DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") forms part of the Agreement entered into between SOPHiA GENETICS (hereinafter "**SG**") and Customer (as such terms are defined in SG's applicable terms and conditions accessible at https://www.sophiagenetics.com/legal-documents/ or, as applicable, in the Agreement) (the "**Principal Agreement**").

By agreeing to the Principal Agreement, Customer agrees to the terms of this Addendum, which shall be fully incorporated by reference into the Agreement and shall form an integral part of the Agreement with effect from the date of the Principal Agreement.

1. Definitions

Capitalized terms used and not otherwise defined in this Addendum shall have the meanings ascribed to them in the Principal Agreement. In this Agreement:

1.1 "**Contracted Processor**" means SG or any Subprocessor.

1.2 "**Customer Data**" means any and all Personal Data, biological samples, or other materials or content, uploaded, submitted through the Software Services or the Licensed Software or otherwise provided by Customer (including by Authorized Users) under, or in connection with, the Principal Agreement.

1.3 "**Data Protection Laws**" means any applicable laws and regulations relating to the processing of Personal Data applicable during the term of the Principal Agreement.

1.4 "**Personal Data"** means any information relating to an identified or identifiable natural person who can be identified directly or indirectly.

1.5 "**Representatives**" means, with respect to a Party, that Party's and its Affiliates' employees, officers, directors, consultants, agents, independent contractors, service providers, sublicensees, subcontractors, and legal advisors.

1.6 "**Transfer Safeguard**" means any appropriate mechanism recognized under applicable Data Protection Laws to legitimize a Restricted Transfer, including, without limitation, adequacy decisions, standard contractual clauses, binding corporate rules, certifications, or other instruments recognized by the competent Supervisory Authorities.

1.7 "**Subprocessor**" means any third party appointed by SG to Process Personal Data on behalf of SG and/or Customer in connection with the Principal Agreement.

1.8 **"Restricted Transfer"** means any transfer of Personal Data across national or territorial borders that requires a legal basis, transfer safeguard, or other mechanism under applicable Data Protection Laws in order to be lawful.

1.9 The terms "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the meaning ascribed to those terms in applicable Data Protection Laws, and their cognate terms shall be construed accordingly.

2. Processing of Customer Data in connection with the performance of the Principal Agreement

The Parties agree that Customer Data to be processed by SG under, or in connection with the Principal Agreement, shall be processed in accordance with the Agreement, this Addendum and relevant mandatory provisions of applicable Data Protection Laws, whereby Customer shall act as Controller of Customer Data and SG shall act exclusively as Processor, under the direction and control of Customer.

2.1 SG's obligations

SG shall:

2.1.1 comply with the relevant applicable Data Protection Laws in the Processing of Customer Data; and

2.1.2 Process Customer Data only on the relevant documented instructions of Customer, unless Processing is required by Data Protection Laws to which the relevant Contracted Processor is subject.

2.2 Customer's obligations

Customer:

2.2.1 warrants and represents that it shall comply with applicable Data Protection Laws and resulting obligations;

2.2.2 instructs SG (and authorizes SG to instruct each Subprocessor) to:

2.2.2.1 Process Customer Data; and

2.2.2.2 in particular, transfer Customer Data to any country or territory,

as reasonably necessary for the performance of the Principal Agreement and consistent with the Principal Agreement and in accordance with this Addendum;

2.2.3 warrants and represents that (i) it is and will at all relevant times remain duly and effectively authorized to give the instruction set out in Section 2.2.2, (ii) it has

obtained and will maintain all necessary rights and authorization for the communication and processing by SG and its Affiliates of the Customer Data in accordance with the Principal Agreement, (iii) it has informed the Data Subject about the processing in accordance with the Principal Agreement, and (iv) Customer Data are adequate, relevant, limited to the purposes of the Processing and up-to-date; and

2.2.4 indemnifies and holds harmless SG and its Affiliates and their directors, officers, employees, agents and other Representatives, against any demands, actions, suits, proceedings or claims emanating from a Data Subject whose Personal Data would be Processed as part of the performance of the Principal Agreement and in accordance with this Addendum.

2.3 Information regarding the Processing

Annex I to this Addendum sets out certain information regarding SG's Processing of the Customer Data. Each Party shall inform the other Party of necessary amendments to Annex I by written notice from time to time. The Parties shall negotiate in good faith the required amendments to Annex I if needed.

3. SG Personnel

SG ensures that its Representatives that are authorized to process the Customer Data have committed themselves to confidentiality undertakings or are under an appropriate statutory obligation 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, SG shall, in relation to the Customer Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk in accordance with the provisions of our cloud service technical documentation as published here: https://www.sophiagenetics.com/legal-documents/ (as amended from time to time) ("**Cloud Service Technical Documentation**").

