

# Data Protection Information

The following data protection information gives an overview of our collection and processing of your data.

## **Duties of disclosure upon collection of personal data in accordance with the Data Protection Legislation.**

Data privacy is important – please read this document.

The entities and establishments listed in section 12 of this statement have issued this Privacy Statement in light of the enactment of the Data Protection Legislation.

With the following information, we<sup>1</sup> would like to give you an overview<sup>2</sup> of how we will process your personal data and of your rights according to Data Protection Legislation (as defined below). The details on what data will be processed and which method will be used depend significantly on the nature of your business relationship with us and (if you are a client) the services applied for or agreed upon.

“**We**”, “**us**” and “**our**” as used in this statement refers to each and any of the entities and establishments listed (as the context requires) as responsible for data processing in section 12 of this statement. In certain situations, multiple entities can be independently responsible for data processing at the same time and/or in different jurisdictions (e.g. when you sign an agreement with several UBS Group entities).

“**You**” and “**your**” as used in this statement refers to individuals:

- with whom we come into contact, or in respect of whom we obtain personal data, in the usual course of dealings with our clients, our service providers, and our other business counterparties or transaction participants, which may include, without limitation, employees, directors, officers, beneficial owners and other personnel of such clients, service providers, business counterparties or transaction participants (each a “**Connected Individual**”), in all cases outside the UBS group (as

---

<sup>1</sup> As a result of the acquisition of Credit Suisse Group by UBS Group, all entities of Credit Suisse Group have become UBS Group entities. Accordingly, the references to “Credit Suisse Group” (and similar references, e.g. “Credit Suisse entities”, “affiliates”, etc.) also include the UBS Group entities.

<sup>2</sup> If the entity responsible for processing your personal data is domiciled in Brazil, please refer to Appendix II for additional information.

- applicable to you, “Your Organisation”); or
- who themselves are our clients.

“**Data Protection Legislation**” means any law and/or regulation (including guidance and codes of practice issued by authorized data protection regulators) in the countries where we operate, which is applicable to the processing of your personal data by us, and which shall include, but is not limited to the laws and regulations indicated in Appendix I to this Data Privacy Statement (all as may be amended, extended, consolidated or re-enacted from time to time).

## 1) What sources and data do we use?

### **Data from you:**

We process personal data about you that we obtain from you in the context of our business relationship with you and / or Your Organisation (as applicable). We do this in order to facilitate, enable and / or maintain that relationship and / or to provide services to our clients or for other reasons specified below. In addition, in carrying on our business relationship with you or Your Organisation, information may be collected about you indirectly from monitoring or other means (e.g. recording of telephone calls and monitoring e-mails). In these circumstances, the information is not accessed on a continuous or routine basis, but it may be used for compliance purposes.

### **Data from other sources:**

We also process personal data about you that we obtain from publicly accessible sources (e.g. Companies House, press including trade press or paid for content, publicly available websites and other publicly available sources of information such as sanctions lists or lists of directors disqualifications) or that is legitimately transferred to us by other companies in the UBS group or from other third parties. These may include Your Organisation as well as third parties not related to you or Your Organisation, such as credit rating agencies, settlement service providers, central securities depositories, exchanges, central clearing counterparties and other similar entities, databases, and third party service providers such as professional advisers, insurers and risk consulting firms.

**Data relating to a third party:** If you provide us with personal data relating to a third party, for example, your spouse, children, parents or a Connected Individual, you represent and warrant that you have the appropriate authorization to share with us this personal data (for example obtaining the separate consent of such third party (when required)) before providing us with such personal data. You must ensure that you make such third parties and your Connected Individuals aware of our name, our contact information, and the scope of and purposes for which we will collect and process their personal data and how it will be processed as set out in this Privacy Statement.

