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 the SG 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 as described to them in the Principal Agreement. In this Agreement:

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

1.2 "**Cross-Border Data Transfer**" means the transfer of Personal Data from one jurisdiction to another, whether through physical, electronic, or other means. It includes the transfer of Personal Data to any third party, data processor, or affiliate located outside the jurisdiction where the data was originally collected.

1.3 "**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.

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

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

1.6 "**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.

1.7 **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of Personal Data to processors established outside the jurisdiction where the data was originally collected;

1.8 "**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.

1.9 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, provided that 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' 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' 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 twenty (20) 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 fulfillment of Customer's obligations, to respond to requests to exercise Data Subjects' rights under the Data Protection Laws. Such measures shall include (i) encryption of data, (ii) restricted access to the data to only those who have a need to know and are under confidentiality obligations, (iii) segregation of administrative data and (iv) pseudonymization of genomics, radiomics, pathology, clinical and other multimodal data. Customer acknowledges that such measures meet its data protection requirements.

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 therequest.

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 Supervising 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 them.

9.2 Subject to Section 9.2, 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 Applicable 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 Applicable Data Protection Laws), including (without limitation) a transfer of Personal Data to a country or territory outside the European Union (EEA), occurs and a transfer safeguard is required in accordance with Applicable Data Protection Laws, Customer (as "data exporter") and each Contracted Processor (as "data importer") shall be deemed to have entered into the Standard Contractual Clauses unless another transfer safeguard (such as an adequacy decision) applies.

11.2 The Standard Contractual Clauses 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 Standard Contractual Clauses apply between SG and said Subprocessor.

12. General Terms

Governing law and jurisdiction

12.1 Without prejudice to the Standard Contractual Clauses:

12.1.1 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

12.1.2 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

12.2 In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail with respect to Restricted Transfers of Personal Data.

12.3 Subject to Sections 12.2, 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

The SOPHiA 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 SOPHiA 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	Data Protection Addendum to the SG General Terms and Conditions
Purpose and nature of the processing	Customer data shall be processed (i) for performing this Agreement; (ii) to pseudonymize and anonymize Customer Data; (iii) for statistical, scientific, or research purposes; (iv) for creating Insights; (v) for providing biomarker identification; (vi) for researching, developing, maintaining, or promoting the SG Technology, Products, or Services; or (vii) as permitted or required by applicable laws, rules, and regulations.
Categories of data subjects	- Individuals involved in research activities - Patients
Types of Personal Data	Biological samples and associated data, genomic data, imaging data (where applicable), 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	Location of the Processing is dependent on Customer's Location. SG stores and process 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 - 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 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 aggregated of 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 process the data on Microsoft Azure certified Health Data hosting Server (HDS) located in France.

January 2025

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 project 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	Research agreement
Purpose and nature of the processing	The details of the processing activities are described in the research protocol agreed between the parties.
Categories of data subjects	
Types of Personal Data	
Duration of processing	
Subcontractors involved in the processing	
Geographical location of the processing	

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.

ANNEX III

LIST OF SUB-PROCESSORS

Name: Microsoft Ireland Operations Limited, c/o Microsoft Schweiz GMBH

Address: Richtistrasse 3, CH-8304 Wallisellen, Switzerland

Description of Processing: Cloud services

Name: Databricks Inc.

Address: 160 Spear Street, Suite 1300, San Francisco, CA 94105, USA

Description of Processing: Data governance & security

Name: Endava GmbH

Address: Eschersheimer Landstraße 14, 60322 Frankfurt am Main, Germany

Description of Processing: Data visualization (engineering support)

Name: Atlassian

Address: Singel 236 1016 AB, Amsterdam, Netherlands

Description of Processing: Customer support, processing users' data only.

ANNEX IV

International Data Transfer (where applicable)

DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data exporter(s):

Name: *SG' Customer as defined in the Principal Agreement*

Address: As per the Principal Agreement

Contact person's name, position and contact details: As per the Principal Agreement

Activities relevant to the data transferred under these Clauses: As per the Principal Agreement

Signature and date: as per the principal agreement

Role (controller/processor): Data Controller

Data importer(s):

Name: *SG as defined in the Principal Agreement*

Address: La Piece 12, CH 1180 Rolle, Switzerland

Contact person's name, position and contact details:

Data Protection Officer – privacy@sophiagenetics.com

Activities relevant to the data transferred under these Clauses:

SG is a technology company dedicated to establishing the practice of data-driven medicine as the standard of care and for life sciences research, with commercial applications for clinical and biopharma markets.

