DATA PROCESSING AGREEMENT

Les éléments en jaune sont des consignes ou éléments à compléter par vos soins.

Les éléments en vert sont fournis à titre d'exemple.

made on DATE

Company, having its registered offices at ADDRESS ("Company"), and covering the following entities and affiliates: LIST,

hereinafter referred to as "Controller",

and

PROCESSOR, a private company with limited liability, incorporated under the laws of COUNTRY, having its statutory seat in CITY and its principal place of business at FULL ADDRESS, registered with the AUTHORITY under FILE NUMBER XXX,

hereinafter referred to as "Processor",

referred to collectively as "Parties",

applicable to

REFERENCE TO PRINCIPAL AGREEMENT

hereinafter the "Principal Agreement"

regarding the

DESCRIPTION OF THE SERVICE

hereinafter the "Service"

1 Introduction

This Data Processing Agreement ("DPA") is made as of and for the duration of the Principal Agreement by and between the Parties. This DPA is applicable in relation to the Principal Agreement.

Save as provided in the Principal Agreement, the Controller and the Processor have concluded this DPA for the processing of Personal Data. A description of the processing and transfers is included in Schedule 1. Organisational and technical measures taken by the Processor are described in Schedule 2. An overview of the type of Personal Data, categories of data subjects, the purposes of processing and the Subprocessors is included in Schedule 3. An overview of the Subprocessors that the Processor has enabled is included in Schedule 4.

This DPA forms an integral part of the Principal Agreement. This DPA is effective upon and subject to the conclusion of the Principal Agreement by both Parties.

The duration, term, and termination of this DPA follow the term of the Principal Agreement. Terms not defined herein shall have the meaning as set forth in the Principal Agreement or within the relevant Data Protection Laws.

The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the General Data Protection Regulation (GDPR), as well as the Swiss Federal Act on Data Protection (FADP).

In consideration of the Principal Agreement, the Parties hereto agree as follows.

2 Definitions and Interpretation

Unless otherwise defined herein, capitalised terms and expressions used in this DPA shall have the following meaning:

- "Affiliate" means, in the context of each party, any corporation or other business entity controlled by, controlling, or under common “control” with a party.
- "Controller" means, for the purpose of this DPA, the party that determines the purposes and means of the processing of Personal Data in accordance with the Swiss Data Protection Laws and/or EU Data Protection Laws.
- "Processor" means, for the purpose of this DPA, the party that processes personal data on behalf of the Controller in accordance with the Swiss Data Protection Laws and/or EU Data Protection Laws.
- "Personal Data" means any personal data processed by the Processor on the Controller's behalf pursuant to or in connection with the Principal Agreement.
- "Data Protection Laws" means EU Data Protection Laws, Swiss Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.
- "EU Data Protection Laws" means the GDPR and European or national laws supplementing the GDPR.
- "GDPR" means EU General Data Protection Regulation 2016/679.
- "Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to third countries which do not ensure an adequate level of protection.
- "Swiss Data Protection Laws" means the Federal Act on Data Protection (FADP) and Swiss laws supplementing the FADP.
- "Subprocessor" means any person appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller in connection with the Principal Agreement.

- "Supervisory Authority" means an independent public authority which is established by an EU member state or Switzerland pursuant to the GDPR or the FADP.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "transfer", "profiling" and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies, and their cognate terms shall be construed accordingly.

3 Processing of Personal Data

PROCESSOR represents and warrants that CONTROLLER is the supplier of Personal Data while PROCESSOR is the Processor of such data, except when CONTROLLER acts as a Processor of Personal Data, in which case PROCESSOR is a Subprocessor; or as stated otherwise in the Principal Agreement or this DPA.

The Processor shall

- comply with all applicable Data Protection Laws in the processing of Personal Data; and
- not process Personal Data other than on the Controller's documented instructions.