### **Types of personal data:**

The types of personal data we process may include:

- personal details relating to you (name, date and place of birth, nationality, gender, domicile)
- contact details, including private and / or business phone numbers, postal and email addresses
- identification data such as passports, National Insurance or Social Security numbers, driving licence, ID cards, property register identification, social network user names, customer identifiers (CIF, IBAN / BIC), relationship identifiers (e.g. client segment and account currency), photographs
- authentication data such as sample signatures
- marital status, name of spouse, number of children (if applicable)
- tax status (e.g. tax ID)
- order data (e.g. payment data and account information)
- data from the fulfilment of our contractual obligations
- information about your financial situation (e.g. source of wealth, incomes, benefits, mortgage information, shareholdings)
- video surveillance and telephone / audio recordings

- data relating to criminal convictions and offences (including excerpts of criminal register)
- data related to designation of your status as a politically exposed person (PEP) and related information
- marketing and sales data (e.g. customer relationship documentation)
- data relating to your habits and preferences
- special categories of personal data, of a more sensitive nature, such as health or medical information or data relating to children
- dietary and access requirements (e.g. for event organisation purposes)
- data from your interactions with us, our branches, our internet websites, our apps, our social media pages, meetings, calls, chats, emails, interviews and phone conversations
- documentation data (e.g. file notes or meeting minutes from a consultation, client needs and product usage)
- data relating to your current and past professional roles and employment, and education (e.g. corporate title, membership of professional associations or bodies, career histories or biographies, job function, knowledge and experience in investment matters, qualifications and skills)
- other data similar to the broad categories mentioned above.

In addition, all of our websites use a standard technology called "cookies" to collect information about how our websites are used, which may include your personal data. The use of cookies is essential to the operation of our websites. You may opt-out of receiving cookies by disabling cookie support but doing so may prevent our websites from functioning properly and you may not be able to use fully all of the website's available features and information. If you would like to know more about our policies in relation to the use of cookies and your online security, please refer to our Privacy & Cookie Policy available at <https://www.credit-suisse.com>.

## 2) What do we process your data for (purpose of processing) and on what legal basis?

We process your personal data for one of the following reasons.

### a. Due to legal obligations

We are subject to various legal and regulatory obligations, including without limitation prudential and conduct regulation of banks and investment firms, as applicable, regulation of financial markets, compliance with any court orders, investor protection regulations, securities regulations, laws and administrative regulations/orders relating to money laundering, terrorism finance, sanctions and any tax laws.

The purposes of processing may include:

- identity checks, fraud and financial crime and market abuse prevention or detection. If fraud is detected, you or Your Organisation, could be refused certain services
- fulfilling control and reporting obligations under applicable financial regulations including, without limitation, securities and financial crime regulations
- fulfilling requirements related to our licences and regulatory permissions
- complying with investor protection or conduct of business regulation (such as carrying out suitability or appropriateness assessments)
- complying with regulatory record keeping obligations
- complying with regulatory obligations in relation to measuring and managing risks within the UBS group

### b. For purposes of legitimate interests

In accordance with applicable law, we may process your personal data, for the purposes of the legitimate business and other interests pursued by us or a third party, in:

- developing, deploying and supporting our products and services
- developing and furthering our business and business relationships

- protecting our businesses and the integrity of the financial markets
- managing risk and securing our systems, assets, infrastructure and premises
- exercising and defending our legal rights and position anywhere in the world
- complying with legal and regulatory obligations and cooperating with regulatory, judicial and other authorities and bodies around the world
- supporting other UBS Group companies in pursuing the above interests.

The purposes for which we may process your personal data (and such processing may involve sharing data between members of the UBS group and/or external parties) in connection with the above interests include the following:

- carrying on business relationships with clients and other parties
- providing services to clients
- due diligence in relation to transactions members of the UBS group are involved in
- performing obligations and exercising rights under and otherwise carrying out contracts, or taking pre-contractual measures with Your Organisation or a third party
- management of the businesses and further development of the services and products of the UBS group
- reviewing and optimizing procedures for needs assessment for the purpose of direct client discussions
- marketing or market and opinion research
- obtaining personal data from publicly available sources for client on-boarding purposes
- compliance with licencing, permission and / or licencing exemption requirements and regulatory requests or guidance related to such licences, permissions or exemptions
- compliance with applicable laws, regulations and judicial orders outside your jurisdiction.
- compliance with regulatory guidance, policy statements, best practice and associated policy requirements and controls in connection with the carrying on business
- facilitation of and responding to, regulatory requests and supervisory visits, and otherwise acting in open and collaborative manner with competent regulatory authorities
- prevention of and investigations related to financial crime, including fraud, financing of terrorism and money laundering, and compliance with sanctions, including know your customer (KYC) and regular politically exposed persons (PEP) screening
- asserting legal claims and defences in legal disputes
- carrying out conflict checks
- handling client complaints
- warehousing appropriate information within a single jurisdiction in order to co-ordinate our services and business activities and satisfying other administrative needs across the UBS group
- facilitating operational actions in connection with our business relationships (e.g. processing of payments, billing)
- validating the authority of signatories (e.g. when concluding agreements and transactions)
- risk control
- mergers, acquisitions and re-organizations including by providing information to future purchasers or transferees
- consulting with credit rating agencies to investigate creditworthiness, the need for a basic account or account maintained with a basic non-seizable balance and credit risks where we may have an exposure to you
- securing and operating UBS group's IT systems
- video surveillance and measures to protect the rights of an owner of premises to keep out trespassers for collecting evidence in hold-ups or fraud, or to prove availability and deposits e.g. at ATMs; and to provide site security (e.g. access controls).

**c. For fulfilment of contractual obligations**

We may process your personal data in order to maintain our business relationship with you in accordance with our legal agreement(s) with you. Such processing may take place in order to carry out obligations or exercise rights we may have pursuant

to the legal agreement(s) with you, to take steps necessary in order to conclude a legal agreement with you or to take other steps at your or your representative's request prior to entering into a legal agreement with you. If you are our client, the level and nature of processing of your personal data that we may carry out pursuant to this paragraph will likely depend on the specific product or service to be provided to you (and can include needs assessments and other assessments to provide advice and support to you, as well as to carry out transactions contemplated in, or necessary to fulfil, such legal agreement). To the extent that transactional documents have more restrictive terms, these terms shall prevail.

**d. As a result of your consent**

There may be circumstances where we ask for your consent to process your personal data. In some locations the consent might be included in the client contractual documentation and covers the purposes of processing mentioned above and disclosure to entities mentioned below. As long as you have granted us this consent, this processing is legal on the basis of that consent. You can withdraw your consent at any time by contacting the Data Protection Office (see section 12 below). Withdrawal of consent does not affect the legality of data processing carried out prior to withdrawal.

**e. When processing special categories of personal data, of a more sensitive nature**

For reasons relating to, for example, substantial public interest, protection of vital interests, in the field of public health, for the establishment of legal claims or where we have obtained your consent in accordance with Data Protection Legislation, we may process special categories of personal data, including sensitive data. We will only do this where we have appropriate lawful bases for processing such data, and in line with applicable Data Protection Legislation.

Please note that, to the extent permissible under applicable laws and regulations, your personal data may be held on cloud platforms which may be managed by third parties subject to contractual obligations of confidentiality and data protection.

### 3) Who receives my data?

The following paragraphs set out details of the recipients or categories of recipients to which we transfer your personal data.

**a. The UBS group**

We will share or otherwise process your personal data with entities in the UBS group and in accordance with section 4 of this statement as applicable, for example:

- in connection with any services offered or provided by us or any other member of the UBS group
- to facilitate carrying on the business of the UBS group and providing services to clients on a global basis
- for risk control including internal approvals processes
- to warehouse appropriate information within a single jurisdiction in order to coordinate the services and business activities of the UBS group
- to the extent permitted under and in accordance with applicable law (including, to the extent necessary, your prior authorization), pass on information about you to any members of the UBS group in connection with any services which we think you or Your Organisation may be interested in
- in connection with financial or regulatory reporting purposes.

**b. External recipients of data**

We may transfer personal data about you:

- to public entities and institutions (e.g. regulatory, quasi-regulatory, tax or other

authorities, law enforcement agencies, courts, arbitrational bodies, fraud prevention agencies)

- to other credit and financial service institutions or comparable institutions in order to carry on a business relationship with you or Your Organisation (depending on the contract, e.g. correspondent banks, custodian banks, brokers, securities exchanges, credit rating agencies)
- to third parties in connection with transactions that members of the UBS group are involved in (e.g. correspondent banks, brokers, exchanges, central clearing counterparties, depositaries, trustees, trade repositories, processing units and third-party custodians, issuers, investors, prospective buyers and other transaction participants and their representatives)
- to prospective buyers as part of a sale, merger or other disposal of any of our business or assets to a natural or legal person, public authority, regulatory agency or body for which you have given us your consent to transfer personal data to
- to professional advisors including law firms, accountants, auditors and tax advisors
- to insurers
- to service providers and agents appointed by us for the purposes given who may be subject to confidentiality obligations. These are companies in the categories of IT services, logistics, printing services, telecommunications, advice and consulting, transaction processing and settlement services, and sales and marketing and translation services.