Signature and date: as per the Principal Agreement

Role (controller/processor): Data Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred:

Category (A): SG' Customers' clients and patients

Category (B): SG' Customers' Representatives.

Categories of Personal Data transferred:

Category (A): Biological samples, clinical data, genomic data, imaging data, reports of analysis, variant flaggings

Category (B): Professional contact details, and aggregated information of Customer's activities while using the Products, Services, and/or the SOPHiA DDM™ Platform (including through, but not limited to, the use of cookies)

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 (A): Health and genetic data

Additional safeguards implemented: pseudonymization by segregation, access restrictions, strict purpose limitation, security measures (HDS, ISO 27001, ISO 27017, ISO 27018), etc.

The frequency of the transfer (e.g,. whether the data is transferred on a one-off or continuous basis).

Categories (A) & (B): Continuous basis

Nature of the processing & Purpose(s) of the data transfer and further processing

Categories (A) & (B):

(i) For the performance of SG' contractual obligations vis-à-vis its Customer; (ii) to pseudonymize and anonymize Customer Data; (iii) to pseudonymize and anonymize Customer Data; (iii) for statistical, scientific, or research purposes; (iv) for creating Insights; (v) for providing biomarker identification; (vi) for researching, developing, maintaining, or promoting the SG Technology, Products, or Services; or (vii) as permitted or required by applicable laws, rules, and regulations.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period

Categories (A) & (B):

The Customer Data is subject to processing and is kept by SG in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Customer Data are Processed (see above).

Customer Data will be available to Customer for the period required under applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Categories (A) & (B): Same as above

C. COMPETENT SUPERVISORY AUTHORITY

Commission Nationale de l'Informatique et des libertés

3 place de Fontenoy – UNESCO

75007 Paris

France

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of (i) 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 (General Data Protection Regulation) and/or (ii) any Applicable Data Protection Laws, for the transfer of Personal Data to a third country).

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the Personal Data, as listed in Annex IV.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex IV.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (the "**Clauses**").

(c) These Clauses apply with respect to the transfer of Personal Data as specified in Annex IV.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided that they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 –Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Annex IV.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the related Appendix.

(b)Once it has completed the Appendix and signed the document, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex IV.A.

(c)The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a)The data importer shall process the Personal Data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the Personal Data only for the specific purpose(s) of the transfer, as set out in Annex IV.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and Personal Data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all Personal Data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all Personal Data processed on its behalf and delete existing copies. For this purpose, deletion shall include anonymization as per General Data Protection Regulation. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a)The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'Personal Data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the Personal Data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)The data importer shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. For this purpose, implementation, management and monitoring shall mean any activities including SG' legitimate purposes referenced under the contract. It shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)In the event of a Personal Data breach concerning Personal Data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex II.

8.8 Onward transfers

The data importer shall only disclose the Personal Data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a)The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least twenty (20) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the Personal Data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a)The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b)In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i)lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d)The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)The data importer agrees that the choice made by the data subject under Section (c) will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex IV.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex IV.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose Personal Data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex IV.C, shall act as competent supervisory authority.

(b)The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the Personal Data by the data importer, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i)the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii)the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii)any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the Personal Data in the country of destination.

(c)The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i)receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a)The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of Personal Data under these Clauses, where:

(i)the data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred Personal Data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of Personal Data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the laws of Principal Agreement.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of of Principal Agreement.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX V

DATA TRANSFERS FROM/TO SWITZERLAND

The Parties agree to supplement these standard clauses with the below provisions, which do not derogate from or contradict Clause 2:

- Clause 18 shall not be interpreted in such a way that Data Subjects in Switzerland are excluded from exercising their rights in accordance with clause 18, c), at their habitual residence in Switzerland.

- The Federal Data Protection and Information Commissioner (FDIPC) is the competent authority for the purposes of the Federal Act on Data Protection of 19 June 1992, as amended from time to time (the “FADP”), where the FADP applies exclusively to the data in question.

- Where the data involves the competent supervisory authority referred to in Annex IV.C., and the FDIPC; both authorities shall have the authority to review the data that is subject to their jurisdiction.