Data Protection Annex

The purpose of this Annex is to define the conditions under which the Service Provider, in its capacity as a Data Processor as defined below, undertakes to carry out the processing of Personal Data on behalf of the Client within the framework of the Agreement.

The Service Provider is authorized to process on behalf of the Client the Personal Data necessary to provide the Service. The nature of the operations performed on the Personal Data concern their storage and the Personal Data made available to the Users in a controlled manner. The purposes of the Processing, the list of the processed Personal Data and categories of Data Subjects are defined below.

1. Definitions

For the purposes of this Annex and notwithstanding any other definition in the Agreement, the capitalized terms herein, whether in the singular or plural, shall have the following meaning:

Data Subject: means any identified or identifiable natural person whose Personal Data is subject to Processing. An "identifiable natural person" is deemed to be a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identifying number or an online identifier.

Controller: means any entity determining the purposes and means of the Processing. For the purposes of the Agreement, the Client acts towards the Service Provider as the Controller.

Data Processor: means an entity processing Personal Data on behalf of, on the instructions of and under the authority of the Controller. When providing access to the Service, the Service Provider acts as a Data Processor.

Processing: means any operation or set of operations carried out, or not, by means of automated processes and applied to Personal Data or sets of Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or otherwise making available, alignment or combination, limitation, erasure or destruction.

Breach of Personal Data: means a security breach leading to the accidental, unauthorized, or unlawful destruction, use, loss, alteration, disclosure, or access to or of Personal Data transmitted, stored and/or otherwise processed.

2. Purpose of the Processing

The Service Provider is authorized to process on behalf of the Client the Personal Data necessary to provide the Services described in the STC.

The Personal Data are subject to the following basic processing activities:

Organization; Storage; Hosting; Maintenance; Consultation, Dissemination, Recording, Registration and Modification by the Client.

The purpose of the Processing is the execution of the Services described in the STC.

The Personal Data processed relate to the following categories of data:

- Identification data: name, surname, telephone number, e-mail address, User profile photograph.
- Professional data: position, organisation chart, etc.
- Connection data: logs.

- Internet data: cookies, IP address.

Personal Data are collected by the Client who enters or imports them on the platform hosting the Service. The Client also imports the documents necessary for the Processing, documents that may include Personal Data, and sets the levels of authorization to be granted to the Users of the Service.

3. General obligations

The Service Provider agrees to use commercially reasonable efforts to:

- process the Personal Data only for the purpose(s) that is/are related to the Services described in the STC.
- process the Personal Data in accordance with the Client's documented reasonable instructions. If the Service Provider considers that an instruction constitutes a violation of the GDPR or any other provision of EU or Member State law or of the laws of the United States or of any state or territory of the United States relating to data protection, it shall immediately inform the Client. In addition, if the Service Provider is required to transfer Personal Data to a third country or to an international organization under the EU law or the law of the Member State to which it is subject, it shall inform the Client of this legal obligation prior to Processing, unless the relevant law prohibits disclosing such transfer on important grounds of public interest.
- ensure the confidentiality of Personal Data processed under this Agreement.
- ensure that persons authorized to process Personal Data under this Agreement:
    - are committed to confidentiality or are subject to an appropriate legal obligation of confidentiality;
    - receive the necessary training in Personal Data protection.
- take into account, with respect to its tools, products, applications or services, the principles of Personal Data protection by design and Personal Data protection by default.

4. Client's instructions

The Service is a standard service that can be used by all clients in the same manner.

On the date of signature, the Agreement constitutes the written instructions of Processing, within the terms and limits of the Agreement, from the Client to the Service Provider.

5. Sub-Processing

The Service Provider shall have the right without the prior written consent of the Client to subcontract with one or more Subprocessors to carry out specific processing activities. Notice of change of Subprocessor(s) shall be given promptly by the Service Provider to the Client.

The Service Provider shall use commercially reasonable efforts to ensure that the Subprocessor provides the same level of service and processing as is required under the terms of the Agreement.

