# UBS EXTERNAL STAFF PRIVACY NOTICE - THAILAND

## DATA PROTECTION UNDER THE THAILAND PERSONAL DATA PROTECTION ACT (PDPA)

To run our business, UBS processes information about individuals ("**Personal Data**"), including information about the employees and contractors of our suppliers ("**you**" or "**External Staff**").

UBS takes your privacy seriously. This Privacy Notice ("**Notice**") contains information on what Personal Data the UBS entity in Thailand referred to in Section 10 ("**UBS**", "**we**", "**our**", or "**us**") and other companies of the group to which we belong (the "**UBS Group**") collect(s) and what we do with that information.

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

- why and how UBS collects, uses and stores your Personal Data;
- what rights you have and our obligations in relation to such processing; and
- the lawful basis for the use of your Personal Data.

**Table of content**


| | |
|---|---|
| 1 What does this Notice cover? | 6 How long do we store your data? |
| 2 What type of Personal Data do we collect? | 7 What are your rights and how can you exercise them? |
| 3 For which purpose do we process your Personal Data and what legal basis do we rely on? | 8 Changes to Personal Data |
| 4 How do we protect Personal Data? | 9 Updates to this Notice |
| 5 Who has access to Personal Data and with whom are they shared? | 10 List of UBS contracting entities covered by this Notice |


### 1 What does this Notice cover?

This Notice applies to any and all forms of use of Personal Data ("**processing**") by UBS in relation to our External Staff in Thailand.

### 2 What type of Personal Data do we collect?

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 External Staff working on UBS premises, we usually collect (to the extent permitted by applicable law):

- 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), 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, and physical characteristics); and
- Information submitted in support of an application to work for UBS on behalf of your employer (e.g., and anything you choose to submit in support of your or your employer's application);

Where relevant and to the extent permitted by applicable law, the Personal Data that we collect will also include special categories of data, such as diversity related information (including data about racial and ethnic origin, and political opinions), or health data (for instance to allow UBS to make appropriate adjustments to your working environment as a result of a disability) and data about alleged or proven criminal offences in each case where permitted by law.

In some cases, the Personal Data 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.

The above-mentioned Personal Data are collected from information that you or your employer directly provide, and, in some cases, UBS will also collect Personal Data indirectly from background check providers such as First Advantage, and other administration services providers, or from publicly available sources such as LinkedIn profiles.

## 3 For which purpose do we process your Personal Data and what legal basis do we rely on?

### 3.1 Purposes of processing

We always process your Personal Data for a specific purpose and only process the Personal Data which is relevant to achieve that purpose. We thereby take into account the role in which you are active with UBS.

In particular, we process Personal Data of our External Staff to:

a) Selection. For example, to:
   - determine the suitability of External Staff qualifications;
   - prepare for and enter into a contract with our supplier.

b) Onboarding. For example, to:
   - set up internal profiles, collect information required to complete the onboarding process. For background checks please see section e) below;
   - assist us in managing external providers such as your employer (see section 5 for further information about when we work with service providers).

c) Staff Administration. For example, to:
   - administer, plan and manage our personnel, suppliers and contractors (including task management and internal workforce analysis and planning);
   - allocate costs, optimize performance and enhance quality;
   - where relevant, manage and make available Personal Data within the UBS Group;
   - carry out supplier performance reviews, satisfaction surveys and other contractor surveys;
   - track staff' interaction with internal email communication (including newsletters, interest groups and messages) to enable delivery of more relevant personalized content for improved readership and engagement.

d) Training, development and other staff offerings. For example, to:

- train our External Staff;
- carry out development initiatives and coaching activities;
- inform you of internal events, leisure activities, and corporate sponsored discounts through approved third-party providers.

e) Compliance & Risk Management and / or Crime Prevention, Detection & Investigation. For example, to:

- check 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;
- carry out periodic vetting checks where relevant;
- receive and handle complaints, requests or reports from employees or third parties made to a compliance function, HR function, or other designated units within UBS or the UBS Group;
- track relevant incidents related to our External Staff and / or persons they might have a connection with, in order to comply with legal or regulatory obligations, internal policies or for risk management purposes;
- monitor and investigate electronic communications in order to be able to comply with legal or regulatory obligations, including compliance with banking regulations and internal policies or for risk management purposes;
- track and record data accesses, to evaluate them and to scan data carriers as well as to evaluate the accessing or storage of data with the objective of ascertaining whether there has been a breach of the obligation to be task-related;
- conduct internal investigations in line with UBS policies and/or as required by applicable legislation;
- reply to any actual or potential proceedings, requests or the inquiries of a public or judicial authority.

