DIFC Private Banking Privacy Notice

HSBC Private Bank (Suisse) SA, DIFC Branch

HSBC Private Banking

PUBLIC

As you are a HSBC private banking client, we will naturally collect personal information about you.

This notice explains how we will use that information, who we might share it with, and what steps we will take to make sure it stays
private and secure. This notice continues to apply even if your agreement for banking or other products and services with us ends.

This notice applies to the personal data processed by HSBC Private Bank (Suisse) SA, Dubai International Financial Center ("**DIFC**") Branch. If we have provided you with separate or further information about how we collect and use your personal information for a particular product or service, those terms will also apply. If you interact with us in a different context, e.g., as a non-private banking client or in a country or jurisdiction outside the DIFC, separate terms might apply to that interaction.

Some of the links on our website lead to other HSBC or non-HSBC websites, with their own privacy and information protection policies, which may be different to this notice.

Before we begin

Wherever we have said "you" or "your", this means you and any Connected Person, as defined below.

"Connected Person" means an individual or entity whose information is provided by you to us or comes otherwise to our knowledge in connection with the services provided by us to you. In relation to you, a Connected Person may include, but is not limited to, (i) any director/officer of a company, (ii) a trustee, settlor or protector of a trust, (iii) any beneficial owner of your assets, (iv) a substantial interest owner (10% of the shares/votes of an entity or of its profits is deemed "substantial"), (v) a controlling person, (vi) a payee of a designated payment, (vii) one of your representative(s) or agent(s) or (viii) any other individual or entity having a relationship with you that is relevant to your business relationship with us.

Wherever we have said 'we' or 'our', this includes HSBC Private Bank (Suisse) SA, DIFC Branch and other HSBC group companies. HSBC Private Bank (Suisse) SA, DIFC Branch (1st Floor, Gate Village Building 8, P O Box 506553, Dubai, UAE) is the data controller in relation to your information relating to the DIFC Services.

Our representative (within the meaning of Article 27 of the EU General Data Protection Regulation (2016/679)) is HSBC Global Services (UK) Limited, 8 Canada Square, London E14 5HQ, United Kingdom.

What information we collect

The information we collect or have about you might come from different sources. It may include information relating to any of our products or services you may have applied for or held previously. Some of it will come directly from you, from an independent asset manager, from another advisor or from a business introducer. Some of it might come from other HSBC group companies or through your agents, which includes but is not limited to your trustees, professional advisers, investment advisers, investment managers or any other third party who instructs us or communicates with us on your behalf, such as your personal assistants. Some of it we might find from publicly available sources, which we have lawfully accessed. Some of it might come from other organisations. Some information may be the result of combining different sets of information (e.g., location information if you have a mobile app, where you have switched on your location permissions).

This information may include in particular:

Information that you provide to us. This includes:

- information about you that you give us by filling in forms or by communicating with us, whether face-to-face, by phone, e-mail, on-line or otherwise;
- contact details (name, address and other contact details such as date and place of birth, and nationality);
- information concerning your identity (e.g., passport information).

Information we collect or generate about you. This includes in particular:

- client relationship information, payment and trade transaction information and other financial information;
- information regarding your financial situation (e.g., information regarding your creditworthiness);
- information we collect to comply with our anti-money laundering obligations);
- authentication information (e.g., template signature and your biometric information);
- geographic information;
- information included in relevant client documentation and other comparable information;
- marketing and sales information, such as details of the services you receive;
- cookie information. We may use 'cookies' and similar technologies on websites and in emails to recognise you, remember your references and show you content we think you are interested in and this may include collecting

information about you. As the case may be, please see our Cookie Policy (available on www.hsbcprivatebank.com) for more details about how we use cookies.

- Information we obtain from other sources. This includes in particular:

    - communication information (e.g., information about you contained in emails, chat messages or other digital communications); and
    - information from publicly available sources and combined information from external sources (e.g., corporate and media broadcasts, information pertaining to social interactions between individuals, organizations, prospects and other stakeholders acquired from companies that collect combined information).