#### 4) Will data be transferred to a third country or an international organization?

In certain circumstances, and where permitted to do so in accordance with the Data Protection Legislation, we may transfer your personal data to another country. You understand that the data protection legislation in such other country may not give you as much protection as the data protection legislation in the country where you are located.

For transfers to third countries which have not been determined by the applicable authorised institutions under the applicable Data Protection Legislation as countries offering an adequate level of data protection, we will either rely on a derogation applicable to the specific situation (e.g. if the transfer is necessary to perform our contract with you such as when making an international payment), or implement standard contractual clauses approved by the relevant institutions, as applicable, to ensure the protection of your personal data.

Please contact our Data Protection Office if you would like to request to see a copy of the specific safeguards applied to the export of your information. Contact details are provided in section 12 below.

#### 5) For how long will my data be stored?

We will process and store your personal data for as long as it is lawful for us to do so. It should be noted here that our business relationships are often long-term relationships, which are set up with you or Your Organisation on the basis of periods of years.

We will normally retain your records for a minimum of ten years to comply with regulatory and contractual requirements unless there is a particular reason to hold the records for longer, including fulfillment of obligations to preserve records according to commercial and tax law or legal hold<sup>3</sup> requirements, which require us to keep records for an undefined period of time.

#### 6) What data privacy rights do I have?

In relation to your personal data, and to the extent permitted under the Data

---

<sup>3</sup> A legal hold is a process that an organisation uses to preserve all forms of relevant information when litigation is reasonably anticipated

Protection Legislation you have the right:

- to request access to, and a copy of, your personal data
- request information on the processing of your personal data
- to request the rectification of inaccurate or incomplete personal data
- to request deletion of your personal data
- to request the restriction of the processing of your personal data
- to data portability
- other rights applicable to you under Data Protection Laws.

In addition to the above rights, you have the right to object at any time to:

- the processing of your personal data for direct marketing purposes, and profiling to the extent related to direct marketing and
- the processing of your personal data for the reasons set out in section 2.b of this statement (including profiling for these purposes), to the extent permitted under the Data Protection Legislation.

To exercise any of the above rights you do not need to use a particular form, but you should write to our Data Protection Office in accordance with section 12 of this statement. We will then assess and respond to your request to exercise your rights.

Please note that some of the above rights are subject to limitations in some situations, and that the exercise of the above rights may affect our ability to continue a business relationship with you or Your Organisation.

If applicable, you also have a right to make a complaint to the competent supervisory authority.

You may also withdraw consent granted to us for the processing of your personal data at any time by contacting the Data Protection Office (see Section 12 below). Please also see section 2.d of this statement for further details on consent.

## 7) Am I obliged to provide data?

In the context of our relationship, you may need to provide certain personal data that is required for accepting and carrying out a business relationship, fulfilling contractual obligations or that we are legally obliged to collect. Without this data, we may not be in a position to enter into a legal agreement, provide services, or initiate or maintain a business relationship.

For example, and where applicable to our business relationship, anti-money laundering regulations may require us to identify you on the basis of your identification documents before establishing a business relationship and to collect and put on record data including your name, place and date of birth, nationality, address and identification details for this purpose. In order for us to be able to comply with these statutory obligations, you must provide us with the necessary information and documents in accordance with such regulations, and to immediately disclose any changes over the course of our relationship. If you do not provide us with the necessary information and documents, we cannot enter into or continue the business relationship you require.

## 8) To what extent is there automated decision making?

In establishing and carrying out a business relationship, we generally do not use any fully automated decision-making pursuant to the Data Protection Legislation. If we use this procedure in individual cases, we will inform you of this separately, provided this is a legal requirement.