6. Right of information of Data Subjects

To the extent required by applicable law, the Client is responsible for providing information to the Data Subjects concerned by the Processing operations at the time of collection of the Personal Data.

7. Exercise of Data Subjects' rights

The Service Provider must respond, in the name and on behalf of the Client, to Data Subjects' requests to exercise their rights with regard to their Personal Information to the extent required by applicable law.

8. Notification of personal data breaches

The Service Provider shall notify the Client of any Personal Data breach not later than forty-eight (48) hours after having become aware of it and by email to the Client's Data Protection Officer or its Authorized Representative. This notification shall be accompanied by any useful documentation to enable the Client, if necessary, to notify the competent supervisory authority of the breach.

The notification shall at least:

- describe the nature of the Personal Data breach including, if possible, the categories and approximate number of Data Subjects affected by the breach and the categories and approximate number of Personal Data records affected;
- communicate the name and contact details of the data protection officer or other point of contact from whom additional information may be obtained;
- describe the likely consequences of the Personal Data breach;
- describe the measures taken or proposed to be taken by the Service Provider to remedy the Personal Data breach, including, if applicable, measures to mitigate its possible adverse effects.

If, and to the extent that, it is not possible to provide all of this information at once, the information may be provided in phases without undue delay.

Notification to the Data Subject is carried out by the Client, who alone is capable of assessing the risk to the rights and freedoms of a natural person.

9. Assistance of the Service Provider in the fulfillment of the Client's obligations

The Service Provider shall assist the Client in carrying out impact assessments relating to the protection of Personal Data.

10. Security measures

The Service Provider undertakes to implement the security measures set out in the SLA and the Agreement.

11. CCPA

If the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act) (the "CCPA") applies to any Personal Data provided to the Service Provider by the Client, the following terms shall apply, and each party agrees to provide the other party with all information and cooperation reasonably necessary to allow the other party to comply with any applicable obligation under the CCPA. Italicized terms have the meanings defined in the CCPA.

The Service Provider (i) will process any *Personal Information* among the Personal Data under the Agreement only for the *Business purpose* specified in clause 2 above, (ii) will not *sell* or *share* such *Personal Information*, and (iii) will not retain, use, or disclose such *Personal Information* other than as is permitted for the Service Provider to perform its obligations under the Agreement or the CCPA. If the Service Provider determines that it can no longer meet its obligations under the CCPA, it will inform the Client. The Client has the right, upon reasonable notice to the Service Provider, to take reasonable and appropriate steps to stop and remediate any unauthorized use of *Personal Information*.

12. Fate of Personal Data

At the termination of the Agreement, the Service Provider undertakes to destroy, to the extent physically possible, all Personal Data, to the extent that the Servicer Provider may destroy such Personal Data using commercially reasonable efforts and such destruction does not violate any applicable law, regulations, contractual obligations or policy of the Service Provider. Once destroyed, the Service Provider must certify the destruction in writing.

13. Record of categories of processing activities

The Service Provider declares that it keeps a written record of all categories of processing activities carried out on behalf of the Client, including:

- the name and contact details of the Client on whose behalf it is acting, of any Subprocessors and, where applicable, of the Data Protection Officer;
- the categories of processing carried out on behalf of the Client;
- in the express case of a court order, transfers of Personal Data to a third country or to an international organization, including the identification of such third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documents attesting to the existence of appropriate safeguards;
- to the extent possible, a general description of the technical and organizational security measures, including inter alia, as appropriate:
    - pseudonymization and encryption of Personal Data;
    - means to ensure confidentiality, integrity, availability and resilience of processing systems and services;
    - means to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident
    - a procedure to regularly test, analyze and evaluate the effectiveness of the technical and organizational measures to ensure the security of processing.

14. Documentation

The Service Provider shall make available to the Client the documentation necessary to demonstrate compliance with all of its obligations and to enable and assist in audits, including inspections, by the Client or another auditor appointed by the Client.

15. Data Protection Officer

The Service Provider's Data Protection Officer details is: contact-DPO@dilitrust.com