

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 Cayman Island Data Protection Law, 2017 (“DPL”).

Data privacy is important – please read this document.

We issue this Privacy Statement in light of the DPL and other applicable data protection and privacy regulations of the Cayman Islands.

With the following information, we would like to give you an overview of how we will process your personal data and of your rights according to data privacy laws. 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:

Credit Suisse AG, Cayman Islands Branch

(full entity and contact details in section 12 of this statement).

“**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, in all cases outside the Credit Suisse organization (as applicable to you, “**Your Organization**”) or
- who themselves are our clients.

Please ensure that any relevant individuals are made aware of this Privacy Statement and the individual rights and information it sets out, prior to providing their information to us or our obtaining their information from another source. If you, or anyone else on your behalf, has provided or provides information on an individual connected to your business to us (or any affiliate), you or they must first ensure that you or they have the authority and appropriate legal basis to do so. Please ensure that any data you give us or ask third parties to provide to us is up to date, accurate and complete in all respects. Please inform us about any changes as soon as reasonably possible.

This Privacy Statement should be read alongside your other documentation you have with us (such as contracts, terms and conditions, subscription agreements and the like) as these may include sections relating to the use and disclosure of information. Where there is any conflict between the terms of this Privacy Statement and any other document in relation to data protection the terms of this Privacy Statement shall prevail, although its contents are not contractual.

1. What Personal Data Do We Collect/Use and Where Did We Obtain the Personal Data?

This Privacy Statement is concerned with personal information (also called personal data) we collect about you. Personal data means any data by which you as an individual can be directly or indirectly (e.g. if several pieces of data are combined) be identified. Data that is completely anonymised or de-personalised will not count as personal data.

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 Organization (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 Organization, 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.

Personal Data from other sources: We also process personal data about you that we obtain from publicly accessible sources (e.g. 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 Credit Suisse organization or from other third parties. These may include Your Organization as well as third parties not related to you or Your Organization, such as 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.

Types of personal data: The types of personal data we process may vary based on the type of services that we provide to you. Please refer to the applicable Supplement Information Notices in the attached Annexes for data processing information connected with the particular services being provided to you.

2. What Do We Process Your Personal Data for (Purpose of Processing) and On What Legal Basis?

We process your personal data to the extent permitted under the DPL for one of the following reasons.

a. Due to legal obligations

We are subject to various legal and regulatory obligations (e.g. applicable anti-money laundering regulations and the Confidential Information Disclosure law (2016)), 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 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, Your Organization, or individuals connected to it or you could be refused certain services
- fulfilling control and reporting obligations under applicable financial regulations, including securities 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 Credit Suisse organization.

b. For purposes of legitimate interests

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, and keeping our clients and other stakeholders satisfied
- 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 Credit Suisse companies in pursuing the above interests.

The purposes for which we may process your personal data (and such processing may involve sharing personal data between Credit Suisse affiliates 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 Credit Suisse affiliates are involved in
- performing obligations and exercising rights under and otherwise carrying out contracts, or taking pre-contractual measures with Your Organization or a third party
- management of the businesses and further development of the services and products of the Credit Suisse organization
- 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 acquisition 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 within and outside the Cayman Islands
- compliance with regulatory guidance, policy statements, best practice and associated policy requirements and controls in connection with the carrying on of Credit Suisse 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 the services and business activities of the Credit Suisse organization and satisfying other administrative needs across the organization
- 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 across the Credit Suisse organization
- consulting with credit rating agencies to investigate creditworthiness and credit risks where we may have an exposure to you
- securing and operating Credit Suisse's IT systems
- video surveillance and measures to protect the rights of an owner of premises to keep out trespassers 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).

d. As a result of your consent

There may be circumstances where we ask for your consent to process your personal data. As long as you have granted us this consent, this processing is legal. You can then 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. Other purposes of processing

There may be other purposes of processing that are unique to the particular services being provided to you. Please refer to the applicable Supplemental Information Notices in the attached Annexes for further information.

3. Who Receives My Personal Data?

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

a. Credit Suisse Affiliates

We will share or otherwise process your personal data with Credit Suisse affiliates, including entities outside of the Cayman Islands, for example:

- in connection with any services offered or provided by us or any other affiliate
- to facilitate carrying on the business of the Credit Suisse 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 co-ordinate the services and business activities of Credit Suisse
- to pass on information about you to any members of the Credit Suisse organization in connection with any services which we think you or your Organization may be interested in
- in connection with financial or regulatory reporting purposes.

b. External recipients of personal 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 Organization (depending on the contract, e.g. correspondent banks, custodian banks, brokers, securities exchanges, credit rating agencies)
- to third parties in connection with transactions that Credit Suisse is 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. These are companies in the categories of IT services, logistics, printing services, telecommunications, advice and consulting, and sales and marketing and translation services.

f. Other applicable recipients of your Personal Data

There may be other recipients who need your personal data due to the particular services that we provide to you. Please refer to the applicable Supplemental Information Notices in the attached Annexes for further information.