The Controller instructs the Processor to process Personal Data in relation to and for the execution of the Principal Agreement. The Processor shall inform the Controller immediately if it believes an instruction issued by the Controller violates legal regulations. The Processor is entitled, without recognition of an obligation to check whether an unlawful instruction exists, to reject or suspend an instruction that it believes is unlawful until it is confirmed or changed by the Controller or to reject obviously illegal instructions at any time or to suspend processing relating to it.

The Processor undertakes to process Personal Data only for the purpose of the activities referred to in this DPA and/or in the Principal Agreement. The Processor guarantees that it will not use the Personal Data which it processes in the context of this DPA for its own or third-party purposes without the Controller’s express written consent unless a mandatory legal provision requires the Processor to do so. In such a case, the Processor shall immediately inform the Controller of that legal requirement before processing such information unless the law explicitly prohibits such disclosure.

The Processor may use and otherwise process Personal Data for its legitimate business operations as detailed in Schedule 3 and within the boundaries set forth in the said Schedule.

4 Confidentiality and Disclosure of Personal Data

Each of the Controller, Processor and/or Subprocessor must keep any information it receives confidential according to the relevant confidentiality provisions set forth in the Principal Agreement and this DPA.

The Processor will not disclose Personal Data except:

- as the Controller directs;
- as described in this DPA; or
- as imposed by mandatory legal provisions.

The Processor will not disclose Personal Data to a government agency unless required by law. If compelled to disclose Personal Data to a government agency, the Processor will, where possible, refer the requesting government agency to the Controller. As of the effective date of the DPA, the Processor represents that it has not been compelled by a governmental authority to disclose Customer Personal Data. The Processor will promptly notify the Controller of such request to allow the Controller to seek appropriate remedy unless prohibited by law. If the Processor is prohibited by law from providing such notification, the Processor will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow the Processor to communicate as much information to the Controller as soon as possible. The Processor will review any requests and challenge any request the Processor deems to be overbroad or inappropriate (e.g. where such request conflicts with Swiss, EU and member state's laws). If, after exhausting the steps described in this section, and the Processor remains compelled to disclose Personal Data, the Processor will disclose only the minimum amount of Personal Data necessary to satisfy the request.

The Processor will not provide any third party:

- direct, indirect, blanket, or unfettered access to Personal Data;
- encryption keys used to secure Personal Data or the ability to break such encryption; or
- access to Personal Data if the Processor is aware that such data is to be used for purposes other than those stated in the third party's request.

In support of the above, the Processor may provide the Controller's basic contact information to the third party.

The Parties and its Affiliates may only disclose the terms of the DPA to a regulator or Supervisory Authority to the extent required by law, such as for the purposes of notifications or approval. The Parties shall take reasonable endeavours to ensure that such regulator or Supervisory Authority do not make this DPA public.

The Controller is solely responsible for the decision on and the procedure for disclosing the information concerned to state authorities/governmental bodies and is to be assisted by the Processor to the best of its ability in the disclosure.

5 Processor Personnel

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

6 Security

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, the Processor shall in relation to the Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in applicable Data Protection Laws, irrespective of whether GDPR applies.

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

7 Data transfer

The Processor may not transfer or authorise the transfer of Data to countries outside Switzerland or the European Economic Area without the prior written consent of the Controller. If Personal Data processed under this DPA is transferred from Switzerland or a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on an adequacy decision issued by the Swiss authorities, or rely on the EU or Switzerland approved Standard Contractual Clauses for the transfer of personal data.

8 Subprocessors

The Processor shall not appoint (or disclose any Personal Data to) any Subprocessor unless required or authorised in writing by the Controller.

The Processor imposes on each Subprocessor to comply with the confidentiality obligations, notification obligations, transfer obligations and security measures relating to the processing of Personal Data, which obligations and measures must at least comply with the provisions of this DPA. The Processor acknowledges being jointly and severally liable for the compliance of the obligations imposed on the Subprocessor because of this DPA.

