DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is between the customer identified in the signature page hereto ("**Controller**"), and Guild.ai ("**Processor**") (each, a "**Party**" and collectively the "**Parties**") and is effective as of the date of last signature below (the "**Effective Date**"). This DPA supplements the Guild.ai Customer Terms of Service entered into between the Parties ("**Agreement**") in relation to the transfer and processing of Covered Data in connection with the performance of the Services.

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The following capitalized terms used in this DPA will be defined as follows:

"**Applicable Data Protection Laws**" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time, including (without limitation): the GDPR, Swiss Data Protection Laws and the US Data Protection Laws.

"**Controller Purposes**" means: (a) undertaking internal research and development to develop, test, improve and alter the functionality of the Services; (b) creating anonymised datasets for training or evaluation of Services; and (c) administering the Controller's relationship with Processor under the Agreement.

"**Covered Data**" means Personal Data that is: (a) provided by or on behalf of Controller to Processor in connection with the Services; or (b) obtained, developed, produced or otherwise Processed by Processor, or its agents or subcontractors, for the purposes of providing the Services, in each case as further described in Schedule 1.

"**Data Subject**" means a natural person whose Personal Data is Processed.

"**Deidentified Data**" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"**EEA**" means the European Economic Area including the European Union ("**EU**").

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**", as defined in section 3 of the Data Protection Act 2018.

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein.

"**Personal Data**" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data", "personal information", "personally identifiable information", or similarly defined data or information under Applicable Data Protection Laws.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorized access to, Covered Data.

"**Services**" means the services to be provided by Processor to Controller under the Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"**Sub-processor**" means, with respect to any Processing performed by Processor as a processor or service provider, an entity appointed by Processor to Process Covered Data on its behalf.

"**Swiss Data Protection Laws**" means the Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**") and the Swiss Data Protection Ordinance of 31 August 2022 (the "**Ordinance**"), and any new or revised version of these laws that may enter into force for time to time.

"UK" means the United Kingdom.

"**US Data Protection Laws**" means all applicable federal and state laws rules, regulations, and governmental requirements relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States.

"**Usage and Administration Data**" means:

(a) diagnostic, usage and performance information collected by Processor in relation to the Controller's and its authorised users' use of the Services, including metadata relating to content and information uploaded by the Controller to the Services;

(b) contact details relating to, and the content of correspondence with the Controller's main account holder or administrator;

(c) support enquiries submitted by the Controller's authorised users in relation to the Services.

1.2 The terms "**controller**", "**processor**", "**business**" and "**service provider**" have the meanings given to them in the Applicable Data Protection Laws.

2. INTERACTION WITH THE AGREEMENT

This DPA is incorporated into and forms an integral part of the Agreement. This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any Processing of Covered Data.

3. ROLE OF THE PARTIES

3.1 Except as set out in Section 3.2, Processor acts as a processor or service provider in the performance of its obligations under the Agreement and this DPA and Controller acts as a controller or business.

3.2 For the purposes of the GDPR and Swiss Data Protection Laws, Processor acts as a controller with respect to the Processing of Usage and Administration Data for the Controller Purposes.

4. DETAILS OF DATA PROCESSING

4.1 The details of the Processing of Personal Data under the Agreement and this DPA (including subject matter, nature and purpose of the Processing, categories of Personal Data and Data Subjects) are described in the Agreement and in Schedule 1 to this DPA.

4.2 Processor shall comply with its obligations under Applicable Data Protection Laws. Save with respect to any Processing of Usage and Administration Data for the Controller Purposes, Processor will only Process Covered Data on behalf of and under the instructions of Controller and in accordance with Applicable Data Protection Laws.

4.3 The Agreement and this DPA shall constitute Controller's instructions for the Processing of Covered Data. Controller may issue further written instructions in accordance with this DPA. Without limiting the foregoing, Processor is prohibited from:

(a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration;

(b) sharing Covered Data with any third party for cross-context behavioural advertising;

(c) retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws;

(d) retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and

(e) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Processor receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

4.4 Processor will:

(a) provide Controller with information to enable Controller to conduct and document any data protection assessments required under Applicable Data Protection Laws; and

(b) promptly inform Controller if, in its opinion, an instruction from Controller infringes the Applicable Data Protection Laws.