4. Will Personal Data Be Transferred to a Third Country or an International Organization?

In certain circumstances, we may transfer your personal data to another country, which may be outside of the Cayman Islands, or a country deemed by the Cayman Islands Privacy Commissioner as providing adequate privacy protection such as, for example, the European Union, Member States of the European Economic Area and other countries with data protection regulation deemed equivalent by the European Commission.

We may also need to transfer your personal data to a country that may not afford the same level of privacy protection as the Cayman Islands ("third countries"). You understand that the data protection legislation in these third countries may not give you as much protection as the data protection legislation within the Cayman Islands. For transfers to third countries, we will transfer the personal data in accordance with Cayman Islands cross border requirements such as relying 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 data transfer contractual provisions meeting the standard imposed under the DPL to ensure the protection of your personal data.

Reasons for having to transfer your personal data outside the Cayman Islands may include:

- we need to carry out our contract with you;
- we have to fulfil a legal and/or compliance obligation;
- we need to protect the public interest; and / or
- for your or our legitimate interests.

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 any information with parties who have the lawful authority and right to see it and only to the extent that such parties are permitted to see it.

5. For How Long Will My Personal 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 Organization 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 legal hold requirements, which require us to keep records for an undefined period of time.¹

We may also keep personal data likewise for longer periods where we have a legitimate interest for doing so, 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?

As an individual or “data subject”, you have certain rights in relation to your personal data. These rights include:

- the right to access information we hold about you and to obtain information about how we process it.
- the right to object to and withdraw your consent to the processing of your information. This right can be exercised at any time. However, we may continue to process your personal information if there is another legitimate reason or legal obligation for doing so. Please also note that depending on which kind of processing you object to, we may no longer be able to perform financial services with you.
- in some circumstances, you have the right to receive certain information you have provided to us in an electronic format and / or request that we transmit it to a third party;
- the right to request that we rectify information we hold about you if it is inaccurate or incomplete;
- in some circumstances, you have the right to request that erasure and deletion of personal data we hold. We may, however, continue to retain it if we are entitled or required by law to do so;
- the right to object to, and to request that we restrict, our processing of your information in some circumstances. Please note that despite this general right we may be entitled under law to continue processing the information and / or to refuse that request.

¹ A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated

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 Organization.

You also have a right to make a complaint to the Cayman Islands Ombudsman:

Cayman Islands Ombudsman
PO Box 2252,
Grand Cayman, Cayman Islands
KY1-1107

Email: info@ombudsman.ky

Phone: 1 (345) 946 6283

You may also be able to seek redress for any violation of your data protection rights in the Cayman Islands courts or challenge a decision by the regulator.

7. Am I Obligated to Provide Personal 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 personal 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 personal 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. 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 personal 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 and offences that pose a danger to assets. Data assessments (including on payment transactions) are also carried out for this purpose. At the same time, these measures also serve to protect you or Your Organization.
- we use assessment tools in order to be able to specifically notify you and advise you or Your Organization regarding products. These allow communications and marketing to be tailored as needed, including market and opinion research.

10. We May Collect Biometric Data From You

Biometric data is classified as sensitive personal data. Therefore, your explicit consent will be required in a separate process to use your Touch ID or other biometric identification to access certain applications.

11. Changes to this Privacy Statement

This privacy statement will take effect on September 30, 2019. We may need to make changes to it in the future. We will post updates to this privacy statement to our website.

12. Who Is Responsible For Data Processing and How Can I Contact Them?

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

Credit Suisse AG, Cayman Island Branch
Attention: J.J. McDonald
Deputy Branch Manager, Director
Eleven Madison Avenue
New York, NY 10010-3629 United States

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

The Data Protection Office
Five Canada Square
London
E14 5AQ
United Kingdom

or by e-mail as follows:

data.protection@credit-suisse.com

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

Supplemental Information Notices

Annex A – IBCM Client Services
Annex B – GM Client Services
Annex C – Independent Wealth Management Services

Annex A – Privacy Statement Supplement for IBCM Clients

1. Types of Personal Data that We Collect from you

- 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 license, ID cards, property register identification, social network user names, customer identifiers, 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
- dietary and access requirements (e.g. for event organization 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.

2. Who we might share your personal data with.

See Section 3 of the Main Privacy Notice

3. How we will use personal data (Purpose of Processing)

See Section 2 of the Main Privacy Notice

Annex B – Privacy Statement Supplement for GM Clients

1. Types of Personal Data that We Collect from you

- 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 license, ID cards, property register identification, social network user names, customer identifiers, 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
- dietary and access requirements (e.g. for event organization 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.

2. Who we might share your personal data with.

See Section 3 of the Main Privacy Notice

3. How we will use personal data (Purpose of Processing)

See Section 2 of the Main Privacy Notice

Annex C – Privacy Statement Supplement for IWM Clients

1. Types of Personal Data that We Collect from you

- 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 license, ID cards, property register identification, social network user names, customer identifiers, 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
- dietary and access requirements (e.g. for event organization 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.

2. Who we might share your personal data with.

See Section 3 of the Main Privacy Notice

3. How we will use personal data (Purpose of Processing)

See Section 2 of the Main Privacy Notice