA will be effective only if executed in accordance with the above instructions, and as of the day that Sage receives the completed DPA from the Institution, or if later, the date of the Agreement.

# Definitions

## In this DPA:

### “**Controller**”, “**Data Subject**”, “**Personal Data Breach**”, “**Processing**”, “**Processor**”, and “**Supervisory Authority**” have the meaning given to them in European Data Protection Law;

### “**Institution Personal Data**” means Personal Data Processed by Sage as a Processor on behalf of Institution or Third Party Controller;

### “**Data Protection Law**” means the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), their national implementations in the European Economic Area (“**EEA**”), including the European Union, and all other data protection laws of the EEA, the United Kingdom (“**UK**”), and Switzerland, each as applicable, and as may be amended or replaced from time to time (“**European Data Protection Law**”) and other privacy and personal data protection laws as amended and replaced from time to time and to which the parties are subject; each as applicable;

### “**Personal Data**” shall be interpreted consistent with the applicable Data Protection Law and includes at a minimum and where applicable “Personal Data” as that term is defined under European Data Protection Law;

### “**Data Subject Rights**” means all rights granted to Data Subjects under Data Protection Law, which may include – depending on applicable law - rights to information, access, rectification, erasure, restriction, portability, objection, the right to withdraw consent, and the right not to be subject to automated individual decision-making;

### “**International Data Transfer**” means any disclosure of Institution Personal Data outside of the country in which the Institution Personal Data was collected;

### “**Services**” means the services provided by Sage to the Institution under the Agreement;

### “**Subprocessor**” means a Processor engaged by Sage to Process Institution Personal Data;

### “**SCCs**” means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended or replaced from time to time;

### “**Third-Party Controller**” means a Controller for which Institution is a Processor; and

### “**UK Addendum**” means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

## Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

# Scope

## This DPA applies to the Processing of Institution Personal Data by Sage, subject to Data Protection Law to provide the Services as outlined in the Agreement.

## The subject matter, nature, and purpose of the Processing, the types of Institution Personal Data and categories of Data Subjects relevant for this DPA are those as set out in **Annex I,** which is an integral part of this DPA.

## The institution is a Controller and appoints Sage as a Processor on behalf of the Institution. The institution is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

## If Institution is a Processor on behalf of a Third-Party Controller, then Institution: is the single point of contact for Sage; must obtain all necessary authorizations from such Third-Party Controller; and undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.

## Institution acknowledges that Sage may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, metric collection, customer support, troubleshooting, improving the Service, creating new products and services, auditing, and compliance with law. Sage is the Controller for such Processing and will Process such data in accordance with Data Protection Law.

# Instructions

## Sage will Process Institution Personal Data to provide the Services in accordance with Institution’s documented instructions. .

## The Controller’s instructions are documented in this DPA, the Agreement, and any applicable statement of work.

## Institution may reasonably issue additional instructions as necessary to comply with Data Protection Law. Sage may charge a reasonable fee to comply with any additional instructions.

## Unless prohibited by applicable law, Sage will inform Institution if Sage is subject to a legal obligation that requires Sage to Process Institution Personal Data in contravention of Institution’s documented instructions.

# Personnel

## Sage will take reasonable steps so that all personnel authorized to Process Institution Personal Data are subject to an obligation of confidentiality.

# Security and Personal Data Breaches

## 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, Sage will implement technical and organizational measures, including the measures listed in **Annex I**I, to ensure a level of security appropriate to the risk.

## Institution acknowledges that the security measures in **Annex II** are appropriate in relation to the risks associated with Institution’s intended Processing and will notify Sage prior to any intended Processing for which Sage’s security measures may not be appropriate.

## Sage will notify Institution without undue delay after becoming aware of a Personal Data Breach involving Institution Personal Data. If Sage’s notification is delayed, it will be accompanied by reasons for the delay.

# Subprocessing

## Institution hereby authorizes Sage to engage Subprocessors. A list of Sage’s current Subprocessors is included in **Annex III**.

## Sage will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.

## Sage will notify Institution prior to any intended change to Subprocessors. Institution may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Sage’s notification of the intended change. Institution and Sage will work together in good faith to address Institution’s objection. If Sage chooses to retain the Subprocessor, Sage will inform Institution at least thirty (30) days before authorizing the Subprocessor to Process Institution Personal Data, and either party may immediately discontinue providing or using the relevant parts of the Services, as applicable, and may terminate the relevant parts of the Services within thirty (30) days.

# Assistance

## Taking into account the nature of the Processing, and the information available to Sage, Sage will assist Institution, including, as appropriate, by implementing technical and organizational measures, with the fulfillment of Institution’s own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

## Sage may charge a reasonable fee for assistance under this **Section 7**. If Sage is at fault, Sage and Institution shall each bear their own costs related to assistance.

# Audit

## Upon reasonable request, Sage must make available to Institution all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested no more than once per year by Institution, and performed by an independent auditor as agreed upon by Institution and Sage. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Institution Personal Data and shall be conducted during normal business hours and in a manner that causes minimal disruption.

