Data Privacy Statement

Banque Internationale à Luxembourg (Suisse) SA ("Bank") has issued this Data Privacy Statement considering the Swiss Federal Act on Data Protection ("FADP") as well as the EU General Data Protection Regulation ("GDPR") which is the privacy regulation of the European Union ("EU").

In this Data Privacy Statement, the Bank would like to outline how it collects, processes and protects personal data about the following persons: (i) prospective clients ("Prospects"), (ii) persons that have or are in the process of applying for an account with the Bank ("Clients") and (iii) individuals or entities whose information is provided by a Client to the Bank or comes otherwise to the Bank's knowledge in connection with services provided by the Bank to a Client ("Connected Parties"). A Connected Party may include, but is not limited to, (i) any director, officer, authorized signatory or employee of a company, (ii) a trustee, settlor or protector of a trust, (iii) any beneficial owner of Client's assets, (iv) a controlling person, (v) a payee of a designated payment, (vi) representative(s) or agent(s) of a Client, (vii) a co-obligor under a loan (e. g. guarantor of a credit) or (viii) any other individual or entity having a relationship with a Client that is relevant to this Client's business relationship with the Bank. Furthermore, this Data Privacy Statement shall also inform Clients, Connected Parties and Prospects of their rights in relation to personal data collected and processed by the Bank. Please note that, how specific personal data are processed and how they are used depends largely on the products and services requested or agreed in each case.

Wherever the Bank uses "you" or "your" in this Data Privacy Statement, this is meant as a reference to a Prospect, a Client and any Connected Party as defined herein.

If the Bank provides separate or further information about how it collects and uses Prospects', Clients' or Connected Parties' personal data for a particular product or service, those terms will also apply.

Furthermore, this Data Privacy Statement continues to apply even if Client's agreements for banking or other products and services with the Bank end.

1. Who is responsible for Data Processing and who can you contact in this regard?

The controller for data processing purposes is the Bank's Data Protection Advisor (according to FADP), who can be reached at:
Banque Internationale à Luxembourg (Suisse) SA
Data Protection Advisor
Bahnhofstrasse 20
8001 Zurich
Switzerland
E-Mail address: bils-dataprotection@bil.ch

The Bank's representative (within the meaning of Article 27 of the GDPR) is Banque Internationale à Luxembourg S.A., 69 route d'Esch, L- 2953 Luxembourg.

2. What sources and data does the Bank use?

The personal data the Bank collects or has about Clients, Connected Parties and Prospects come from different sources. This includes personal data relating to the business relationship or a prospective business relationship with the Bank or any of the Bank's products or services that the Client or a Connected Party or prospective client has applied for or held previously.
Some of the personal data will come directly from the Client, the Connected Party, or the prospective client. Some might be obtained from an independent asset manager, another advisor, a business introducer or from other third parties. Personal data might also come from other BIL Group entities, or the Bank might obtain such personal data lawfully by accessing publicly available sources or combining different sets of information.
Personal data collected may include, in particular:

a) ***Information a Client, a Connected Party or a Prospect provides to the Bank, such as:***

- Identification data (e.g., name, date and place of birth, nationality).
- Contact details (e.g., postal address, email address, phone number).
- Official documents (e.g., identity card, passport).
- Economic and transactional data (e.g., assets, income, source of wealth and source of funds, banking history).
- Authentication data (signature).

b) ***Information the Bank collects or generates about the Client, a Connected Party or a Prospect, such as:***

- Client relationship data (e.g., products held and services rendered), securities and payment transaction data and other financial information.
- Information regarding a Client's, a Connected Party's or a Prospect's financial situation such as credit data (e.g., information regarding Client's creditworthiness, individual credit application history).
- Information the Bank collects or generates to comply with its obligations under the anti-money laundering regulatory framework (e.g., information on origin of assets, beneficial ownership).
- Information the Bank collects or generates for risk management purposes such as client due diligence data (including periodic review results), client risk profiles, data to assess suitability/appropriateness, client qualification data (e.g., status as qualified investor), screening alerts (transaction screening, name screening), tax data or complaint information.
- Geographic information.
- Information included in client files, client documentation and other comparable information.
- Marketing and sales information (e.g., newsletters, documents received, invitations to and participation at events and special activities, personal preferences and interests, opt-in and opt-out declarations).
- Information used in "cookies" and similar technologies on websites, mobile applications and in emails to recognize a data subject, remember a data subject's preferences and show a data subject content the Bank thinks he/she/it is interested in.
- Registration of phone conversations between the Bank, the Clients, Connected Parties, potential clients to safeguard the interests of the Bank in case of claim or proceedings.