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

5. Subprocessing

5.1 Customer hereby authorizes the use of the Subprocessor(s) set out herein in Annex III for Processing Customer Data. If SG (or any Subprocessor) appoints a new Subprocessor, or intends to make any changes concerning the addition or replacement of any Subprocessor set out in Annex III, it shall provide Customer with thirty (30) days' prior written notice (or any shorter notice period as may be agreed between Customer and SG), during which Customer is allowed to object against the appointment or replacement. If Customer does not object, SG

may proceed with the appointment or replacement. If, however, the Parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Principal Agreement for convenience, with the effects of termination as described in the Principal Agreement.

SG shall ensure that it has a written agreement in place with all Subprocessors which contains obligations on each Subprocessor that offer at least the same level of protection for Customer Data as those set out in this Addendum.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, SG shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations to respond to requests to exercise Data Subjects' rights under the Data Protection Laws.

6.2 SG shall:

6.2.1 promptly notify Customer if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Customer Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Customer or as required by Data Protection Laws to which the Contracted Processor is subject, in which case SG shall to the extent permitted by Data Protection Laws inform Customer of that legal requirement before the Contracted Processor responds to the request.

6.3 In any event, Customer, as the Controller of the Processing, shall be solely liable for the fulfillment of its obligations concerning the rights of all Data Subjects.

7. Personal Data Breach

7.1 SG shall (i) notify Customer without undue delay upon SG or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Data, and (ii) provide Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or the competent Supervisory Authority of the Personal Data Breach under the Data Protection Laws.

7.2 SG shall assist Customer, taking into account the nature of Processing and the information available to SG, in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

SG shall assist Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required, in each case solely in relation to Processing of Customer

Data by Contracted Processor and taking into account the nature of the Processing and information available to SG.

9. Customer Data retention

9.1 SG shall retain Customer Data necessary for the performance of the Principal Agreement. Where the Customer Data is no longer necessary for the performance of the Principal Agreement, SG reserves the right, at its sole discretion, to delete such Customer Data.

9.2 Subject to Section 9.3, Customer may in its absolute discretion by written notice to SG within thirty (30) days of the date of cessation of the Principal Agreement ("**Cessation Date**") require SG to (a) return a copy of Customer Data provided by the Customer by secure file transfer in such format as is reasonably defined by SG; and/or (b) delete all copies of Customer Data Processed by any Contracted Processor. The Parties shall determine the conditions of such destruction or return in accordance with applicable Data Protection Laws. For this purpose, Customer acknowledges and accepts that SG (or its Affiliate) may keep the backup of Customer Data for archiving purposes. Deletion shall include anonymization as per Data Protection Laws.

9.3 In addition, each Contracted Processor may retain Customer Data to the extent required by Data Protection Laws and only to the extent and for such period as required by Data Protection Laws, and always provided that SG shall ensure (i) the confidentiality of all such Customer Data, and (ii) that such Customer Data is only Processed as necessary for the purpose(s) specified in the Data Protection Laws requiring its storage and for no other purpose.

10. Audit rights

10.1 Subject to Section 10.2, SG shall make available to Customer on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Data by the Contracted Processors.

10.2 Where Customer undertakes an audit or inspection pursuant to Section 10.1, Customer shall give SG notice of at least forty-five (45) days of any such audit or inspection, shall ensure that each of its mandated auditors shall have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and shall make (and ensure that each of its mandated auditors make) all commercial efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.2.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.2.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit or inspection has given notice to SG that this is the case before attendance outside those hours begins; or

10.2.3 where one (1) audit or inspection, in respect of each Contracted Processor, has already occurred in any given calendar year, except for any additional audits or inspections which Customer is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory.

11. Restricted Transfers

11.1 In case a Restricted Transfer (within the meaning of Data Protection Laws) occurs and a Transfer Safeguard is required in accordance with Data Protection Laws, Customer (as "data exporter") and each Contracted Processor (as "data importer") shall implement the applicable Transfer Safeguard recognized under the Data Protection Laws governing that transfer.

11.2 The applicable Transfer Safeguard shall come into effect under Section 11.1 on commencement of the applicable Restricted Transfer.

11.3 SG warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not an Affiliate of SG, SG shall ensure that the applicable Transfer Safeguard recognized under Data Protection Laws applies between SG and said Subprocessor.

