CREDIT SUISSE

Privacy statement

Table of contents

Duties of disclosure upon collection of personal data from the data subject in accordance with the Data Protection Legislation.

Data privacy is important – please read the statement below.

With the following information, we would like to give you an overview of how we will collect and process your data and of your rights according to Data Protection Legislation. The details on what data will be processed and which method will be used depend significantly on thenature of the business relationship.

"Data Protection Legislation" means any law and/or regulation (including guidance and codes of practice issued by authorized data protection regulators) in Qatar Financial Centre (QFC) which is applicable to the processing of your personal data by us, and which shall include, but is not limited to the Data Protection Regulations and Rules 2021 amended, extended, consolidated or re- enacted from time to time.

This information is kept up to date and made available at any time under: https://www.credit-suisse.com/qa/en/legal/privacy-statement.html.

1. Who is responsible for data processing and how can I contact them?

The legal entity responsible is (hereinafter referred to as "we" "us" or "Aventicum"):

Aventicum Capital Management (Qatar) Llc

You can reach our privacy officer at:
Credit Suisse Group Data Protection Officer
One Cabot Square
London
E14 4QA
United Kingdom

Phone: +44 20 7888 8888
E-mail: data.protection@credit-suisse.com

2. What sources and data do we use?

In order to facilitate, enable and/or maintain our current, possible or former business relationship Aventicum provides a broad range of services including managing investments, advising on investments, arranging deals in investments, and dealing in investment (as Agent) (our **"Services")** to our current, prospective and former clients and related parties (hereinafter our **„Clients"**). Aventicum is also using delegates, suppliers or third party service providers (hereinafter the **„Service Providers"**) when performing the Services. When performing the Services, Aventicum collects and otherwise processes Personal Data relating to you in your capacity as director, officer, authorized signatory, employee, investor, beneficial owner and/or any other related person(s) (hereinafter each an **"Affected Person"**) of our Clients or Service Providers. Depending on the circumstances and the respective processing activity, Aventicum may act as a data processor or a data controller in its own right.

We process **Personal Data** (also referred to as **"Data"**), as defined below, that we collect directly from the relevant data subject (being our Client, Service Provider or the Affected Person, as defined above) in the context of our business relationship in various ways, including from the forms and any associated documentation that you complete when subscribing for an

investment or make transactions with respect to the funds, in course of due diligence enquiries and on-boarding documentation or when you provide it to us in correspondence, which may include written, telephone or electronic communications.

We also process – insofar as necessary to provide our Services – Personal Data that we obtain from publicly accessible sources (e.g. commercial and association registers, press, internet), bankruptcy registers, tax authorities, including those that are based in and outside the QFC, governmental and competent regulatory authorities, credit agencies, fraud prevention and detection agencies and organizations and internal lists for prevention and detection of financial crime activities maintained by UBS group[1] globally or that is legitimately transferred to us by other UBS Group companies or other third parties (e.g. third party service providers, investment funds, their management companies and/or general partners and their relevant service providers and delegates such as the portfolio managers, distributors, etc.).

Relevant Data processed by us include, but is not limited to:

Contact details
Name, surname, gender, physical and electronic address data, phone numbers

Other confidential data
Date and place of birth, nationality, identification information and documentation (e.g. ID card details), taxpayer identification number (TIN), Bank account number, Client number (CIF) and authentication Data (e.g. sample signature), information on regulatory or financial situation (e.g. for due diligence purposes), PEP status, private, professional, marketing and sales data, phone recording

Criminal records
Data relating to criminal convictions and offences (including excerpts of criminal register)

We may also incidentally process "sensitive personal data" targeted by article 12 of the Data Protection Regulations 2021 when processing non-sensitive personal data (e.g. personal data revealing political affiliations or opinion, racial or ethnic origin or religious beliefs may be disclosed in official identification documents such as passport we receive for the purpose of implementing our AML/ KYC obligations). If you do not want us to process this information, we therefore strongly suggest that you refrain from providing or making available such sensitive data, e.g. by removing this type of data from any document made available to us.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. What do we process your data for (Purpose of Processing) and on what legal basis?

We process personal data in accordance with the provisions of Data Protection Legislation.

For fulfillment of contractual obligations
Data is processed in order that we may provide the services for which we are engaged or to carry out pre-contractual measures necessary under the applicable regulations.

The purposes of Data processing depend primarily on the concrete Services (e.g. investment management and advice, arrangement of deals, etc.) and can include advice and support.

[1] 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.

You may find other details about the purposes of Data processing in the relevant contractual documentation for those services.

If processing of Personal Data is necessary for the purpose of compliance with a legal obligation to which Aventicum is subject:
As a as a financial institution, regulated by the QFC Regulatory Authority (QFCRA), we are subject to various legal obligations and statutory requirements (e.g. QFCRA rules and regulations on: the financial sector; fight against money laundering and terrorist financing, remuneration rules). Purposes of processing include inter alia assessment of various risks, identity checks (know-your-customer), anti-fraud, anti-money laundering and combating the financing of terrorism, fulfilling control and reporting obligations under fiscal laws, regulatory reporting.

In the context of balancing interests pursued by Aventicum, as the data controller, or a third party:
We process Personal Data beyond the actual performance of the contract or legal obligations, for the purposes of the legitimate interests pursued by Aventicum or a third party. For example, improving products and services, asserting legal claims and defence in legal disputes, guarantee of UBS group security and operation, prevention and detection of frauds, risk management and reporting, compliance, internal supervision and internal audit, marketing of our products and services (to the extent it does not involve profiling), 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), mergers, acquisitions and re-organizations including by providing information to future purchasers or transferees.
Whenever we intend to rely on legitimate interest as the legal basis for the processing of Personal Data, we will give due consideration to the Client's/Service Provider's and any Affected Person's rights and freedoms.