## 9) Will profiling take place?

We process some of your data automatically, with the goal of assessing certain personal aspects (profiling). For example, we use profiling in the following ways:

- due to legal and regulatory requirements, we are required to combat money laundering, terrorism financing, fraud, assess risk and offences that pose a danger to assets. Data assessments (including on payment transactions) are also carried out for this purpose.
- We may use scoring as part of the assessment of your creditworthiness. In doing so, the probability that a client will meet their payment obligations pursuant to the contract is calculated. This calculation may be influenced by the client's earning capacity, expenses, pending liabilities, occupation, employer, term of employment, experience from the business relationship thus far, contractual repayment of previous credits, and information from credit information offices, for instance. Scoring is based on a mathematically and statistically recognized and established process. The calculated scores help us to make decisions in the context of product sales and are incorporated into ongoing risk management.
- we use assessment tools in order to be able to specifically notify you and advise you or Your Organisation regarding products, but only to the extent permitted under applicable laws. These allow communications and marketing to be tailored as needed, including market and opinion research.

## 10) We may collect biometric and other sensitive personal data from you

Biometric data is classified as sensitive personal data under the Data Protection Legislation.

We may process your sensitive personal data (such as Touch ID or other biometric identification to access certain applications) for the purposes of prevention of fraud and the safety of your data in processes of identification and authentication in electronic systems or to the extent processing is necessary for CS to comply with legal and regulatory obligations. CS will obtain your explicit consent for the processing of your sensitive personal data if required under applicable privacy law.

## 11) Changes to this privacy statement

This Privacy Statement is effective as of June 12<sup>th</sup>, 2023. We may need to make further changes to this Privacy Statement in the future. If we do, we will post updates to our website.

## 12) Who is responsible for data processing and how can I contact them?

The legal entities and establishments responsible for the processing of your personal data and their contact details are:

<b>Entity / Establishment</b>	<b>Contact Details</b>
Credit Suisse Asset Management, LLC	Eleven Madison Avenue New York 10010-3629 NY <b>United States</b>
Instituto CSHG Banco de Investimentos Credit Suisse (Brasil) S.A. Banco Credit Suisse (Brasil) S.A. Credit Suisse (Brasil) S.A. Corretora de Títulos e Valores Mobiliários Credit Suisse Hedging-Griffo Wealth Management S.A. Credit Suisse Hedging-Griffo Corretora de Valores S.A. Latam (Brasil) Investimentos Limitada, Credit Suisse Consultoria de Investimentos Ltda.	Rua Leopoldo Couto de Magalhães Jr., 700 – 10º andar São Paulo – SP 04542-000 <b>Brazil</b>

---

Credit Suisse AG, Cayman Island Branch

Credit Suisse AG, Cayman Island Branch  
Eleven Madison Avenue  
New York, NY 10010-3629  
**United States**

---

Banco Credit Suisse (México), S.A.  
C. Suisse Asesoría México, S.A. de C.V.

Paseo de la Reforma No. 115, Piso 25  
Col. Lomas de Chapultepec  
C.P. 11000  
Mexico City  
**Mexico**

---

**You can reach our Data Protection Officer for all of the legal entities and establishments listed above at:**

The Data Protection Office  
One Cabot Square, London E14 4QA, United Kingdom

**or by e-mail as follows:**

- For legal entities and establishments in **Brazil**:  
[brazil.data-protection@credit-suisse.com](mailto:brazil.data-protection@credit-suisse.com)
- For legal entities and establishments in **Bermuda, Cayman Islands, Mexico**:  
[americas.data-protection@credit-suisse.com](mailto:americas.data-protection@credit-suisse.com)

**Important note:** when contacting our Data Protection Office, please ensure that you specify the correct legal name of the legal entity or establishment to which your query relates.