See Appendix 1 for additional details on the information we collect and process about you

How we'll use your information

We will collect information about you for various reasons as set out in this notice, including to:

- deliver our products and services, or process your transactions;
- check you are who you say you are;
- gather insights from information through data analytics;
- carry out your instructions;
- improve our products and services;
- keep track of our conversations with you (by phone, in person, by email or any kind of communication);
- manage our relationship with you – including telling you about our products, or carrying out market research;
- prevent or detect crime including fraud and financial crime;
- correspond with legal advisers and third party intermediaries;
- manage our internal operational requirements for credit and risk management, system or product development and planning, insurance, audit and administrative purposes.

Processing for any of the above purposes is necessary to enable us to pursue our legitimate business interests (or the legitimate business interests of one or more of our affiliates). It may also be necessary for other reasons, as outlined below.

We will only use your information where we have a lawful basis for using it. These lawful bases include where:

- we need to pursue our legitimate business interests;
- we need to process the information to perform our contract with you;
- we need to process the information to comply with a legal obligation;
- the use of your information as described is in the public interest, such as for the purpose of preventing or detecting crime; and
- we have your consent.

See Appendix 2 for additional details on how we use your information

Even if you ask us not to use your information, we may continue to use your personal information in circumstances where (a) the law says we have to; (b) we need to for the purposes of performing a contract; (c) we have a public interest to do so; or (d) we have a legitimate business reason for doing so (which may, in exceptional circumstances, override your interest that we no longer process your personal data).

Profiling / Automated Decision Making

We reserve our right to analyse and evaluate personal data in an automated manner in the future, so as to identify significant personal characteristics of yourself or to predict developments and to create client profiles. These may in particular be used for business-related checks, individual management, advisory or financial services and the provision of offers and information that we, or our affiliates, may make available to you.

When providing you with our services, we may make decisions about you by automated means. For example, we use technology that helps us identify the level of risk involved in client or account activity (e.g., for credit, fraud or financial crime reasons. For example, we may also use information received by third party providers to identify if someone else is using your card without your permission. You have a right to certain information about how we make these decisions. We ensure that a suitable contact person is available if you wish to express a view on any automated individual decision where such opportunity to express a view is required by law. Please refer to the section "More details about your information" below.

Tracking or recording what you say or do

We may record and keep track of conversations you have with us – including phone calls, face-to-face meetings, letters, emails, live chats, video chats and any other kinds of messaging in order to use these recordings to check your instructions to us, assess, analyse and improve our services, train our people, manage risk or to prevent and detect fraud and other crimes. We

use closed circuit television (CCTV) in and around our branches and offices for security purposes and so we may collect photos or videos of you, or record your voice through various video and telephony systems such as CCTV.

Marketing and market research

We may use your information for marketing purposes. We may send you marketing messages by email, text, phone, sms or secure
messages with information about our products and services. Even if you tell us not to send you marketing messages, we will continue to use your contact information to provide you with important service information, such as changes to your terms and conditions and account statements, or where we're required to do so by law.

We may use your information for market research and statistical purposes.

Who we might share your information with

We may share your information with our affiliates or with entities external to the HSBC group where:

- we need to for the purposes of providing you with products or services you have requested (e.g., opening an account for you, or performing our contract with you, e.g., to fulfil a payment request);
- we have a public or legal duty to do so (e.g., to assist with detecting fraud and tax evasion, financial crime prevention, regulatory reporting, litigation or defending legal rights);
- we have a legitimate reason for doing so (e.g., to manage risk, verify your identity, or assess your suitability for products and services); or
- we have asked you for your permission to share it, and you have agreed.