5. COMPLIANCE

5.1 Controller shall comply with its obligations as a controller, business or equivalent term under the Applicable Data Protection Laws, and shall:

(a) provide such information to Data Subjects regarding the Processing of their Covered Data in connection with the Controller's use of the Services as required under Applicable Data Protection Laws;

(b) obtain any consents required for the lawful Processing of Covered Data (other than Processor's Processing of Usage and Administration Data for the Controller Purposes) under this DPA in accordance with Applicable Data Protection Laws; and

(c) implement appropriate technical and organisational measures to give effect to Data Subject rights under Applicable Data Protection Laws, and shall comply with requests from Data Subjects to exercise their rights under Applicable Data Protection Laws within the timeframe and subject to any exemptions prescribed in the Applicable Data Protection Laws.

6. CONFIDENTIALITY AND DISCLOSURE

6.1 Processor shall:

(a) limit access to Covered Data to personnel who have a business need to have access to such Covered Data; and

(b) ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data to which they have access.

7. SUB-PROCESSORS

7.1 Processor may Process Covered Data anywhere that Processor or its Sub-processors maintain facilities, subject to the remainder of this clause 7.

7.2 Controller grants Processor general authorisation to engage any of the Sub-processors listed at the following url: https://app.guild.ai/legal/subprocessors, as amended in accordance with clause 7.4 (the "**Authorised Sub-processors**"), to Process Covered Data.

7.3 Processor shall:

(a) enter into a written agreement with each Authorised Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Processor's obligations under this DPA; and

(b) remain liable for each Authorised Sub-processor's compliance with the obligations under this DPA.

7.4 Processor will provide Controller with at least fourteen (14) days' notice of any proposed changes to the Authorised Sub-processors. Controller shall notify Processor if it objects to the proposed change to the Authorised Sub-processors (including, where applicable, when exercising its right to object under clause 9(a) of the SCCs) by providing Processor with written notice of the objection within fourteen (14) days after Processor has provided notice to Controller of such proposed change (an "**Objection**").

7.5 In the event Controller submits an Objection to Processor, Processor and Controller shall work together in good faith to find a mutually acceptable resolution to address such Objection. If Processor and Controller are unable to reach a mutually acceptable resolution within a reasonable timeframe, which shall not exceed thirty (30) days, Controller may terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to Processor.

7.6 Processor shall notify the Controller of any failure by the sub-processor to fulfil its obligations under that contract.

8. DATA SUBJECT RIGHTS REQUESTS

8.1 Processor will notify Controller without undue delay of any request received by Processor or any Authorised Sub-processor from a Data Subject to assert their rights in relation to Covered Data under Applicable Data Protection Laws (a "**Data Subject Request**").

8.2 Other than in respect of any Processing of Covered Data for the Controller Purposes, Controller will have sole discretion in responding to the Data Subject Request, and Processor shall not respond to the Data Subject Request, save that Processor may advise the Data Subject that their request has been forwarded to Controller.

8.3 Taking into account the nature of the Processing and the information available to Processor, Processor will provide Controller with reasonable assistance as necessary for Controller to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

9. SECURITY

9.1 Processor will implement and maintain appropriate technical and organisational data protection and security measures designed to ensure security of Covered Data, including,

without limitation, protection against unauthorised or unlawful Processing and against accidental loss, destruction, or damage of or to Covered Data.

9.2 When assessing the appropriate level of security, Processor shall take into account the nature, scope, context and purpose of the Processing as well as the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Covered Data.

9.3 Processor will implement and maintain as a minimum standard the measures set out in Schedule 2.

10. INFORMATION AND AUDITS

10.1 Processor shall notify Controller promptly if Processor determines that it can no longer meet its obligations under Applicable Data Protection Laws.

10.2 Controller may take reasonable and appropriate steps to:

(a) ensure that Processor uses Covered Data in a manner consistent with Controller's obligations under Applicable Data Protection Laws; and

(b) upon reasonable notice, stop and remediate unauthorized use of Covered Data.

10.3 Controller may audit Processor's compliance with this DPA at least annually. The Parties agree that all such audits will be conducted:

(a) upon reasonable written notice to Processor;

(b) only during Processor's normal business hours; and

(c) in a manner that does not materially disrupt Processor's business or operations.