If processing of Personal Data is based on your consent:
If we have been granted consent to process Personal Data relating to you as Client, Service Provider or Affected Person for certain purposes (e.g. for marketing of our products and/or services that involves profiling), the related processing of Data is based on your consent as data subject. Consent given can be withdrawn at any time. Withdrawal of consent does not affect the legality of Data processed prior to withdrawal.

4. Who receives my data

The following paragraphs set out details on where we transfer Personal Data relating to the Client, Service Provider and Affected Person (as the case may be) to and the purpose for any such transfer.

The UBS Group
We may share your personal data with other entities in the UBS group where required to fulfill our contractual and legal obligations including for example carrying out anti-money laundering and know your client checks. We may transfer your personal data in connection with any services offered by any other member of the UBS group or for risk control due to statutory or regulatory obligation or based on legitimate interest.
We may also pass on information about you to any other members of the UBS group in connection with any services which we think you may be interested in.

External recipients of data
We may transfer personal data about you in the course of conducting our usual business, or if legal, regulatory or market practice requirements demand it to the following external recipients, or if you have given your consent (e.g. to process a financial transaction you have ordered us to fulfil) for the following purposes:

- To public entities and institutions (e.g. financial authorities such as the QFCRA and law enforcement agencies) either upon providing a legal or regulatory request or as part of our legislative and regulatory reporting requirements.

- To third parties (for example correspondent banks, brokers, exchanges, trade repositories, processing units and third-party custodians, issuers, authorities, and their representatives) for the purpose of ensuring that we can meet the requirements of applicable law, contractual provisions, market practices and compliance standards in connection with transactions you enter into and the services that we provide you with.
- To service providers and agents. We may transfer your personal data to service providers and agents appointed by us for the purposes given, subject at all times to such third parties being under a duty themselves to preserve confidentiality. These are companies in the categories of banking services, IT services, logistics, printing services, telecommunications, collection, advice and consulting, and sales and marketing.

We have implemented appropriate organisational and technical safeguards to protect the personal data for which we act as data controller at all times.

5. Will data be transferred to a third country or an International Organisation?

Data transfer to legal entities in countries outside QFC and states with data protection laws deemed adequate by the Data Protection Office (together known as "third countries") takes place so long as 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 authorised institutions, as applicable, to ensure the protection of your personal data.

Please contact our Data Protection Officer 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 1 above.

6. For how long will my data be stored?

We will process Personal Data relating to the Client, the Service Provider and any Affected Person (as the case may be) for as long as is necessary for the purposes described in section 3.

If the Data is no longer required in order to fulfill contractual or statutory obligations, it is deleted, unless its further processing is required – for a limited time – for the following purposes:

- Fulfilling obligations to preserve records according to commercial and tax laws as well as financial sector laws and regulations. In general, for this purpose we keep Personal Data relating to the Client, the Service Provider and any Affected Person (as the case may be) for a maximum period of 10 years upon termination of the business relationship;
- As an investment manager and being part of UBS Group, we can face legal holds[2] , which might require us to keep records for a longer period of time.

7. What data privacy rights do I have?

Each data subject has in relation to their personal data:

- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.

[2] A legal hold is a process that an organization uses to preserve all forms of relevant information in case of pending or anticipated litigation, investigation and other legal proceedings

- The right to object.
- The right to data portability.
- The right to object to data processing for direct marketing purposes. In individual cases, we process your personal data in order to conduct direct marketing. You have the right to object to the processing of your personal data for the purpose of this type of marketing at any time. This also applies to profiling, insofar as it is in direct connection with such direct marketing. If you object to processing for the purpose of direct marketing, we will no longer process your personal data for this purpose.
- Individual right of objection on grounds relating to your particular situation. You shall have the right of objection to processing of your personal data at any time. If you submit an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate reasons for processing, which override your interests, rights, and freedoms, or processing serves the enforcement, exercise, or defense of interests. Please note, that in such cases we will not be able to provide services and maintain a business relationship.

Any requests in relation to exercising your data privacy rights do not need to be made in a particular form however, it should be addressed to:
Credit Suisse Group Data Protection Officer
One Cabot Square
London
E14 4QA
United Kingdom
Phone: +44 20 7888 8888
E-mail: data.protection@credit-suisse.com

If applicable, you also have a right to make a complaint to the Data Protection Office, QFC Tower 1, West Bay, PO Box 23245, Doha, Qatar. E-mail: dataprotection@qfc.qa.

8. Am I obliged to provide personal data?

In the context of our business relationship, you must provide all Personal Data that is required for accepting and maintaining the business relationship and for fulfilling the accompanying contractual obligations or that we are legally obliged to collect.

In particular, anti-money laundering regulations require us to identify you on the basis of your identification documents before establishing a business relationship with our client and to collect and put on record 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 the applicable anti-money laundering regulations, and to immediately disclose any changes over the course of the business relationship. If you do not provide us with the necessary information and documents, we cannot enter into or continue the business relationship with our client.

9. 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.

10. Will profiling take place?

We may process some of your data for the purposes of profiling. We use profiling in the following ways:

- Due to legal and regulatory requirements, we are required to combat money laundering, terrorism financing, fraud, and assess risk 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.
- We use assessment tools in order to be able to specifically notify you and advise you regarding products.

11. Do You Collect Biometric Data?

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.

12. Changes to this privacy statement

This Privacy Statement was last updated in June 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.