An overview of the Subprocessors that the Processor has enabled is included in Schedule 4. Change to the Subprocessors named in said Schedule or the use of further Subprocessors shall be permitted if:

- the Processor indicates such outsourcing to Subprocessors to the Controller in advance in writing or in an appropriate electronic form within a reasonable time, which may not be less than 14 days; and
- the Controller does not object to the planned outsourcing in writing or in a suitable electronic form to the Processor by the time of the disclosure or transmission of the data; and
- this is based on a contractual agreement in accordance with Article 9 FADP or Article 28 GDPR, which meets the level of data protection and security of data processing required for the processing.

9 Data Subject Rights

Considering the nature of the processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

The Processor shall

- promptly notify the Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and
- ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Applicable Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the Processor responds to the request.

10 Personal Data Breach

If the Processor becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Controller Data or Personal Data while processed by the Processor (each a "Security Incident"), the Processor will promptly and without undue delay notify the Controller of the Security Incident, investigate the Security Incident and provide the Controller with detailed information about the Security Incident and take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.

The notification to the Controller shall contain at least the following information:

- a description of the personal data breach incident;
- Information on the data and data sets concerned and the scope of the data subjects;
- a preliminary assessment of the likely consequences of the personal data breach;
- a description of the measures and/or proposals for measures already taken/to be taken by the Processor to avert or mitigate adverse consequences affecting data subjects.

Notification(s) of Security Incidents will be delivered to the Controller's Data Protection Officer or any other employee acting as a point of contact, by any appropriate communication means selected by the Processor, including emails.

The Processor shall make reasonable efforts to assist the Controller in fulfilling its obligation under applicable laws to notify the relevant authorities and data subjects about such Security Incident. The Processor shall inform the Controller immediately if a Supervisory Authority takes action against the contractor and this also concerns processing on behalf of the Controller carried out by the Processor.

The Processor's notification of or response to a Security Incident under this section is not an acknowledgement by the Processor of any fault or liability with respect to the Security Incident.

The Processor must notify the Controller promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Service.

11 Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required by the FADP, GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the processing of Personal Data by, and taking into account the nature of the processing and information available to, the Processor.

12 Deletion or return of Personal Data

The Processor shall not retain Personal Data longer than the duration agreed with the Controller and in no event longer than what is requested by the Data Protection Laws. If no such duration is set, then the retention duration shall be limited to the duration of the Agreement.

The Processor shall promptly and in any event within 10 business days of the date of the total or partial cessation of the Service involving the processing of Personal Data (the "Cessation Date"), delete or return in a Controller selected readable format all the Personal

Data, and delete all existing copies, unless the Processor is legally required to store (part of) the Personal Data.

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

13 Audit rights and inspections

Subject to this section or any other provisions of the Principal Agreement, the Processor shall allow the Controller to carry out checks on compliance with technical and organisational measures. The Processor shall cooperate and contribute to audits and inspections, in a swift and unlimited manner.

The Controller may perform such audits once per year or more frequently if required by Data Protection Laws applicable to the Controller, or by a Supervisory Authority. The Controller may use an independent third party to perform the audit on its behalf, provided the third party is mutually agreed to by the Controller and the Processor. Audits must be conducted during regular business hours, subject to the Processor's policies, and may not unreasonably interfere with the Processor's business activities. They must be notified at least 14 days in advance.

The Processor will provide reasonable resources and documentation necessary to support audits per the DPA, in particular to prove the implementation of the technical and organisational measures. Proof of the technical and organisational measures for compliance with the special requirements of data protection in general as well as those relating to the order can be provided by

- current attestations, reports or report extracts from independent bodies;
- suitable certification by an IT security or data protection audit.

If other proof enables the Controller to satisfy itself that the technical and organisational measures in accordance with Schedule 2 to this DPA are being complied with in a manner that is reasonable and in line with the protection requirements, this proof shall also be suitable.