10.4 With respect to any audits conducted in accordance with clause 10.3:

(a) Controller may engage a third-party auditor to conduct the audit on its behalf;

(b) Processor shall not be required to facilitate any such audit unless and until the Parties have agreed in writing the scope and timing of such audit.

10.5 Controller shall promptly notify Processor of any non-compliance discovered during an audit.

10.6 The results of the audit shall be Processor's confidential information.

10.7 Processor shall provide to Controller upon request, or may provide to Controller in response to any audit request submitted by Controller to Processor, either of the following:

(a) data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company; or

(b) such other documentation reasonably evidencing the implementation of the technical and organisational data security measures in accordance with industry standards.

10.8 If an audit requested by Controller is addressed in the documents or certification provided by Processor in accordance with paragraph 10.7, and:

(a) the certification or documentation is dated within twelve (12) months of Controller's audit request; and

(b) Processor confirms that there are no known material changes in the controls audited,

Controller agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

11. SECURITY INCIDENTS

11.1 Processor shall notify Controller in writing without undue delay, and in any event within forty-eight (48) hours, after becoming aware of any Security Incident.

11.2 Processor shall take reasonable steps to contain, investigate, and mitigate any Security Incident, and shall send Controller timely information about the Security Incident, to the extent known to Processor or as the information becomes available to Processor, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation.

11.3 Processor shall provide reasonable assistance with Controller's investigation of any Security Incidents and any of Controller's obligations in relation to the Security Incident under Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

11.4 Processor's notification of or response to a Security Incident under this paragraph 11 shall not be construed as an acknowledgement by Processor of any fault or liability with respect to the Security Incident.

12. TERM, DELETION AND RETURN

12.1 This DPA shall commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Processor's deletion of all Covered Data as described in this DPA.

12.2 Unless otherwise required by applicable law, Processor shall:

(a) if requested to do so by Controller within thirty (30) days of expiry of the Agreement (the "**Retention Period**"), provide a copy of all Covered Data in such commonly used format as requested by Controller, or provide a self-service functionality allowing Controller to download such Covered Data; and

(b) on expiry of the Retention Period, delete all copies of Covered Data Processed by Processor or any Authorised Sub-processors, other than any Covered Data Processed for the Controller Purposes.

13. STANDARD CONTRACTUAL CLAUSES

13.1 The Standard Contractual Clauses shall, as further set out in Schedule 3, apply to the transfer of any Covered Data from Controller to Processor, and form part of this DPA, to the extent that:

(a) the GDPR or Swiss Data Protection Law applies to the Controller when making that transfer; or

(b) the Applicable Data Protection Laws that apply to the Controller when making that transfer (the "**Exporter Data Protection Laws**") prohibit the transfer of Covered Data to Processor under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Covered Data, and any one or more of the following applies:

(i) the relevant authority with jurisdiction over the Controller's transfer of Covered Data under this DPA has not formally adopted standard data protection clauses or another transfer mechanism under the Exporter Data Protection Laws; or

(ii) such authority has issued guidance that entering into standard contractual clauses approved by the European Commission would satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(iii) entering into standard contractual clauses approved by the European Commission would reasonably satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or

(c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

13.2 The Parties agree that execution of the Agreement shall have the same effect as signing the SCCs.

14. DEIDENTIFIED DATA

If Processor receives Deidentified Data from or on behalf of Controller, Processor shall:

(a) take reasonable measures to ensure the information cannot be associated with a Data Subject;

(b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information; and

(c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

15. GENERAL

15.1 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

15.2 The Parties agree that any limitations on either Party's liability under the Agreement shall not apply to any claims, losses or damages arising in respect of a breach of the SCCs.

15.3 The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

IN WITNESS WHEREOF, the Parties hereto have executed this DPA as of the Effective Date.

Customer: _____	**Guild.ai**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:
Email:	Email:
Phone:	Phone:

SCHEDULE 1
DETAILS OF PROCESSING

A. List of Parties

The Parties are set out in the preamble to this DPA. With regard to any transfers of Covered Data falling within the scope of the GDPR from Controller to Processor, additional information regarding the data exporter and data importer is set out below.

