PRIVACY NOTICE FOR CLIENTS – BAHAMAS

DATA PROTECTION UNDER THE DATA PROTECTION ACT 2003 (DPA)

To run our business, UBS processes information about individuals ("**Personal Data**"), including information about our current and former clients ("**you**").

UBS takes your privacy seriously. This Privacy Notice ("**Notice**") contains information on what Personal Data the UBS Group entities in the Bahamas 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), what we do with that information, and what rights you have.

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;
- the lawful basis for the use of your Personal Data; and
- what your rights are in relation to such processing and how you can exercise them.

Table of Content

1 What does this Notice cover?

This Notice applies to any and all forms of use ("**processing**") of Personal Data by us in the Bahamas if you are a former, current or prospective client of any of the UBS entities listed in Section 10.

2 What types of Personal Data do we collect?

For former and current clients or prospective clients with whom we are taking steps to enter into a contractual relationship, we collect (to the extent permitted by applicable law):

- personal details such as your name, identification number, date of birth, compliance related documents (including a copy of your national identity card or passport), phone number, address and domicile, electronic address, and family details such as the name of your spouse or partner;
- financial information, including payment and transaction records and information relating to your assets (including fixed properties), financial statements, liabilities, taxes, revenues, earnings and investments (including your objectives);
- tax domicile and other tax-related documents and information;
- where relevant, professional information about you, such as your job title and work experience;
- details of our interactions with you and the products and services you use, including electronic interactions across various channels such as e-mails and mobile applications;

- any records of phone calls between you and UBS, specifically phone log information such as your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls;
- voice recording and communication data;
- where relevant, details of your nomination of a mandate;
- identifiers we assign to you, such as your client, business relation, partner or account number, including identifiers for accounting purposes;
- when you access UBS websites or our applications, data transmitted by your browser or device you are using and automatically recorded by our server, including date and time of the access, name of the accessed file as well as the transmitted data volume and the performance of the access, your device, your web browser, browser language and requesting domain, and IP address (additional data will only be recorded via our Website if their disclosure is made voluntarily, e.g., in the course of a registration or request). When you visit a UBS website, that website will contain additional information about how we use your information while you are visiting that website; and
- in some cases (where permitted by law), Sensitive Personal Data, such as your biometric information, political opinions or affiliations, health information, religious or philosophical beliefs, and, to the extent legally possible, information relating to criminal convictions or offences.

In some cases, we collect this information from public registers (which, depending on the product or service you receive and the country of the UBS entity with which you have a contractual relationship, may include beneficial ownership and other registers), public administration or other third-party or public sources, such as wealth screening services, credit reference agencies, fraud prevention agencies, intermediaries that facilitate data portability, and other UBS Group entities.

We might also collect certain of the above Personal Data types in relation to your business relationship, such as account holders, business partners (including other shareholders, or beneficial owners), dependants or family members, representatives or agents.

3 For which purposes 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. In particular, we process Personal Data, within applicable legal limitations, for the following purposes:

a) Client Onboarding:

- to verify your identity and assess your application. For legal and regulatory compliance checks (for example, to comply with anti-money laundering regulations, and prevent fraud), please see Section d) below.

b) Client Relationship Management:

- to manage our relationships with you including to communicate with you in relation to your account.

c) Product implementation and execution:

- to provide services to you ensuring their proper execution, for instance by ensuring that we can identify you and act in accordance with your instructions and the product terms.

d) Compliance and Risk Management and / or Crime Prevention, Detection and Investigation:

