UBS

Global Supplier Policy

Data Protection Policy

WHY

To meet our legal and regulatory requirements.

WHEN

Whenever you Process any Personal Data which is shared for the purposes of the Agreement.

WHAT to know about HOW to comply

This Data Protection Policy applies as follows:

i) **sections 1-3 and 7-9 apply where you and we act as independent Controllers;** and

ii) **sections 1, 2 and 4-9 apply where you act as Processor on behalf of UBS as Controller**.

1. Processing of Personal Data

- You acknowledge that the factual circumstances dictate whether you act as a controller or processor. The Supply Order provides details of the Personal Data and purposes to be Processed by you in connection with this Agreement and the Parties' anticipated designation.

2. Our obligations as a Controller

- Where we are a Controller in respect of Personal Data Processed by you, we will comply with our obligations under Data Protection Laws.

3. Your obligations where you act as a Controller

- Where you act as a Controller in respect of Personal Data you must (and must ensure any third parties to whom you disclose such Personal Data):
  - not Process the Personal Data for any other purpose than those expressly set out within the Agreement, or to comply with your legal and regulatory obligations, or as agreed in writing with us; and
  - not sell Personal Data, or use or share for cross contextual behavioral advertising purposes; and
  - promptly notify us upon becoming aware of a Personal Data Breach, and, where reasonably practicable, provide a copy of any proposed notification and consider in good faith any comments made by UBS before notifying the Personal Data Breach to any third parties.

4. Your obligations where you act as a Processor

- Where you Process Personal Data as a Processor on our behalf, you must comply with all your obligations under Data Protection Laws and not knowingly cause us, as the Controller, to breach Data Protection Laws.
- You must promptly notify us if you become aware:
  - that you have received or are likely to receive Personal Data other than in accordance with the Agreement (and upon our request, promptly return to us or delete any such Personal Data received to us); or
  - of any non-compliance or reasonable suspicion of non-compliance with Data Protection Laws relating to the Processing of Personal Data under the Agreement.
- You must unless prohibited by Applicable Law:
  - only Process Personal Data (i) on our prior documented instructions and only to the extent necessary for performance of the Agreement, or (ii) to the extent required by Applicable Law. If an Applicable Law requirement is placed on you to Process Personal Data for other purposes, you must provide prior written notice to us;
  - promptly inform us if, in your reasonable opinion, our instructions breach, or will result in a breach, of Data Protection Laws;
  - promptly notify us of: (i) any request from Data Subject(s) exercising their rights under Data Protection Laws or other complaints or allegations from Data Subjects; and (ii) any requests from a Regulator in relation to Personal Data or the Processing of Personal Data in connection with this Agreement.
- You must provide all reasonable assistance and information to us, and within 10 Working Days of our request, to enable us to comply with our obligations under Data Protection Laws, which may include:
  - allowing for and contributing to audits (including inspections) by us or on our behalf not more than once per year, save for audits which are requested in relation to any Personal Data Breach or as you and we may otherwise agree;
  - fulfilling Data Subjects' requests;
  - taking necessary actions to minimize the impact of any complaints or allegations of Data Subjects (and to prevent their reoccurrence);
  - agreeing to additional provisions or obligations in relation to the protection and security of Personal Data;
  - conducting privacy impact assessments (and any related consultations); and
  - maintaining all documentation of processing operations.
- You must promptly delete or return to us all copies of Personal Data Processed by you in connection with this Agreement as we may reasonably request, save to the

extent that you are required by Applicable Law to retain a copy of the same.

5. Breach notification and assistance

- In the event you become aware of or suspect (or reasonably should have suspected) that there has been a Personal Data Breach, you must:
  - immediately investigate the Personal Data Breach to seek to identify, prevent and mitigate the effects of the Personal Data Breach (as the case may be) and to carry out any recovery or other action reasonably necessary to remedy the Personal Data Breach;
  - without undue delay and no later than 48 hours after becoming so aware or so suspecting, notify us in writing of the known or suspected Personal Data Breach (as the case may be) and follow up with a detailed description in writing. Such notice must contain at least the following details:
    i) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
    ii) a description of the causes of the Personal Data Breach;
    iii) a description of the likely consequences of the Personal Data Breach;
    iv) a description of the actions or remedial measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects; and
    v) the name and contact details of the data protection officer or other appropriate contact point where more information can be obtained;
  - update us as often as we reasonably require in the circumstances and in any event at least every 48 hours after the first notification;
  - promptly conduct, or support us in respect of, any investigation or analysis that we require;
  - promptly implement measures proposed in the notification and any additional actions or remedial measures which we consider necessary;
  - promptly support us in any notification of the Personal Data Breach to any Regulator and/or Data Subjects; and
  - promptly notify us of any new information relating to the Personal Data Breach and the identity of each affected Data Subject as soon as such information can be collected or otherwise becomes available.
- Unless required by Applicable Law, you must not notify any Regulator of any events set out in this paragraph without our prior written consent.

6. Security

- You must comply with the requirements of the Cyber and Information Security (CIS) Policy / Security Exhibit as applicable. In respect of backup and recovery management you must:
  - establish procedures to ensure the security of your information systems during disasters and other adverse situations, and periodically review the same; and
  - maintain data backup and recovery processes and procedures in order to ensure availability of UBS Data and operation of your information systems, in adverse situations.
  - ensure that all persons authorized to Process Personal Data on your behalf in connection with this Agreement are contractually bound to keep all such Personal Data confidential at all times during and after the term of this Agreement. Such contracts must be made available to us for inspection promptly upon request.

7. Restricted Transfers

- In the event of any Restricted International Transfer of Personal Data from or on behalf of us to you, you must take such measures as reasonably specified by us to ensure that such transfer complies with Data Protection Laws, and enter into (and ensure that such other persons or entities as we may reasonably specify enter into) our Supplier IDTA with us.
- If the Agreement is with a UBS entity registered in the United States, you must not transfer In-scope Personal Data to any "Country of Concern" or "Covered Person" or Process In-scope Personal Data in a way that would constitute a "Restricted Transaction" or "Prohibited Transaction," all as defined in the U.S. Department of Justice's Data Security Program ("28 C.F.R. § 202"). For purposes of this section, "In-scope Personal Data" means bulk U.S. sensitive personal data, as defined in 28 C.F.R. § 202.

8. Subprocessors

- You must take all reasonable steps to ensure that any subprocessors that you engage comply with the Agreement and applicable Data Protection laws. You will remain liable for the acts and omissions of your subprocessors. Approved subprocessors are specified in the Supply Order. Any new or replacement subprocessors during the term of the Agreement must also be approved by us in writing. If any subprocessor meets the definition of a "Subcontractor", the Subcontractor Policy will also apply.

9. Data Privacy Notices

- To the extent that you provide us with your employees' and contractors' Personal Data (other than business contact information), you must provide them with the applicable version of the UBS External Staff Privacy Notice, available here.

10. Other

- You must immediately inform us if you suspect that Personal Data which is in your possession or under your control is threatened with seizure or confiscation (including through bankruptcy or settlement proceedings or other actions of a third party). You will take all reasonable measures to protect our rights and position including informing all relevant third parties that ownership and control over the Personal Data lies with us