The Parties agree that on-site inspections will take place at most once a year and are only necessary if compliance with the obligations of the Processor under Article 9 FADP or Article 28 GDPR cannot already be proven by evidence within the meaning of this section. In addition, on-site inspections by the Controller are to be justified under indication of the particular reason and are only permissible on more than one audit day per year in special exceptional cases.

Nothing in this section shall require the Processor to breach any duties of confidentiality owed to any of its customers or employees.

In the event of a necessary (on-site) inspection by the Controller on the Processor's premises, each party shall bear the costs incurred for the inspection, such as inspection, personnel and travel costs, itself. If the Processor's cooperation in connection with inspections exceeds the extent required according to this Section and if this is associated with higher inspection expenses or the commissioning of external service providers by the Processor, the costs incurred for this may be invoiced to the Controller according to the customary hourly and daily rates in the industry.

14 General Terms

Notwithstanding the foregoing, in addition to the applicable provisions set forth in the Principal Agreement, all notices and communications given under this DPA must be in writing and will be sent by email. The Controller shall be notified by email sent to the address: email. The Processor shall be notified by email sent to the address: email.

In the event of any conflict of inconsistency between the Data Protection Laws, this DPA, and the Standard Contractual Clauses (if any), the conflict or inconsistency shall be resolved by giving precedence in the following order: (i) terms of the Data Protection Laws; (ii) the Standard Contractual Clauses (if executed between the parties); and (iii) this DPA.

Regarding the termination of this DPA, the specific provisions of the Principal Agreement apply.

15 Governing Law and Jurisdiction

The choice of law and competent court comply with the applicable provisions of the Principal Agreement.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK. SIGNATURE PAGE FOLLOWS

For CONTROLLER (Controller):

____

Place, Date

____

Name, Title

____

Signature

For PROCESSOR (Processor):

____

Place, Date

____

Name, Title

____

Signature

For CONTROLLER (Controller):

____

Place, Date

____

Name, Title

____

Signature

For PROCESSOR (Processor):

____

Place, Date

____

Name, Title

____

Signature

Schedule 1: Description of the processing / Transfers

Describe the processing activities, the transfers and the Service offered by the Processor and covered by this DPA. Also indicate the frequency of transfers (continuous, weekly, monthly, etc.) and their purpose.

The Processor will store Personal Data at rest in COUNTRY.

The Processor will otherwise process Personal Data in COUNTRY.

Schedule 2: Technical and Organisational Measures

Describe below the appropriate technical and organisational measures to be taken by the Processor (and the Controller if needed).

Programs and Policies

Access Control

Business Continuity

Security

Privacy

Infrastructure, Network and Application

Back-ups

Logging and Monitoring

Personnel

Certifications, Audits, Attestations

Security Incidents

Schedule 3: Instructions of the Controller regarding the processing of Personal Data

The nature of the processing of the Personal Data is set out in the Principal Agreement and this DPA.

The duration of the processing shall be in accordance with the Principal Agreement, the Controller's instructions, and the terms of this DPA. In any case, the following data retention periods apply to the above-mentioned processing:

- List of applicable retention periods

The purposes of the processing are

- List of purposes

For the purposes of this DPA, the Processor's legitimate business operations consist of the following:

- List of different business operations conducted by the Processor for its own legitimate business operations (such as statistics)

When processing for its legitimate business operations, the Processor will not use or otherwise process Personal Data for profiling, or advertising or similar commercial purposes. In addition, where the Processor is processing this data for legitimate business operations, the Processor will process it only for the purposes set out above. To the extent the Processor uses or otherwise processes Personal Data in connection with its legitimate business operations, the Processor will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations.

The categories of data subjects are

- List of data subjects

The categories of Personal Data are

- List of categories of personal data

Schedule 4: Subprocessors

Operations and data processing	Name and Address	Personal data stored in or accessed from
IT Support		Countries
Cloud services		Countries