f) Supporting, Enhancing and Maintaining UBS's technology. For example:

- to provide for a centralized, global approach to the provision of IT services to our External Staff and enable External Staff within the UBS group to interact with one another and UBS employees. This normally involves the hosting of your contact and e-mail information to allow UBS's global IT network to be established and populated with relevant details;
- to manage our IT resources, including infrastructure management and business continuity.

g) Other purposes:

- to exercise our duties and/or rights vis-à-vis you or third parties;
- to enable a transfer, merger or disposal to a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer, merger or disposal 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;
- to offer our products and services to our customers (e.g., we may communicate professional contact details of one of our employees to a customer or supplier, indicating that this person is the contact person within the UBS organization);
- to collect data to ensure the security of buildings as well as property and information located or stored on the premises, to prevent, and, if necessary, investigate unauthorized physical access to secure premises (e.g., maintaining building access logs and CCTV system images).

### 3.2 Basis for the processing of Personal Data

Depending on the purpose of the processing activity (see section 3.1), the legal basis for the processing of your Personal Data will be one of the following:

- necessary to comply with our legal or regulatory obligations, such as tax reporting or reference requirements;
- necessary to protect the vital interests of the relevant individual or of another natural person, such as providing disability access to places of work where applicable;
- necessary for the legitimate interests of UBS, without unduly affecting your interests or fundamental rights and freedoms and to the extent such Personal Data is necessary for the intended purpose (See below for more examples of legitimate interests of UBS);
- necessary for the performance of a task carried out in the public interest; or
- in some cases, and as may be requested from you from time to time, we have obtained prior consent (for instance where required by law), or processed with your explicit consent in the case of special category of Personal Data (such as your health data).

Examples of the "legitimate interests" referred to above are processing necessary:

- to benefit from cost-effective services, efficient solutions and subject-matter expertise (e.g., we may opt to use certain IT platforms offered by suppliers, or share basic Personal Data with another UBS entity if you transfer to that entity, for use by that UBS entity in conducting legally required background checks without collecting the information from you again (the UBS entity's use of that data will be notified to you at the time). We may also share Personal Data with another UBS entity so that a team with the appropriate subject-matter expertise can provide advice or support);
- to offer our products and services to our customers (e.g., we may communicate professional contact details of one of our External Staff to a customer or supplier, indicating that this person is the contact person within the UBS organization);
- to prevent fraud or criminal activity, misuses of our products, resources or services as well as the security of our premises, information, IT systems, architecture and networks;
- to provide for a centralized, global approach to the provision of IT services to our staff and enable staff within the UBS group to interact with one another. This normally involves the hosting of your contact and e-mail information to allow UBS's global IT network to be established and populated with relevant details;
- to monitor, investigate and ensure compliance with internal UBS policies, relevant laws or regulations;
- to cooperate with a request made in any actual or potential proceedings or the inquiries of a public or judicial authority.

To the extent that we process any special categories of data relating to you, we will do so because:

- the processing is necessary for the establishment, exercise or defense of a legal claim;
- the processing is necessary for reasons of substantial public interest; or
- you have given your explicit consent to us to process that information (where legally permissible).

## 4 How do we protect Personal Data?

All personnel accessing Personal Data must comply with the internal rules and processes in relation to the processing of your Personal Data to protect them and ensure their confidentiality.

UBS and the UBS Group have also implemented adequate technical and organizational measures to protect your Personal Data against unauthorized, accidental or unlawful destruction, loss, alteration, misuse, disclosure or access and against all other unlawful forms of processing.

## 5 Who has access to Personal Data and with whom are they shared?

### 5.1 Within the UBS Group

We make available Personal Data to members of our personnel and within the UBS Group for the purposes indicated in section 3.1. Other companies of the UBS Group may process your Personal Data on behalf and upon request of UBS.

### 5.2 Outside UBS and the UBS Group

#### 5.2.1 Third Parties

We share Personal Data with other credit and financial services institutions and comparable institutions (including brokers, exchanges, upstream withholding agents; swap or trade repositories, stock exchanges, central securities depositaries), with our professional advisers and consultants (e.g., lawyers, tax accountants or labour consultants) or clients as part of you working on tasks related to or involving those parties.