# Appendix I to the Data Protection Information for AM clients and other counterparties.

## Data Protection Legislation and Competent Data Protection Supervisory Authorities

### 1. Data Protection Legislation

Data Protection Legislation, as defined in the Data Privacy Statement, shall include, but is not limited to:

<b>in the Americas countries</b>	<ul style="list-style-type: none"><li>• Bermuda: <a href="#">Personal Information Protection Act 2016 (PIPA)</a></li><li>• Brazil: Lei Geral de Proteção de Dados 13.709/18 (<a href="#">LGPD</a>);</li><li>• Cayman Islands Data Protection Law, 2017 (DPL) and as amended under the <a href="#">Cayman Islands Data Protection Act 2021</a></li><li>• Mexico Federal Data Protection Law (<a href="#">FLPPDHPP/LFPDPPP</a>);</li></ul>
----------------------------------	--

## 2. Competent Data Protection Supervisory Authorities

COUNTRY	AUTHORITY	CONTACT DETAILS
<b>Bermuda</b>	Bermuda Data Privacy Commissioner	Government Administration Building, 3rd Floor 30 Parliament Street Hamilton HM 12 Bermuda (441) 295 5151 x1563 Online form: <a href="#">Contact   Government of Bermuda</a> ( <a href="http://www.gov.bm">www.gov.bm</a> )
<b>Brazil:</b>	<a href="#">Autoridade Nacional de Proteção de Dados (ANPD)</a>	Autoridade Nacional de Proteção de Dados Esplanada dos Ministérios, Ministério da Economia, Bloco C, 2º andar Brasília – DF, 70297-400 e-mail: <a href="mailto:presidencia@anpd.gov.br">presidencia@anpd.gov.br</a>
<b>Cayman Islands :</b>	<a href="#">Cayman Islands Ombudsman</a>	Cayman Islands Ombudsman PO Box 2252, Grand Cayman, Cayman Islands KY1-1107 Phone: 1 (345) 946 6283 Email: <a href="mailto:info@ombudsman.ky">info@ombudsman.ky</a>
<b>Mexico:</b>	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ( <a href="#">INAI</a> )	Insurgentes Sur No. 3211 Col. Insurgentes Cuicuilco, Alcaldía Coyoacán, C.P. 04530 <a href="http://inicio.ifai.org.mx/SitePages/ifai.aspx">http://inicio.ifai.org.mx/SitePages/ifai.aspx</a>

# Appendix II to the Data Protection Information for Brazil clients and other counterparties.

## Additional information for Brazil clients and counterparties

The information in this appendix needs to be read together with the rest of this document, as it does not replace what is stated in the main document.

### 1) What sources and data do we use?

**Data from other sources:**

In certain circumstances, we may also obtain your personal data from another sources (such as from our service providers' database) for purposes of: (a) background check and financial restrictions of prospects, or (b) check for any client's registration data updates in case we cannot contact such client.

### 2) What do we process your data for (purpose of processing) and on what legal basis?

We process your personal data for one of the following reasons.

**a. Due to legal obligations**

The purposes of processing may include:

- complying with regulatory obligations in relation to information security and cyber security.

### 4) Will data be transferred to a third country or an international organization?

Reasons for having to transfer your personal data outside Brazil may include:

- need to carry out our contract with you;
- need to fulfil with legal and/or compliance obligation;
- need to protect the public interest;

- for international legal cooperation between government intelligence, investigations, and prosecution authorities, according to instruments of international law, or when it is the result of a commitment established in an international cooperation agreement;
- for the regular exercise of rights, in court, administrative, or arbitration proceedings.

In some countries the law might compel us to share certain information with governmental and/or regulatory authorities (e.g. with tax authorities). We will only share information with parties who have the lawful authority and right to receive it and only to the extent that such parties are permitted to receive it.

## 5) For how long will my data be stored?

When no longer necessary for us to retain your personal data, it will be deleted or made anonymous in a safe and permanent manner or access to it will be blocked to the extent that statutory data retention requirements apply.

We may also keep personal data likewise for longer periods if permitted under Data Protection Legislation for instance to address complaints, assert or defend our rights in litigation or other dispute resolution procedures or to respond to requests from regulators or assist judicial authorities.

## 6) What data privacy rights do I have?

In relation to your personal data, and to the extent permitted under the Data Protection Legislation you have the right:

- be informed about any personal data we process
- oppose against data processing activities, request anonymization and elimination of personal data, in specific circumstances
- to receive information regarding the usage or sharing of your personal data
- to request the review of automated decisions that may affect your interests
- to be informed about the consequences of denying a request for consent if and when requested