12. General Terms

Governing law and jurisdiction

12.1 The Parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.2 This Addendum and all non-contractual or other obligations arising out of or in connection with this Addendum are governed by the laws of the country or territory governing the Principal Agreement.

Order of precedence

12.3 In the event of any conflict or inconsistency between the provisions of this Addendum and any other agreements between the Parties, including the Principal Agreement and including agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail with respect to Processing of Personal Data.

Severance

12.4 If any provision in this Addendum is held to be illegal, invalid or unenforceable, in whole or in part, under any applicable law, competent court or regulation, then such provision or part of it shall be deemed not to form part of this Addendum, and the legality, validity or enforceability of the remainder of this Addendum shall not be affected. In such case, each Party hereto shall use reasonable efforts to immediately negotiate in good faith a valid replacement provision that is as close as possible to the original intention of the Parties and has the same or as similar as possible economic effect.

Liability

12.5 The Parties agree that the limitations of liability stipulated in the Principal Agreement shall apply to this Addendum.

13. Processing of Customer Data for which SG is acting as the Controller

13.1 For the purposes of the Principal Agreement and the contractual relationship between SG and Customer, SG will process Personal Data of members of the personnel of Customer or any Customer Affiliates (contact details: name, address, email address and phone number).

13.2 This Personal Data is necessary for the performance of the Principal Agreement and the contractual relationship between the Parties. When such Personal Data is communicated by Customer to SG, Customer represents and warrants that (i) it is and will at all times remain duly and effectively authorized to provide such Personal Data to SG, (ii) it has obtained and will maintain all necessary rights and authorization for such communication and processing by SG

in accordance with the Principal Agreement and this Addendum, (iii) it has informed the Data Subject about the processing in accordance with the Principal Agreement and this Addendum, and (iv) such Personal Data is adequate, relevant, limited to the purposes of this Personal Data Processing, accurate and up-to-date.

13.3 SG will process said Personal Data in accordance with the terms of its privacy policy as accessible here: https://www.sophiagenetics.com/privacy-policy/ and as amended from time to time.

ANNEX I

DESCRIPTION OF PROCESSING OF PERSONAL DATA

SG Platform

This document describes the processing of Personal Data by SG on behalf of the Customer in the context of providing the services related to the SG Platform.

The Parties shall keep this document up to date throughout the Processing of Personal Data.

Data Controller	Customer
Data Processor	SG
Agreement to which this document relates	Principal Agreement
Purpose and nature of the processing	Customer data shall be processed to (a) provide the Services; (b) to maintain, develop, improve and demonstrate the SG Technology, products and services; and (c) as permitted or required by applicable laws, rules, and regulations.
Categories of data subjects	Individuals and patients
Types of Personal Data	Direct identifying data*, demographic* (date of birth, gender, ethnicity), unique identifiers assigned by the Data Controller, SOPHiA GENETICS identifier and institution-specific identifier, genomic and associated technical metadata relating to biological sample analysis, health data* (disease information, personal medical history) **For user convenience, certain data fields are optional and are not required to be completed*
Duration of processing	Duration of the Principal Agreement, without prejudice to any retention obligations or limitation periods.
Subcontractors involved in the processing	As listed in Annex III
Geographical location of the processing	Location of the Processing is dependent on Customer's location. SG stores and processes the data on the following Microsoft Azure servers: - France - certified Health Data hosting Server (HDS) - Netherlands - certified Health Data hosting Server (HDS) - Switzerland - United States of America - Canada - Australia - Brazil - Japan

	- United Arab Emirates

SOPHiA Unity

This document describes the processing of Personal Data by SG on behalf of the Customer in the context of providing the services related to SOPHiA Unity

The Parties shall keep this document up to date throughout the Processing of Personal Data.

Data Controller	Customer
Data Processor	SG
Agreement to which this document relates	SOPHiA UNITY Network Agreement
Purpose and nature of the processing	SG will process Customer Personal data for the following purposes: • The aggregation of Multimodal Data for use in monocentric or multicentric academic research, to be designed and performed under the strict and direct control of the participating sites and subject to applicable research and ethics committees' approval. All such Academic Collaborative Research Projects will be presented to the SOPHiA UNITY Research Committee. Publication strategies will be developed and agreed with the participating Contributing Members in accordance with the applicable Network Policies; • The anonymization by aggregating data stacks for use in offerings designed and performed by SG for Commercial Partners. • Other processing of data stacks for collaborations with Commercial Partners as may be agreed, on a case-by-case basis, between SG and participating Contributing Members.
Categories of data subjects	- Individuals involved in research activities - Patients
Types of Personal Data	Data associated to a biological sample, genomic data, imaging data, pathology data, clinical data, reports of analysis, variant flagging and annotations.
Duration of processing	Duration of the Principal Agreement, without prejudice to any retention obligations or limitation periods.
Subcontractors involved in the processing	As listed in Annex III
Geographical location of the processing	SG stores and processes the data on Microsoft Azure certified Health Data hosting Server (HDS) located in France.