We may transfer and disclose your information to:

- other HSBC group companies and any contractors (see also below), sub-contractors, agents or service providers who work for, or provide services to us, or other HSBC group companies (including their employees, sub-contractors, directors and officers);
- any joint account holders, trustees, beneficiaries or executors where appropriate for trust accounts, the people who do your banking for you, the people you make payments to, your beneficiaries, intermediary, correspondent and agent banks, clearing houses, clearing or settlement systems, market counterparties, upstream withholding agents, swap or trade repositories, stock exchanges, and any companies you hold securities in through us (e.g., stocks, bonds or options);
- other financial institutions, tax authorities and debt recovery agents;
- any independent asset manager who provides asset management or advisory services to you and any other financial intermediary or business introducer who introduces you to us or deals with us for you;
- any person, company or other entity that has an interest in or takes on the risk in relation to or in connection with the products or services that we provide to you;
- any prospective or new HSBC companies (e.g., if we restructure, or acquire or merge with other companies) – or any entity that buys part or all of any HSBC group entity;
- auditors, regulators or dispute resolution bodies to comply with their requests;
- other companies who do marketing or market research for us (but not without your prior permission);
- if there is a dispute over a transaction, anyone else who is involved;
- law enforcement, government, courts, credit bureaus or our regulators;
- our card processing supplier(s) process your payments, issue and manage your card.

Contractors are third parties that process personal data on our behalf. If personal data is disclosed to contractors, they are only permitted to process the data received to the extent that we are permitted to do so. We select our contractors carefully and contractually require them to guarantee confidentiality, bank-client confidentiality and the security of personal data. Depending on the kind of product or service that is used, personal data may also be disclosed to contractors located outside of the DIFC. Please refer to the section "Transferring your information outside of DIFC" below for further information on this topic.

Sharing Aggregated or Anonymised Information

We may share aggregated or anonymised information outside of the HSBC group with partners such as research groups, universities or advertisers. For example, we may share such information publicly to show trends about the general use of our services. However, you will not be able to be individually identified from this information.

How long we'll keep your information

We will keep your information for as long as you have a relationship with us or use our platforms (e.g., our website and mobile apps). We will continue to keep information after you stop banking with us or stop using our platforms, for instance, (i) to respond to enquiries and complaints, (ii) to comply with laws and regulations, or in accordance with our internal policies and procedures, or (iii) to protect our interests.

There may be occasions where for technical reasons we are unable to delete your personal data. Where this is the case, we will apply appropriate technical and organizational security measures to keep your personal data secure or archived in a manner that it is put beyond further use. We are continually working towards technical solutions to permanently delete the information, when available.

Transferring your information outside the DIFC

Your information may be transferred to, and stored at, a destination outside the DIFC, including locations which may not have the same level of protection for personal information as the DIFC. We may need to transfer your information in this way to perform our contract with you, to fulfil a legal obligation, to protect the public interest and/or for our legitimate business interests, for example in the context of an outsourcing project. The recipient of your information outside of the DIFC may be an HSBC group affiliate or a third party.

Where we transfer your information outside the DIFC, we will ensure that it is protected by us in a manner that is consistent with
how your information will be protected by us in the DIFC. We will always do this in a way that is permissible under data protection rules.

Depending on the kind of product or service that is used, personal data may also be disclosed to third parties domiciled in countries
which do not have an appropriate level of data protection. If data is transferred to such a country, we take appropriate measures (e.g., contractual arrangements (such as the DIFC or EU Standard Contractual Clauses - see Article 27(2)(c) of the DIFC Data Protection Law 2020 or other precautions or justifications) so that personal data continues to receive appropriate protection.

You can obtain more details of the protection given to your information when it is transferred outside the DIFC by contacting us in
accordance with the "More details about your information" section below.

Your rights

You have a number of rights in relation to the information that we hold about you. These rights include:

- the right to obtain information regarding the processing of your information and access to the information which we hold about you (we will notify you of the personal data in our databases, including available details about the origin of the data, the purpose and, where appropriate, the legal basis for the processing and the categories of the processed personal data, the parties involved in the data collection and the data recipients. Please send us requests for information in writing, together with a clearly legible copy of a valid official ID document (e.g., passport, ID card, driving licence));
- in certain circumstances, the right to withdraw your consent to our processing of your information at any time. Please note, however, that we may still be entitled to process your information if we have another legitimate reason for doing so and your withdrawal of consent will not affect the lawfulness of processing taken place previously;
- in some circumstances, the right to receive some information electronically and/or request that we transmit the information to a third party where this is technically feasible. Please note that this right only applies to information which you have provided to us;
- the right to request that we rectify your information if it is inaccurate or incomplete;
- the right to request that we erase your information in certain circumstances. Please note that there may be circumstances where you ask us to erase your information but we are legally entitled to retain it;
- the right to lodge a complaint with the DIFC Commissioner of Data Protection (details of which are provided below) if you think that any of your rights have been infringed by us.