Data Exporter

The data exporter is: the Controller operating in the countries which comprise the European Economic Area, UK and/or Switzerland and/or – to the extent agreed by the Parties – Controller in any other country to the extent the GDPR applies.

The data exporter's contact person's name, position and contact details as well as (if appointed) the data protection officer's name and contact details and (if relevant) the representative's contact details are provided in the signature page to the Agreement.

The activities relevant to the data transfer under these Clauses are defined by the Agreement and the data exporter who decides on the scope of the Processing of Personal Data in connection with the Services further described in section B of this Schedule 1.

Data Importer

The data importer is: the Processor.

The data importer's contact person and contact details are: Cristina Vasile, General Counsel, privacy@guild.ai.

The data importer's activities relevant to the data transfer under these Clauses are as follows: the data importer Processes Personal Data provided by the data exporter on behalf of the data exporter in connection with providing the Services to the data exporter as further described in section B of this Schedule 1 and in the Agreement.

B. Description of Processing

Categories of Personal Data

Controller may submit Personal Data to the Services, the categories of which will depend upon Controller's use of the Services which is determined and controlled by Controller in its sole discretion, but it may include, but is not limited to names, contact information (such as phone number, email address, physical address, or time zone), name of employer, third-party service account information and authorized content, and AI code and chat content.

Special categories of Personal Data (if applicable)

Processor does not intentionally or knowingly collect any special categories of Personal Data.

Categories of Data Subjects

The categories of Data Subjects whose Personal Data are Processed may include, but are not limited to: Controller's employees, customers, and generally Users.

Frequency of the Processing

The Processing is performed continuously.

Subject matter and nature of the Processing

The subject matter of the Processing is: the Processor's provision of AI-agent building and integration services to Controller, as further described in the Agreement.

Purpose(s) of the data transfer and further Processing

The purpose/s of the data transfer and further Processing is: for Processor's provision of AI-agent building and integration services to Controller, as further described in the Agreement.

Storage Limitation

The period during which the Personal Data will be Processed, or, if that is not possible, the criteria used to determine that period: if Personal Data is not deleted upon request by Controller during the term of the Agreement, the duration of Processing corresponds to the duration of this DPA as defined in clause 12 of the DPA.

Sub-processor (if applicable)

For Processing by sub-processors, specify subject matter, nature, and duration of the Processing:

The subject matter and the nature of Processing by sub-processors is set forth at the following url: https://app.guild.ai/legal/subprocessors. If Personal Data is not deleted upon request by Controller during the term of the Agreement, the duration of Processing corresponds to the duration of this DPA as defined in clause 12 of the DPA.

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with clause 13 of the SCCs:

The competent supervisory authority is the supervisory authority of Ireland.

SCHEDULE 2

Technical and OrganiZational Measures

Processor has implemented the following technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

1) Organizational management and staff responsible for the development, implementation, and maintenance of Processor's information security program.

2) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Processor's organization, monitoring and maintaining compliance with Processor's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3) Utilization of commercially available and industry standard encryption technologies for Covered Data that is:

a) being transmitted by Processor over public networks (i.e., the Internet) or when transmitted wirelessly; or

b) at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).

4) Data security controls which include at a minimum, but may not be limited to, logical segregation of data, logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

5) Password controls designed to manage and control password strength and usage including prohibiting users from sharing passwords and requiring that Processor's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on Processor's computer systems; (iii) must have a history threshold to prevent reuse of recent passwords; and (iv) newly issued passwords must be changed after first use.

6) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

7) Engage cloud service providers who ensure physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Processor facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

8) Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Processor's possession.

9) Change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Processor's technology and information assets.

10) Incident / problem management procedures design to allow Processor to investigate, respond to, mitigate, and notify of events related to Processor's technology and information assets.

11) Network security controls that provide for the use of firewall systems designed to protect systems from intrusion and limit the scope of any successful attack.

12) Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate, and protect against identified security threats, viruses, and other malicious code.

13) Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

14) Security Training. The company requires all new hires to complete security and privacy awareness training as part of initial on-boarding. Participation in annual training is required for all employees to provide a baseline for security and privacy basics..

SCHEDULE 3
STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

With respect to any transfers referred to in clause 13, the Standard Contractual Clauses shall be completed as follows:

1.1 Module One (*controller to controller*) of the SCCs will apply with respect to Processor's Processing of Covered Data for the Controller Purposes; otherwise, Module Two (*controller to processor*) of the SCCs will apply.

