UBS

Global Supplier Policy

Data Protection Policy

WHY

To meet our legal and regulatory requirements.

WHEN

Whenever you Process Personal Data.

WHAT to know about HOW to comply

1. Details of Personal Data processed under the Agreement

- The Supply Order provides details of the Personal Data to be Processed by you in connection with the Agreement.

2. Our obligations as a Controller

- We are the Controller in respect of Personal Data Processed by you and will comply with our obligations under Data Protection Legislation in relation to Processing Personal Data.

3. Your obligations as a Processor

- You act as a Processor on behalf of us whenever you Process Personal Data. You must comply with your obligations under Data Protection Legislation.
- You must promptly notify us if:
  - you become aware that you have received or are likely to receive Personal Data as a Processor (and upon our request, promptly return any such Personal Data received to us); or
  - you become aware of any non-compliance or risk of non-compliance with Data Protection Legislation relating to the Processing of Personal Data under the Agreement.
- You must ensure that you:
  - only Process Personal Data on our prior documented instructions and only to the extent reasonably necessary for performance of the Agreement, or 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 unless this is prohibited by Applicable Law;
  - promptly inform us if our instructions would be in breach of Data Protection Legislation;
  - promptly notify us of any requests from Data Subjects exercising their rights under Data Protection Legislation or other complaints or allegations from Data Subjects, provide full cooperation to us with handling such requests (including by providing us with a written description of Personal Data held by you in relation to the Data Subject and a copy of such Personal Data within 15 days of our request) and take reasonable action necessary to minimise the impact of the request, complaint or allegation and prevent reoccurrence;
  - unless prohibited by Applicable Law, promptly notify us of any requests from a Regulator in relation to Personal Data or the Processing of Personal Data;
  - unless prohibited by Applicable Law, provide reasonable assistance to us within the timescales requested to enable us to comply with our obligations under Data Protection Legislation which may include agreeing to additional provisions or obligations proposed by us in relation to the protection and security of Personal Data, notifying us of any breach of Personal Data, conducting privacy impact assessments (and any related consultations) and maintaining all documentation of processing operations; and
  - not create any copies of Personal Data without our prior written consent, unless required for the Services.

4. Breach notification and assistance

- In the event you become aware of or suspect 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 in its sole opinion as a result of the Personal Data Breach;
- 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.

5. Security

- You must comply with the requirements of the Security Exhibit. 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.
- In respect of human resources security you must ensure the reliability and personal integrity of all Staff who have access to your information systems or UBS Data and that any Staff accessing UBS Data knows their obligations and the consequences of a security incident.
- You must procure that such Staff and all natural persons and legal entities with access to UBS Data are contractually bound to keep UBS Data confidential at all times during and after the term of this Agreement and/or the respective employment contract between you and Staff. Such contracts must be made available to us for inspection promptly upon request.

6. Restricted Transfers

- Without our prior written consent, you must not access or provide access to CID (in a Restricted Country) from outside a Restricted Country or transfer or allow the transfer of any CID outside a Restricted Country.
- In the event of any Restricted International Transfer of Personal Data from or on behalf of us to you, you must take such measures reasonably specified by us to ensure that such transfer complies with Data Protection Legislation, and enter into (or ensure that such other persons or entities as we may reasonably specify enter) our Supplier IDTA with us.

7. Subcontractors

- If you use any Subcontractor that Processes Personal Data, you must comply with the requirements of the Subcontractor Policy.

8. Notices

- You must provide the applicable version of the UBS External Staff Privacy Notice, available here, to any of your employees and contractors that you employ or engage in the provision of the Services to us.

9. 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.