You also have the right to object to, and the right to request that we restrict, our processing of your information in certain circumstances. That being said, there may be circumstances where you object to, or ask us to restrict, our processing of your information but we are legally entitled to continue processing your information. However, we will not use your information for direct marketing purposes if you ask us not to do so.

You can exercise your rights by contacting us using the details set out in the “More details about your information” section below. You can find out more information about your rights by contacting the DIFC Commissioner of Data Protection, or by visiting the website at www.difc.ae/laws-regulations/data-protection.

Fraud and Money Laundering

To comply with the law and in our own legitimate interest we may also use your information to verify the accuracy of the information
you have provided to us in order to enable us to assess and manage risk and to prevent criminal activity, fraud and money laundering.

What we expect from you

You are responsible for making sure the information you give us is accurate and up to date. And you must tell us if anything changes, as soon as possible. If we ask you for any information and you do not provide it to us, we may stop providing existing services to you.

If you give us any information about another person connected to your account (such as a Connected Person as defined above), you must tell them what information you have given to us, and make sure they are informed of the content of this notice and agree we can use it as set out in this notice. You must also tell them how they can
see what information we have about them and correct any mistakes.

How we keep your information secure

We implement internal technical and organisational measures to keep your information safe and secure which may include encryption, anonymisation and physical security measures. We require our staff and any third parties who carry out any work on our
behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate
measures for the use and transfer of information.

More details about your information

If you would like further information on any of the information above, please address questions, comments and requests to our Data Protection Officer via email at: pbbusinessmanagement@hsbcpb.com. Also, if we do not meet your expectations with respect to the processing of personal data or you wish to complain about our data protection practices, please contact our Data Protection Officer. This gives us the opportunity to examine your issue and make improvements, where necessary.

This notice is available on our website: https://www.hsbcprivatebank.com/en/utilities/privacy-statement

Appendix 1 – Information we collect and process about you

The personal data which we collect and process about you (and/or any Connected Person) falls within the following categories:

A. **Personal identification data**

Personal identification data means:

- Contact details, such as name, address and contact information, date and place of birth, contract/account number(s) and duration, information about (i) the account, (ii) concluded transactions and (iii) Connected Persons;
- Identification information, such as identification documents (which may contain a picture);
- Sensitive personal data, which refers to personal data revealing:
  - racial, communal, or ethnic origin;
  - political opinions, religious or philosophical beliefs or trade union membership;
  - genetic data, biometric data for the purpose of uniquely identifying a natural person;
  - data concerning health
- Note: We may also collect and process personal identification data about prospective clients (which may (or may not) include persons who have a link with you (e.g., family or business relationship)). This information includes:
  - Personal identification data listed in the three bullet points above (Contact details / Identification information / Sensitive personal data);
  - Information on potentially applicable products or services, client acquisition likelihood and lifecycle, as well as sales pipeline information; and
  - Personal data necessary to perform background checks and other verifications before initiating a business relationship with a prospective client, as required in particular pursuant to the anti-money laundering regulatory framework applicable to us.

B. **Transactional data**

Transactional Data means:

- Client relationship data, such as information regarding your financial situation, products held and services rendered (including pricing information);
- Payment transaction data, such as records from payment processing systems that contain the information about executed transactions and includes order information (e.g., a payment order), payment information and other information deriving from the fulfilment of contractual and legal obligations;
- Securities transaction data, such as records from securities transaction systems that contain the information about executed transactions and includes order information (e.g., a purchase or a sell order), payment information and other information deriving from the fulfilment of contractual obligations, information about exchanges in ownership of cash, securities or financial instruments between individuals or organizations through an exchange (e.g., an organized market) or over the counter (OTC), which results in one or more transaction(s) recorded in the account(s);
- Credit data, such as information regarding creditworthiness, individual credit application history, credit decision variables and assumptions, credit scoring/ratings, likelihood estimates that you cannot meet the commitment you have entered into, calculated exposures, allocated credit lines and loan products, credit account arrangements and credit mitigants (e.g., collateral agreements and posted collateral).