## Sage will inform Institution if Sage believes that Institution’s instruction under **Section 8.1** infringes Data Protection Law. Sage may suspend the audit or inspection or withhold requested information until Institution has modified or confirmed the lawfulness of the instructions in writing.

## Sage and Institution each bear their own costs related to an audit.

# International Data Transfers

## Sage and Institution shall comply with applicable Data Protection Law when Processing Personal Data in the context of this DPA, including any International Data Transfer restrictions.

## Institution hereby authorizes Sage to perform International Data Transfers outside the EEA, the UK or Switzerland to any country deemed to have an adequate level of data protection by the European Commission or the competent authorities, as appropriate; on the basis of adequate safeguards in accordance with applicable Data Protection Law; or pursuant to the SCCs and the UK Addendum referred to in **Sections 9.3** and **9.4**.

## By signing this DPA, Sage and Institution conclude Module 2 (controller-to-processor) of the SCCs and, to the extent Institution is a Processor on behalf of a Third-Party Controller, Module 3 (Processor-to-Subprocessor) of the SCCs, which are hereby incorporated, apply to International Data Transfers outside the EEA and Switzerland, and are completed as follows: the “data exporter” is Institution; the “data importer” is Sage; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in **Section 6.3** above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Dublin, Ireland; Annex I and II to Module 2 and 3 of the SCCs are **Annex I** and **II** to this DPA respectively. For International Data Transfers from Switzerland Data Subjects who have their habitual residence in Switzerland may bring claims under the SCCs before the courts of Switzerland..

## By signing this DPA, Sage and Institution conclude the UK Addendum, which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the “Exporter” is Institution and the “Importer” is Sage, their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the “Approved EU SCCs” are the SCCs referred to in **Section 9.3** of this DPA; (iii) in Table 3, Annexes 1 (A and B) and II to the “Approved EU SCCs” are **Annex I and II** respectively; and (iv) in Table 4, both the “Importer” and the “Exporter” can terminate the UK Addendum.

## If Sage’s compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Sage’s control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Institution and Sage will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative standard contractual clauses or UK standard contractual clauses are approved by competent authorities, Sage reserves the right to amend the Agreement and this DPA by adding to or replacing, the standard contractual clauses or UK standard contractual clauses that form part of it at the date of signature in order to ensure continued compliance with Data Protection Law.

# Liability

## Where Sage has paid compensation, damages, or fines, Sage is entitled to claim back from the Institution that part of the compensation, damages, or fines corresponding to the Institution’s part of responsibility for the compensation, damages, or fines.

## Sage’s liability under this DPA is limited to the greater of (a) the amount Institution has paid to Sage for access to and use of the Services in the 12 months prior to the event or circumstance giving rise to the claim and (b) US$100. For the sake of clarity, Sage and Institution expressly agree that such an amount is not in addition to the liability caps under the Agreement.

# Termination and return or deletion

## This DPA is terminated upon the termination of the Agreement.

## Institution may request the return of Institution Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Sage will delete all remaining copies of Institution Personal Data within one hundred eighty (180) days after returning Institution Personal Data to Institution.

# Applicable law and jurisdiction

## This DPA is governed by the laws of [Country]. Any disputes relating to this DPA will be subject to the exclusive jurisdiction of the courts of [Country, City].

# Modification of this DPA

## This DPA may only be modified by a written amendment signed by both Sage and Institution.

# Invalidity and severability

## If any provision of this DPA is found by any court or administrative body of a competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

**ANNEX I**

**DESCRIPTION OF THE PROCESSING AND TRANSFERS**

1. **LIST OF PARTIES**

Data exporter:

* Name: Institution (as defined above)
* Address: See signature page above.
* Contact person’s name, position, and contact details: See signature page above.
* Activities relevant to the data transferred under these Clauses: The institution receives Sage’s Services as described in the Agreement and provides Sage with Personal Data in that context.
* Signature and date: See signature page above.
* Role (controller/processor): Controller, or Processor on behalf of Third-Party Controller.

Data importer:

* Name: Sage (as defined above)
* Address: See signature page above.
* Contact person’s name, position, and contact details: See signature page above.
* Activities relevant to the data transferred under these Clauses: Sage provides its Services to the Institution as described in the Agreement and Processes Personal Data on behalf of the Institution in that context.
* Signature and date: See signature page above.
* Role (controller/processor): Processor on behalf of Institution, or Subprocessor on behalf of Third-Party Controller.