1.2 Clause 7 of the Standard Contractual Clauses (*Docking Clause*) does not apply.

1.3 Option 2 of Clause 9(a) (*General written authorization*) shall apply, and the time period to be specified is determined in clause 7.4 of the DPA.

1.4 The option in Clause 11(a) of the Standard Contractual Clauses *(Independent dispute resolution body*) does not apply.

1.5 With regard to Clause 17 of the Standard Contractual Clauses (*Governing law*), the Parties agree that option 1 will apply and the governing law will be Irish law.

1.6 In Clause 18 of the Standard Contractual Clauses (*Choice of forum and jurisdiction*), the Parties submit themselves to the jurisdiction of the courts of Ireland.

1.7 For the purpose of Annex I of the Standard Contractual Clauses, Schedule 1 of the DPA contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.

1.8 For the purpose of Annex II of the Standard Contractual Clauses, Schedule 2 of the DPA contains the technical and organisational measures.

2. UK Addendum

2.1 This paragraph 2 (*UK Addendum*) shall apply to any transfer of Covered Data from Controller (as data exporter) to Processor (as data importer), to the extent that:

(a) the UK Data Protection Laws apply to Controller when making that transfer; or

(b) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"**Approved Addendum**" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK

Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the "Addendum EU SCCs" shall refer to the SCCs as they are incorporated into this Agreement in accordance with clause 13 and this Schedule 3;

(b) Table 1 of the Approved Addendum shall be completed with the details in paragraph A of Schedule 1;

(c) the "Appendix Information" shall refer to the information set out in Schedule 1 and Schedule 2

(d) for the purposes of Table 4 of the Approved Addendum, Processor (as data importer) may end this DPA, to the extent the Approved Addendum applies, in accordance with Section 19 of the Approved Addendum; and

(e) Section 16 of the Approved Addendum does not apply.

3. Swiss addendum

3.1 This Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR.

3.2 Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"**Addendum**" means this addendum to the Clauses;

"**Clauses**" means the Standard Contractual Clauses as incorporated into this DPA in accordance with clause 13 and as further specified in this Schedule 3; and

"**FDPIC**" means the Federal Data Protection and Information Commissioner.

(b) This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfils the Parties' obligations under Article 16(2)(d) of the FADP.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer; and

(ii) as standard data protection clauses approved, issued or recognised by the FDPIC for the purposes of Article 16(2)(d) of the FADP.

3.3 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws

To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.4) the following amendments are made to the Clauses:

(a) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(b) Clause 6 Description of the transfer(s) is replaced with:

"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 those

specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer."

(c) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(d) References to Regulation (EU) 2018/1725 are removed.

(e) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(f) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(g) Clause 17 is replaced to state:

"These Clauses are governed by the laws of Switzerland".

(h) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

3.5 Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by paragraph 3.4 of this Addendum:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum); and

(B) subject to the provisions of paragraph 2 of this Schedule 3 (UK Addendum), the supervisory authority identified in Schedule 1 shall

act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(b) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses.

4. Transfers under the laws of other jurisdictions

4.1 With respect to any transfers of Personal Data referred to in clause 13.1(b) (each a "**Global Transfer**"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

4.2 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the applicable data exporter to the data importer, to the extent the Exporter Data Protection Laws apply to that data exporter's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data Protection Laws.

4.3 The amendments referred to in paragraph 4.2 include (without limitation) the following:

(a) references to the "GDPR" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) reference to the "Union", "EU" and "EU Member State" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "**Exporter Jurisdiction**");

(c) the "competent supervisory authority" shall be the applicable supervisory in the Exporter Jurisdiction; and

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

4.4 Where, at any time during Processor's Processing of Covered Data under this DPA, a transfer mechanism other than the SCCs is approved under the Exporter Data Protection Laws with respect to transfers of Covered Data by Controller to Processor, the Parties shall promptly enter into a supplementary agreement that:

(a) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(b) incorporates the details of Processing set out in Schedule 1; and

(c) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

4.5 Where required under the Exporter Data Protection Laws, the relevant data exporter shall file a copy of the agreement entered into in accordance with paragraph 4.4 with the relevant national authority.