- to carry out legal and regulatory compliance checks as part of the onboarding process, including to comply with anti-money laundering regulations and fraud prevention;
- to meet our on-going regulatory and compliance obligations (e.g., laws of the financial sector, anti-money laundering and tax laws), including in relation to recording and monitoring communications, disclosures to tax authorities, financial service regulators and other regulatory, judicial and governmental bodies or in proceedings and investigating or preventing crime;
- to receive and handle complaints, requests or reports from you or third parties made to designated units within UBS or the UBS Group;
- to reply to any actual or potential proceedings, requests or the inquiries of a public or judicial authority;
- to prevent and detect crime, including fraud or criminal activity, misuses of our products or services as well as the security of our IT systems, architecture and networks;
- to undertake transactional and statistical analysis, and related research.

e) Supporting, Enhancing and Maintaining UBS's technology:

- to take steps to improve the use of technology, including testing and upgrading of systems and processes, and conducting market research to understand how to improve of our existing products and services.

f) Other purposes:

- for the UBS Group's prudent operational management (including technological support services, reporting, insurance, audit, systems and products training and administrative purposes);
- 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 collect data to ensure the security of buildings, the safety of staff and visitors, as well as property and information located, stored on or accessible from the premises, to prevent, and if necessary, investigate unauthorized access to secure premises (e.g., maintaining building access logs and CCTV system images to prevent, detect and investigate a theft of equipment or asset owned by UBS, visitor or staff, or threats to the safety of personnel working at the office);
- testing and calibrating analytical models. In such case only pseudonymized data are used;
- to exercise our duties and/or rights vis-à-vis you or third parties.

We use both automated (including artificial intelligence) and manual methods to process your Personal Data for these purposes. Our automated methods often are related to and supported by our manual methods. For example, our artificial intelligence systems may analyse your data to identify patterns and trends, which are usually manually reviewed and interpreted by humans.

3.2 Basis for 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 for taking steps to enter into or executing a contract with you for the services or products you request, or for carrying out our obligations under such a contract;
- required to meet our legal or regulatory responsibilities, including when we conduct the legal and regulatory compliance checks and make the disclosures to authorities, regulators and government bodies;

- 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); or
- in limited circumstances, 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 Sensitive Personal Data (such as your biometric data).

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

- manage our relationship with you and to help us to learn more about you as a client, and services you receive;
- to prevent fraud or criminal activity, misuses of our products or services as well as the security of our information, IT systems, architecture and networks and security of UBS premises;
- to receive and handle complaints, requests or reports from you or third parties made to designated units within UBS or the UBS Group;
- to take steps to improve our products and services and our use of technology and to conduct market research;
- to cooperate with a request made in any actual or potential proceedings or the inquiries of a public or judicial authority;
- certain situation when we make the disclosures referred to in Section 5 below, providing products and services and assuring a consistently high service standard across the UBS Group, and keeping our clients, employees and other stakeholders satisfied;

in each case provided such interests are not overridden by your privacy interests.

Where the Personal Data we collect from you is needed to meet our legal or regulatory obligations or enter into an agreement with you, if we cannot collect this Personal Data there is a possibility we may be unable to on-board you as a client or provide products or services to you (in which case we will inform you accordingly).

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

- the processing is necessary to carry out our obligations under local laws requiring such processing, such as Anti Money-Laundering;
- the processing is necessary for the establishment, exercise or defense of a legal claim;
- you have given your explicit consent to us to process that information (where legally permissible).

4 How do we protect Personal Data?

All UBS employees accessing Personal Data must comply with our 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 organisational measures to protect your Personal Data 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 Data and with whom are they shared?

5.1 Within the UBS Group

We usually share Personal Data with other UBS Group companies, for the purposes indicated in section 3.1, in order to ensure a consistently high service standard across our group, and to provide services to you. 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 Service Providers

In some instances, we share personal data with our suppliers, who are contractually bound to confidentiality, such as IT hardware, software and outsourcing providers, logistics, mail, courier, printing services and storage providers, marketing and communication providers, facility management companies, market data service providers, transportation and travel management providers and others. When we do so we take steps to ensure they meet our data security standards, so that your personal data remains secure.

Where UBS transfers your data to service providers processing data on UBS behalf, we take steps to ensure they meet our data security standards, so that your Personal Data 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).