c) ***Information about the Client, a Connected Party or a Prospect that the Bank collects from other sources, for example:***

- Communication information (e.g., information contained in e-mails, chat messages or other digital communications).
- 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).

The Bank may also collect and process additional personal data about which the Bank will inform you from time to time.

3. What does the Bank process personal data for (i.e., purpose of the processing) and on what legal basis?

The Bank processes personal data of Clients, Connected Parties and Prospects for various purposes in accordance with the provisions of the FADP and the GDPR and only uses such personal data where the Bank has a legal basis for using it. The legal basis and purposes include processing:

a) ***For the performance of a contract (Article 6 para. 1b of the GDPR)***

The processing of personal data is carried out to perform banking transactions and financial services pursuant to contracts with the Bank's Clients and their Connected Parties or to take steps prior to entering into a contract (e.g., with Prospects):

- Provide financial advice to Clients and Connected Parties.
- Execute an order or transaction based on a Client's or Connected Party's instructions.
- Process a Client's or Connected Party's application for a specific product offering.

b) In the context of legitimate business interests pursued by the Bank (Article 6 para. 1f of the GDPR)

Where required, the Bank processes personal data beyond the actual fulfilment of the contract for the purposes of safeguarding the legitimate interests pursued by the Bank or a third party (including the entities of the BIL Group), such as:

- Management of Prospects' data.
- Video surveillance to safeguard the Bank's premises against trespassers, for collecting evidence in the event of holdups or frauds, or to document withdrawals and deposits.
- Send satisfaction surveys and process the replies in order to improve the quality of service.

c) Based on your consent (Article 6 para. 1a of the GDPR)

Insofar as you have granted the Bank consent to process your personal data for marketing purposes (such as receiving commercial content by email or mail), this processing is based on your consent. A consent given may be revoked at any time. Please be advised that a withdrawal of consent does not affect the lawfulness of processing of data prior to revoking such consent.

d) Due to legal obligations (Article 6 para. 1c of the GDPR)

Furthermore, the Bank is subject to various legal obligations, i.e., statutory requirements as well as bank regulatory requirements, such as to:

- Ensure compliance with all applicable anti-money laundering and counter-terrorist financing rules and regulations.
- Document all transactions and orders carried out for a Client or Connected Party.
- Record telephone conversations related to transactions and order-taking.
- Ensure compliance with all applicable tax regulations (e.g., FATCA/QI, CRS).
- Ensure compliance with all applicable financial market regulations.

4. Who receives personal data?

The Bank personnel is given access to personal data of Clients, Connected Parties and Prospects on a need-to-know basis in order to carry out the processing activities described in the Data Privacy Statement. Some service providers appointed by the Bank may also receive data for the purposes aforementioned.
With regard to transferring data to other recipients outside the Bank, it is to be noted that the Bank is generally obliged to maintain secrecy about any customer-related information, which the Bank may acquire or have knowledge of. The Bank may process information about you only if legal provisions demand it, if you have given your consent (e.g., to execute a financial transaction ordered by a Client or Connected Party), and/or if the Bank is required to provide information. Under these circumstances, the recipients of the personal data can be, for example:

- Public authorities and institutions (e.g., the Swiss National Bank, Swiss Financial Market Authority (FINMA), other financial authorities, tax authorities, criminal prosecution authorities, courts) insofar as a statutory or official obligation exists.
- Other credit and financial service institutions, comparable institutions and data processors to which the Bank transfers a data subject's personal data in order to perform the business relationship with such data subject (depending on the contract, e.g. market counterparties, correspondent and agent banks, custodian banks, clearing houses, clearing or settlement systems, brokers, stock exchanges, information offices, service providers, companies that a data subject holds securities in, credit/debit card processing supplier(s)).
- Other companies within BIL Group for risk control purposes due to statutory or official obligation or for the purpose of outsourcing data processing activities within the BIL Group mainly in the categories of banking services, IT services, logistics, telecommunications, advice and consulting, as well as sales and marketing.
- Joint account holders, trustees, beneficiaries, holders of power of attorney or executors.
- 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 the Bank or deals with the Bank for you.
- Auditors or dispute resolution bodies.
- Service providers with whom the Bank took all necessary measures to ensure compliance with the FADP and GDPR.