Research projects

This document describes the processing of Personal Data by SG on behalf of the Customer in the context of providing the services associated to research projects initiated and/or sponsored by the Customer.

The Parties shall keep this document up to date throughout the Processing of Personal Data.

Data Controller	Customer
Data Processor	SG
Agreement to which this document relates	Applicable research agreement
Purpose and nature of the processing	The details of the processing activities are described in the research agreement or, as applicable, research protocol agreed between the parties. The fields below shall be completed on a case-by-case basis in accordance with the applicable research agreement or protocol.
Categories of data subjects	
Types of Personal Data	
Duration of processing	
Subcontractors involved in the processing	
Geographical location of the processing	

SOPHiA Carepath

This document describes the processing of Personal Data by SG on behalf of the Customer in the context of providing the services related to SOPHiA Carepath.

The Parties shall keep this document up to date throughout the Processing of Personal Data.

Data Controller	Customer
Data Processor	SG
Agreement to which this document relates	Principal Agreement
Purpose and nature of the processing	Customer data shall be processed to (a) provide the services set out in the Principal Agreement; (b) to maintain, develop, improve and demonstrate the SG Technology, products and services; and (c) as permitted or required by applicable laws, rules, and regulations.
Categories of data subjects	- Individuals involved in research activities - Individuals and/or patients
Types of Personal Data	Individuals and/or patients A. Direct identifying data – First name and last name – Contact details (postal address, email address, phone number) – SOPHiA GENETICS patient identifier – Institution-specific patient identifier B. Indirect identifying data (quasi-identifiers) – Month and year of birth – Weight and height – Ethnicity and origin – Smoking status C. Clinical data and health data – Personal and family medical history – Dates and details of diagnoses – Clinical performance status – Therapies and treatments received and response to treatment – Disease progression information – Vital status and, where applicable, date and cause of death D. Biological and genomic data – Tumor profile (including anatomopathological classification) – Identified genomic and molecular markers – Relevant biological and laboratory results collected at baseline and during follow-up

	E. Imaging data (health data – special category under GDPR) – Diagnostic and follow-up medical imaging – Radiological assessments, including metastatic burden and response evaluation metrics (e.g., RECIST scores) F. Free-text data – Any additional information entered by users which may contain clinical and/or identifying information.
Duration of processing	Duration of the Principal Agreement, without prejudice to any retention obligations or limitation periods.
Subcontractors involved in the processing	As listed in Annex III
Geographical location of the processing	Location of the Processing is dependent on Customer's Location. SG stores and processes the data on the following Microsoft Azure servers: - France - certified Health Data hosting Server (HDS)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

- ISO27001:2022 Information Security Management Systems;
- ISO 27017:2015 Information technology — Security techniques;
- ISO 27018:2019 Protection of personally identifiable information (PII) in public clouds;
- Access control to premises and facilities;
- Access control to systems;
- Access control to data;
- Login information regulated with password and token;
- Password policies, clean desk policies, etc.;
- Endpoint Security controls;
- Limitation of the data communicated to SG to the extent required by the services;
- Encryption of data;
- Confidentiality undertaking of all representatives who access the data;
- Segregation of the data;
- Information security procedures may be provided upon request and are integrated as part of SG's Quality Manual;
- For French customers: Data hosted by an authorized "HébergeurAgréé".

Further details about the technical and organizational measures implemented by SG are presented in the Cloud Technical documentation https://www.sophiagenetics.com/legal-documents (as amended from time to time).

April 2026

ANNEX III

LIST OF SUB-PROCESSORS

Name	**Address**	**Description of processing**
Microsoft Ireland Operations Limited, c/o Microsoft Schweiz GMBH	Richtistrasse 3, CH-8304 Wallisellen, Switzerland	Cloud services
Oracle America Inc.	500 Oracle Parkway, Redwood Shores, CA 94065-1677, USA	Backup Data Storage
Databricks Inc.	160 Spear Street, Suite 1300, San Francisco, CA 94105, USA	Data governance & security
Endava GmbH	Eschersheimer Landstraße 14, 60322 Frankfurt am Main, Germany	data visualization (engineering support)
Atlassian	Singel 236 1016 AB, Amsterdam, Netherlands	Customer support, processing users' data only