5.2.2 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.

5.2.3 Others:

- 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 transfers 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 by the Data Protection Commissioner. In some cases, UBS can also transfer your Personal Data to Countries that do not guarantee adequate protection only if at least one of the following conditions is met:

- you have provided your consent to the transfer;
- the transfer is necessary for the performance of a contract between you and us, for the implementation of precontractual measures taken at your request, or for the performance of a contract concluded in your interest between us and a third party;
- the transfer is necessary to comply with a legal obligation on UBS;
- the transfer has been authorized by the Data Protection Commissioner

In any case, UBS transfers your data based on appropriate safeguards (e.g., standard contractual clauses adopted by the European Commission to the extent recognized by the competent Data Protection Authority or another statutory exemption) provided by local applicable law.

A copy of these measures can be obtained by contacting the Group Data Protection Office .If and to the extent required by applicable law, we implement the necessary legal, operational and technical measure and/or enter into an agreement with you before such transfers.

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 requirements. To help us do this, we apply criteria to determine the appropriate periods for retaining your Personal Data depending on its purpose.

We will keep your personal data for as long as you are our customer to allow us to provide you with the services and to meet our regulatory requirements, as specified in this document.

Once our relationship with you has ended (for example, after your account has closed or following a transaction such as a payment, your application for a product is refused, or you decide not to go ahead with an application), we will only keep your personal data for a period that is appropriate, which in many cases is up to 10 years after your account closes or following a transaction such as a payment. The period we keep information for is often linked to the amount of time available to bring a legal claim, required by law or regulations, or for compliance and risk management.

We will keep your personal data after this time if we have to do so by law, if there are existing claims or complaints that will reasonably require us to keep your information, or for regulatory reasons. If we do need to keep your information for a longer period, we will continue to protect that information. However, if you wish to have your Personal Data removed from our databases, you can make a request as described below, which we will review as set out therein.

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

7.1 Your rights

To the extent permitted by applicable laws, you have a 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 may also have the right to:

- object to the processing of your Personal Data;
- request the erasure of your Personal Data.

UBS will honour such requests, erasure 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.

7.2 Exercising your rights

To exercise the above rights, please send an e-mail to:

- HUBahamas@ubs.com, if you are a Credit Suisse AG, Nassau Branch client;
- sh-ibdiso@ubs.com if you are a Credit Suisse Brazil (Bahamas) Limited client;
- SH-HR-DATA-REQUESTS-SNOW@ubs.com, if you are a former UBS employee or candidate;

If you are not satisfied with UBS' response, you have the right to make a complaint to the data protection Commissioner in Bahamas. The contact details of the Data Protection Commissioner Office of the Bahamas can be found below:

31A Poinciana House, North Building
East Bay Street, P. O. Box N-3017
Nassau, N.P., The Bahamas –
E-mail: dataprotection@bahamas.gov.bs
Phone: (242) 604-1001

8 Changes to your Personal Data

We are committed to keeping your Personal Data accurate and up to date. Therefore, if your Personal Data changes, please inform us of the change as soon as possible.

9 Updates to this Notice

This Notice was updated in May 2024. We reserve the right to amend it from time to time.

10 List of UBS entities covered by this Notice:

Entity Name	Registered Address
Credit Suisse AG, Nassau Branch	Bahamas Financial Centre, 4th Floor, Shirley and Charlotte Streets, Nassau, P.O. Box N-3241, Bahamas
Credit Suisse Brazil (Bahamas) Limited	Bahamas Financial Centre, 4th Floor, Shirley and Charlotte Streets, Nassau, P.O. Box N-3241, Bahamas
Credit Suisse Trust Limited (Bahamas)	P.O. Box N3023 Bahamas Financial Centre Shirley & Charlotte Streets,

If you have any questions or comments about this Notice, please contact the Group Data Protection Office at dpo-americas@ubs.com