UBS VENDOR STAFF PRIVACY NOTICE – NEW ZEALAND

DATA PROTECTION UNDER NEW ZEALAND PRIVACY ACT 2020

UBS takes your privacy seriously. This privacy notice contains information on what Personal Information UBS and its group companies ("**UBS**", "**we**", "**our**", or "**us**") collect, what they do with that information, and what rights you have. To run our business, UBS collects and uses information about living individuals (also known as "**Personal Information**"), including information about the employees and contractors of our suppliers.

As part of our commitment to protect your Personal Information in a transparent manner, we want to inform you:

- why and how UBS collects, uses and stores your Personal Information; and
- what your rights and our obligations are in relation to such processing.

1. What does this Privacy Notice cover?

This notice applies to any and all forms of use of Personal Information ("**processing**") by us in New Zealand

2. What type of Personal Information do we collect?

For the employees and contractors of our suppliers, we collect basic identification information, such as your name, title, position, professional history, experience, language skills and contact details. Such information will be collected if provided to us by your employer, for instance on a CV you have prepared, even if you do not ultimately work on an assignment for UBS.

In addition, for such employees and contractors working on UBS premises, we will usually collect the following, always according to the legal basis and purposes set forth in section 4 below:

- Detailed identification information (e.g. address, office location, business telephone number, date and place of birth, picture, emergency contact details, ID card, passport details and other national ID numbers as required);
- Detailed professional information (e.g. academic, professional and industry qualifications and certifications (including dates), previous employer contact details, directorship information, contact details of references, previous employment dates, rank or seniority, line manager contact information, working arrangements (such as full or part time), assignment allocation and absence information);
- Electronic identification data (e.g. login information, access right, badge number, IP address, online identifiers/cookies, logs and connection time, sound or image recording such as CCTV or voice recordings);
- Personal and physical characteristics (e.g. gender, date of birth and immigration status, including visa and/or permit numbers);
- Information submitted in support of an application to work for UBS on behalf of your employer (e.g. recordings of any video interviews in which you participate, and anything you choose to submit in support of your or your employer's application); and
- Where relevant, certain financial information and other information required to undertake background and periodic checks for money laundering, criminal activities, corruption, terrorist financing and related matters
- Where relevant and to the extent permitted by applicable law, diversity related information (including data about racial and ethnic origin, political opinions, religious beliefs and other beliefs of a similar nature, trade union membership and data about sexual orientation), or health data (such as sickness

records, disability records, smoker records, fitness for work and health insurance where it contains data relating to sickness) and data about alleged or proven criminal offences.

In some cases, the Personal Information we collect from you is needed to meet our legal or regulatory obligations, to perform our obligations under UBS's contract with your employer (UBS's supplier), or to enter into that contract. If so, we will indicate to you that the provision of this information is mandatory, and the consequences if we cannot collect this information.

In some cases, UBS will also collect Personal Information indirectly from background check providers such as First Advantage and other administration services providers (for instance Hays, who provide non-permanent workforce resources), or from publicly available sources such as LinkedIn profiles.

3. For which purposes do we process Personal Information?

We always process your Personal Information for a specific purpose and only process the Personal Information which is relevant to achieve that purpose. In particular, we process Personal Information of our suppliers' employees and contractors to:

- determine the suitability of prospective suppliers' employees' and contractors' qualifications, checking for any existing or potential conflicts of interest or any other restrictions which may otherwise restrict or prevent a prospective engagement on a matter with UBS, and to carry out periodic vetting checks where relevant;
- administer, plan and manage our personnel, suppliers and contractors (including task management and internal workforce analysis and planning);
- allocate costs, optimise performance and enhance quality;
- assist us in managing external providers such as your employer (see below for further information about when we work with third parties);
- implement tasks and plan activities in preparation of or under existing contracts;
- train our staff, suppliers and contractors;
- carry out supplier performance reviews, satisfaction surveys and other contractor surveys;
- monitor our suppliers' employees' and contractors' activities in the workplace, including compliance with banking regulations and internal policies as well as health and safety rules in place;
- manage our IT resources, including infrastructure management and business continuity;
- where relevant, manage and make available Personal Information within the UBS Group;
- receive and handle internal complaints or reports made to a compliance hotline;
- reply to an official request from a public or judicial authority with the necessary authorisation;
- comply with any legal obligations imposed on UBS in relation to its employees and contractors; and
- enable a transfer to a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of UBS's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it.

4. How do we protect Personal Information?

All personnel accessing Personal Information must comply with the internal rules and processes in relation to the processing of Personal Information to protect them and ensure their confidentiality. They are also required to follow all technical and organisational security measures put in place to protect the Personal Information.

We have also implemented adequate technical and organisational measures to protect Personal Information against unauthorised, accidental or unlawful destruction, loss, alteration, misuse, disclosure or access and against all other unlawful forms of processing.

5. Who has access to Personal Information and with whom are they shared?

5.1 Within the UBS Group

We make available Personal Information of our suppliers' employees and contractors to other companies of the group to which we belong (the "UBS Group"), for the purposes indicated in section 3.