#### 5.2.2 Service Providers

In some instances, we also share Personal Data with our suppliers, who are contractually bound to confidentiality, such as IT system or hosting providers, payroll providers, cloud service providers, database providers, training, education and development providers and third parties who carry out vetting checks, and other goods and services providers (such as communication service providers). When we do so we take steps to ensure they meet our data security standards, so that your Personal Data remains secure.

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).

#### 5.2.3 Public or regulatory authorities

If required from time to time, we disclose Personal Data to public authorities, regulators or governmental bodies, courts or party to proceedings where we are required to disclose information by applicable law or regulation, under a code of practice or conduct, at their request, or to safeguard our legitimate interests.

#### 5.2.4 Other

- 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;
- Any legitimate recipient required by applicable laws or regulations.

### 5.3 Data Transfer to other Countries

The Personal Data transferred within or outside UBS and 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 Data 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 one of the following conditions:

- the transfer is based on appropriate safeguards including enforceable rights and effective legal remedies for data subjects;
- you have provided explicit consent to the transfer after being informed of the risks;
- the transfer is necessary for the performance of a contract between you and us or for the implementation of precontractual measures taken at your request;
- the transfer is necessary to comply with a legal obligation;
- the transfer is necessary for carrying out activities in relation to substantial public interest.

You may request additional information in this respect and obtain a copy of the relevant safeguard by contacting the Group Data Protection Office at dpo-apac@ubs.com. A list of the countries in which UBS and the UBS Group operate can be found at https://www.ubs.com/global/en/our-firm/locations.html.

## 6 How long do we store your data?

We will only retain Personal Data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory or internal policy requirement. In general, your Personal Data will be kept in our systems during your engagement with UBS and up to 10 years, from the day that your engagement with UBS terminates. There may be exceptions to this general rule, for example:

a) Personal Data that is no longer required or has become obsolete may be destroyed while the External Staff relationship is still ongoing for proportionality reasons;

b) In certain cases, UBS may store and process Personal Data for a longer period than 10 years, in particular for compliance or risk management purposes, to comply with (other) legal and regulatory requirements, or if it is in UBS' legitimate interest.

If you were previously or are currently a Credit Suisse External Staff: Your information after your transition to UBS will be stored as per above. However, your information prior to your transition to UBS and/or any activities performed under the Credit Suisse entities, will continue to be stored as per the applicable Credit Suisse retention requirements until the full integration of systems and processes into UBS are completed.

However, if you wish to have your Personal Data removed from our databases, you 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 have the right to access and to obtain information regarding your Personal Data that we process. If you believe that any information, we hold about you is incorrect or incomplete, you may also request the correction of your Personal Data.

You also have the right to:

- object to the processing of your Personal Data;
- request the erasure of your Personal Data;
- request restriction on the processing of your Personal Data; and/or
- withdraw your consent where UBS obtained your consent to process Personal Data (without this withdrawal affecting the lawfulness of any processing that took place prior to the withdrawal).

UBS will honour such requests, withdrawal or objection 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.

In certain circumstances UBS may process your Personal Data through automated decision-making. Where this takes place, you will be informed of such automated decision-making that uses your Personal Data 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.

### 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 data, please let us know and we will investigate your concern. Please raise any concerns by contacting the Group Data Protection Office under dpo-apac@ubs.com.

If you are not satisfied with UBS's response or you think we are not complying with any provision under the PDPA, you have the right to make a complaint to the Data Protection Committee.

## 8 Changes to Personal Data

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

## 9 Updates to this Notice

This Notice was updated in February 2026. We reserve the right to amend it from time to time. Any amendment or update to this Notice we will make available to you here. Please visit the UBS website frequently to understand the current Notice, as the terms of this Notice are closely related to you.

## 10 List of contracting UBS entities covered by this Notice

| Entity Name | Registered Address |
|---|---|
| UBS Securities (Thailand) Ltd | 195 One Bangkok Tower 4, 15th Floor, Unit 1505-1508, Wireless Road, Lumpini, Pathumwan, Bangkok, Bangkok, 10330, Thailand |
| CS Bangkok (Thailand) Limited | 93/1 GPF Witthayu Tower A, 2nd Floor, Wiresless Road, Lumpini, Pathumwan, Bangkok, 10330, Thailand |

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. For additional information please visit goto/groupdpo.