C. **Risk management data**

Risk management data means:

- General risk data:
  - such as predicted transactional behaviour, client due diligence and periodic review results, Financial Crime Risk Management (FCRM) rating (high/medium/low), screening alerts (e.g., transaction screening, name screening, anti-money laundering information);
  - such as information collected and processed to assess the suitability/appropriateness of certain financial products, your client investment profile (recording in particular your investment objectives, your investment knowledge and experience, as well as your risk appetite and your ability to absorb losses), your possible characterization as a qualified investor (or similar characterization);
- Tax data, such as information regarding the source and tax status of assets held on the account(s) or transiting through the account(s) and information on your proper tax status;
- Credit risk data, such as credit risk ratings and risk identification information, risk and investment profiles, individual credit impairments;
- Information collected to fulfil our duties under the anti-money laundering regulatory framework, such as information regarding your personal/educational/professional background (including your possible characterization as a Politically Exposed Person (PEP)), information requested to clarify certain transactions, your client profile (which is established to comply with the applicable Know Your Customer (KYC) rules);

- Data pertaining to known or suspected risk associated with clients, such as information acquired from external watch lists or intelligence reports and internal risk intelligence systems;
- Investigation data, such as information pertaining to results from investigations on our business practices, processes and operations, as well as content and meta-data related to exchanges of information between and among employees, service providers, other stakeholders or entities of the HSBC Group;
- Complaint information, such as information connected to disputes/litigation/complaints (e.g., legal case and matter information, document productions, depositions and court transcripts, legal billing and time booking information, correspondence between legal advisors and stakeholders, minutes of face-to-face meetings).

D. **Communication data**

Communication data means:

- Data regarding our interactions with you, such as information collected and processed through the channels and modes of interaction with us (e.g., recorded telephone conversations, call history, emails, chat messages, digital communications, visits and face-to-face meetings);
- Data regarding interactions about you, such as information collected and processed through the channels and modes of interaction (e.g., recorded telephone conversations, call history, emails, chat messages, digital communications, visits and face-to-face meetings) between our employees (as well as employees of other entities of the HSBC Group) and our service providers (as well as service providers of other entities of the HSBC Group) about you.

E. **Marketing data**

- General marketing data, such as information on your needs, wishes and preferences;
- Social data, such as data acquired from external information aggregators. The information is typically user-generated and/or provided by and includes information from sources such as LinkedIn, Facebook, Google Plus or Twitter.

F. **Technical data,** such as internal and external identifiers, business numbers, IP addresses, records of access or records of changes.

Appendix 2 - How we use your information

We will use your information for the following purposes:

1. Deliver our products and services, or process your transactions: We will use your information to provide you with our products and services and to process your transactions (e.g., payments, invoices, accounts, credit/debit cards, financing, advisory and asset management services, financial planning, investments, stock exchange transactions, pension plans, incorporation of legal entities, succession planning, insurance services and electronic financial services). We will do this in line with our legitimate business interests, our legal obligations and in order to perform our contract with you.

2. Banking operations support: We will use your information to enable and facilitate the provision and productivity of our banking services in line with regulations, laws and client rights and interests (e.g., complaints management and exit management). We will use your information to carry out administration services, accounting, IT operations and infrastructure management, inventory/asset management and analytics.

We will also use your information to provide you with services and assess the performance of these services in line with regulations, laws and client rights and interests. The lawful bases for these personal data processing activities are our legitimate business interests, our legal obligations and the performance of our contract with you.

3. Online banking, mobile apps and other online product platforms: When using HSBC online platforms and mobile apps, we use your information to allow us to provide you with these platforms. The platform may allow you to directly or indirectly communicate with us (e.g., online bank products and services). The lawful basis for using your information for this purpose is to perform our contract with you.