5.2 Outside the UBS Group

For the purposes listed in section 3.2 above, and to the extent permitted under applicable law, we may also transfer Personal Information to third parties outside UBS and the UBS Group, such as:

a) third party service providers, who are contractually bound to confidentiality, such as IT system or hosting providers, payroll providers, third parties that provide benefits or help us provide benefits to our staff (such as third parties who administer the Compensation Plans on our behalf), transport companies for work travel, cloud service providers, database providers, consultants (e.g. lawyers, tax accountants labour consultants or recruitment agencies), training, education and development providers and third parties who carry out pre-employment checks on employees, and other goods and services providers (such as food service providers);

b) third parties that submit complaints, requests or reports to compliance or other units within UBS or the UBS Group;

c) a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of UBS's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it;

d) authorities, e.g. regulators, enforcement or exchange body or courts or party to proceedings where we are required to disclose information by applicable law or regulation or at their request, or to safeguard our legitimate interests;

e) other banks, market counterparties (including brokers, exchanges, upstream withholding agents; swap or trade repositories, stock exchanges, central securities depositaries) or client (as part of you working on tasks related to or involving those parties);

f) public or private social security bodies, trade unions (when the employee is a member) and trade unions internal representatives (including for the purposes of compliance with national collective bargaining agreements), and trade associations;

g) any central or local government department and other statutory or public bodies; or

h) any legitimate recipient required by applicable laws or regulations.

Where we transfer your data to third party service providers processing data on UBS behalf, we take steps to ensure they meet our data security standards, so thar your Personal Information remains secure. Third party service providers are thereby mandated to comply with a list of technical and organisational security measures, irrespective of their location, including measures relating to: (i) information security management; (ii) information security risk assessment and (iii) information security measures (e.g. physical controls; logical access controls; malware and hacking protection; data encryption measures; backup and recovery management measures).

5.3 Data Transfer to other Countries

The Personal Information transferred within or outside the UBS Group as set out in sections 5.1 and 5.2, is in some cases also processed in other countries. We only transfer your Personal Information abroad to countries which are considered to provide an adequate level of data protection, or in the absence of such legislation that guarantees adequate protection, based on appropriate safeguards (e.g. standard contractual clauses or another statutory exemption provided by local applicable law).

A list of the countries in which UBS operates can be found at
https://www.ubs.com/locations.html

6. How long do we store your data?

We will only retain Personal Information for as long as necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory or internal policy requirements (including for the facilitation and operation of the compensation plans). In general, although there may be limited exceptions, staff data is kept for the time period defined in the UBS Records Retention Schedule.

However, if individuals wish to have their Personal Information removed from our databases, they can make a request as described in section 7 below, which we will review as set out therein.

7. What are your rights and how can you exercise them?

7.1 Your rights

You may have a right to access and to obtain a copy of your Personal Information as processed by UBS. If you believe that any information we hold about you is incorrect or incomplete, you may also request the correction of your Personal Information.

You may also have the right to:

- request the erasure of your Personal Information; and
- request for information on the identities or types of third parties with whom your Personal Information is shared

In certain circumstances UBS may process your Personal Information through automated decision-making. Where this takes place, you will be informed of such automated decision-making that uses your Personal Information and be given information on criteria and procedures applied. You can request an explanation about automated decision making carried out and that a natural person reviews the related decision where such a decision is exclusively based on such processing.

UBS will honour such requests as required under applicable data protection rules but these rights are not absolute: they do not always apply and exemptions may be engaged. We will usually, in response to a request, ask you to verify your identity and/or provide information that helps us to understand your request better. If we do not comply with your request, we will explain why.

7.2 Exercising your rights

To exercise the above rights, please send an email to: sh-hr-data-requests-snow@ubs.com.

If you are not satisfied with how UBS processes your Personal Information, please let us know and we will investigate your concern. Please raise any concerns by contacting the Group Data Protection Office at: dpo-apac@ubs.com.

If you are not satisfied with UBS's response, you have the right to make a complaint to the Data Protection Authority. The contact details of the Data Protection Authority can be found at the following website: https://www.privacy.org.nz/

8. Changes to Personal Information

In the interests of keeping Personal Information properly up to date and accurate, we will ask you periodically to review and confirm the Personal Information we hold about you and/or to inform us of any change in relation to your Personal Information (such as a change of address).

9. Changes to this Privacy Notice

This notice was published in November 2020. It may be subject to amendments. Where there is a material change to this notice it will be communicated to you through an appropriate channel, depending on how we normally communicate with you.

10. List of UBS employing entities:

For employees and contractors of UBS New Zealand, the name and address of the relevant UBS employing entity which is collecting and holding your Personal Information is listed below.

Entity Name	Registered Address
UBS New Zealand Limited	Level 27, PwC Tower, 188 Quay Street, Auckland, 1010, New Zealand

If you have any questions or comments about this notice, please contact the Group Data Protection Office at the following email address: dpo-apac@ubs.com.