1. **DESCRIPTION OF INTERNATIONAL DATA TRANSFER**

* Categories of Data Subjects whose Personal Data is transferred:

| **#** | **Category of Data Subjects** |
| --- | --- |
|  | *Institution’s study participants and research subjects* |
|  | *Institution’s survey, interview, and focus group participants* |
|  | *Institution’s personnel, staff and contractors* |
|  | *[Other (specify)]* |

* Categories of Personal Data transferred:

| **#** | **Category of Personal Data** |
| --- | --- |
|  | *Genetic data* |
|  | *Health/disability data* |
|  | *(Professional) contact details* |
|  | *Identification information* |
|  | *[Other (specify)]* |

* Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

| **#** | **Category of Sensitive Data** | **Applied restrictions or safeguards** |
| --- | --- | --- |
|  | *Genetic data* | *See restrictions and safeguards in Annex II* |
|  | *Health data* | *See restrictions and safeguards in Annex II* |
|  | *Biometric data* | *See restrictions and safeguards in Annex II* |

* The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): *On a continuous basis.*
* Nature of the processing: *The Personal Data will be processed and transferred as described in the Agreement to support the [Self-Managed Plan or DCC Plan] including data storage, data consulting, data cleansing.*
* Purpose(s) of the data transfer and further processing: *The Personal Data will be transferred and further processed for the provision of the Services as described in the Agreement.*
* The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.*
* For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing: *The* *subject* *matter* *and* *nature* *of* *the* *Processing are* *referenced to the Agreement and this DPA. The Processing will take place for the duration of the Agreement.*

1. **COMPETENT SUPERVISORY AUTHORITY**

* The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Supervisory Authority of the Institution’s country of establishment in the EEA. If the Institution is not established in the EEA, the Supervisory Authority will be that of the EEA country where the Institution’s EU data protection representative is located. If the Institution does not have an EU data representative, the competent Supervisory Authority is one of the EEA countries where the Data Subjects are located.
* The UK Information Commissioner is the competent authority for the Processing of Personal Data relating to Data Subjects located in the UK.
* The Swiss Federal Data Protection and Information Commissioner is the competent authority for the processing of personal data relating to data subjects located in Switzerland.

**ANNEX II**

**TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

Sage will, at a minimum, implement the following types of security measures:

# Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Institution Personal Data are Processed, include:

* Establishing security areas, and restriction of access paths;
* Establishing access authorizations for employees and third parties;
* Access control system (ID reader, magnetic card, chip card);
* Key management, card-keys procedures;
* Door locking (electric door openers etc.);
* Security staff, janitors;
* Surveillance facilities, video/CCTV monitor, alarm system; and
* Securing decentralized data processing equipment and personal computers.

# Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

* User identification and authentication procedures;
* Strong ID/password security procedures (special characters, minimum length and complexity requirements, change of password);
* Automatic blocking (e.g. password or timeout);
* Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous password attempts;
* Creation of one master record per user, user-master data procedures per data processing environment; and
* Encryption of archived data media.

# Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Institution Personal Data in accordance with their access rights, and that Institution Personal Data cannot be read, copied, modified or deleted without authorization, include:

* Internal policies and procedures;
* Control authorization schemes;
* Differentiated access rights (profiles, roles, transactions and objects);
* Monitoring and logging of accesses;
* Disciplinary action against employees who access Institution Personal Data without authorization;
* Reports of access;
* Access procedure;
* Change procedure;
* Deletion procedure; and
* Encryption.

# Disclosure control

Technical and organizational measures to ensure that Institution Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic) and that it can be verified to which companies or other legal entities Institution Personal Data are disclosed, include:

* Encryption/tunneling;
* Logging; and
* Transport security.

# Entry control

Technical and organizational measures to monitor whether Institution Personal Data have been entered, changed, or removed (deleted), and by whom, from data processing systems, include:

* Logging and reporting systems; and
* Audit trails and documentation.

# Control of instructions

Technical and organizational measures to ensure that Institution Personal Data are Processed solely in accordance with the instructions of the Controller include:

* Unambiguous wording of the contract;
* Formal commissioning (request form); and
* Criteria for selecting the Processor.

# Availability control

Technical and organizational measures to ensure that Institution's Personal Data are protected against accidental destruction or loss (physical/logical) include:

* Backup procedures;
* Mirroring of hard disks (e.g. RAID technology);
* Uninterruptible power supply (UPS);
* Remote storage;
* Anti-virus/firewall systems; and
* Disaster recovery plan.

# Separation control

Technical and organizational measures to ensure that Institution Personal Data collected for different purposes can be Processed separately include:

* Separation of databases;
* “Internal client” concept / limitation of use;
* Segregation of functions (production/testing); and
* Procedures for storage, amendment, deletion, and transmission of data for different purposes.

1. **Testing controls**

Technical and organizational measures to test, assess and evaluate the effectiveness of the technical and organizational measures implemented in order to ensure the security of the processing include:

* Periodical review and test of disaster recovery plan;
* Testing and evaluation of software updates before they are installed;
* Authenticated (with elevated rights) vulnerability scanning; and
* Test bed for specific penetration tests and Red Team attacks.

1. **IT governance**

Technical and organizational measures to improve the overall management of IT and ensure that the activities associated with information and technology are aligned with the compliance efforts include:

* Certification/assurance of processes and products;
* Processes for data minimization;
* Processes for data quality;
* Processes for limited data retention;
* Processes for ensuring accountability; and
* Data subject rights policies.

Sage will contractually require its Subprocessors to implement the same or at least equivalent technical and organizational measures to provide assistance to the Institution.

**ANNEX III  
  
LIST OF SUBPROCESSORS**

The institution authorizes Sage to engage the Subprocessors listed here: <https://sagebionetworks.org/trust-center/>.