4. Compliance with laws and regulations: We will use your information to comply with the law and any relevant rules or regulations. This may include to help detect or prevent crime (including terrorism, money laundering, other financial crimes and implementation of international sanctions), filing of relevant reports to regulators, disclosing information to authorities, regulators or government agencies to fulfil our legal obligations. These personal data processing activities are carried out to comply with our legal obligations, because it is in the public interest and because it is in our legitimate business interest to do so.

5. Preventing and detecting crime: We will use your information to take measures to prevent crime including fraud monitoring and mitigation and fraud risk management, carrying out client due diligence, name screening, transaction screening and client risk identification, in order to comply with our legal obligations, because this is in the public interest and because it is in our legitimate business interest to do so. We may share your information with law enforcement authorities and other third parties (in the DIFC and abroad) where the law allows us to do so for the purpose of preventing or detecting offenses. This includes legal or regulatory disclosure, notification or reporting obligations vis-à-vis civil, criminal or administrative authorities (in the DIFC or outside of the DIFC), compliance with official orders or statutory/regulatory duties (e.g., automatic exchange of information with foreign tax authorities, injunctions from the Dubai Financial Services Authority or, communications made with respect to obligations under the UAE's Anti-Money Laundering framework.

Additionally, we may take steps to help prevent financial crime and manage risk where we have a legal obligation or legitimate business interest to do so, or if this in the public interest, such as where it is important to prevent or detect crime. We may be required to use your information to do this, even if you have asked us to stop using your information. That could include (among other things):

- screening, intercepting and investigating any payments, instructions or communications you send or receive (including drawdown requests and application forms);
- investigating who you are paying or who is paying you (e.g., checks on payments in and out of your account
- combining the information we have about you with information at the disposal of other HSBC group entities;
- checking whether the people or organisations you are paying or receiving payments from are who they say they are, and are not subject to any international sanctions.

6. Risk management: We will use your information to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or client risk. This includes credit risk, market risk, trading risk, operational risk and insurance risk. We will do this to fulfil our legal obligation and also because we have a legitimate business interest in using your information for these purposes.

7. Security and business continuity: We will use your information to take measures to aid business continuity, information security and physical security activities. The lawful bases for processing your information for these purposes are the fulfilment of our legal obligations and the implementation of an internal risk strategy as required by our legitimate business interest.

8. Product & service improvement: We will use your information to identify possible service and product improvements (including profitability) by analysing your information (e.g., assessing the use of bank products and services, assessing financial

returns, developing ideas for new (or assessing existing) products, services, procedures or technologies). The lawful basis for processing your information for this purpose is our legitimate business interests.

9. Marketing: Save to our head office and for the purposes of the provision of group services by relevant affiliates, neither we nor our affiliates shall make any marketing approaches to you with regard to any other products and services that we or they provide. If there is any product or service information that we believe is of particular interest to you, then you shall be contacted personally by us in this respect. The lawful basis for this personal data processing is our legitimate business interest.

10. Data analytics for client targeting: We will perform analysis on your information to identify relevant opportunities to promote our products and services to existing or prospective clients. This may include reviewing historical client transactional behaviour or comparison of client activity so we can provide more targeted products and services. The lawful basis for this personal data processing is our legitimate business interests.

11. Information as a product: Where we collect your information for another purpose (e.g., for client on-boarding), we may, subject to compliance with our confidentiality obligations, share such information or analytics results with third parties including other HSBC group entities where it is in our legitimate business interest to do so.

12. Protecting our legal rights: We may need to use your information to protect our legal rights such as in the case of defending, or the protection, of our legal rights and interests, or those of our clients (including yourself). This includes collecting money owed, defending rights of intellectual property, court actions, managing complaints or disputes, managing claims against ourselves, yourself or other of our clients.

We may also need to use your information in the event of a restructuring of companies or merger and acquisition (M&A) transactions. We will do this in line with our legitimate business interests and our legal obligations.