5. Is the data transferred to a third country or to an international organisation?

In certain circumstances personal data may be transferred to, and stored at, a destination outside Switzerland, including locations which may not have the same level of protection for personal data as Switzerland. The Bank will always do this in a way that is permissible under data protection rules. The Bank may need to transfer your information in this way for example:

- To perform its contract with you (e.g., due to the kind of product or service that is used and in order to fulfil a legal obligation).
- Where enforceable under applicable data protection laws to protect the public interest.
- For the Bank's legitimate business interests (e.g., in the context of an outsourcing project).

Transfer of personal data to recipients in countries outside Switzerland, the EEA and the EU (i.e., so called third countries) will take place if:

- It is necessary for the execution of orders or a contract (e.g., payments and securities orders).
- It is required by law (e.g., reporting obligations under fiscal law).
- It is in the context of commissioned data processing; or
- You have given consent to the Bank.

Where your personal data is to be disclosed to third parties domiciled in countries which do not have an appropriate level of data protection, the Bank ensures that where necessary it takes appropriate measures (e.g., contractual arrangements, such as the EU Standard Contractual Clauses (see Article 16 para. 2d of the FADP and Article 46 para. 2c of the GDPR), 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 Switzerland by contacting the Bank in accordance with the information provided in Section 1 above.

6. How long will personal data be stored?

The Bank will process and store personal data of Clients, Connected Parties or Prospects for as long as it is necessary in order to fulfil the Bank's contractual and statutory obligations. It should be noted that the business relationship with the Bank is a continuing and long-term obligation, intended to last for several years.
In general, the Bank is required to store the personal data of Clients and Connected Parties for a 10-year period after the end of the business relationship.

7. What data protection rights do you have?

Under the applicable data protection laws you may have the following rights:

- Right of access (as defined in Article 25 of the FADP and Article 15 of the GDPR).
- Right to rectification (as defined in Article 32 of the FADP and Article 16 of the GDPR).
- Right to erasure (as defined in Article 17 of the GDPR).
- Right to restriction of processing (as defined in Article 32 of the FADP and Article 18 of the GDPR).
- Right to object to the data processing (as defined in Article 32 of the FADP and Article 21 of the GDPR).
- Right to data portability, if applicable, (as defined in Article 28 of the FADP and Article 20 of the GDPR).

The right of access and the right to erasure are subject to certain restrictions under Articles 26, 27 and 29 of the FADP and Article 23 of the GDPR.

Where the Bank processes personal data based on your granted consent, you may revoke your consent specifically granted to the processing of personal data at any time. Please be advised that the withdrawal will only take effect in the future. Any processing that was carried out prior to the withdrawal shall not be affected thereby.

8. Are you required to provide the data?

In the context of a business relationship with the Bank, a Client or a Connected Party must provide all personal data required to start a business relationship and for the performance of the associated contractual obligations. As a rule, the Bank would not be able to enter into or perform any contract or – consequently - accept and execute any order without collecting and processing personal data.
Data subjects are responsible to make sure the information provided to the Bank is accurate and up to date.
In particular, provisions of anti-money laundering laws require that the Bank verifies a data subject's identity before entering into the business relationship by means of a document of evidentiary value (e.g., identity card) and that the Bank collects and records a data subject's name, place of birth, date of birth, nationality, residential address and other data for that purpose. In order for the Bank to be able to comply with this statutory obligation, a data subject must provide

the Bank with the necessary information and documents in accordance with all applicable anti-money laundering laws and regulations and notify the Bank without undue delay of any changes that may arise during the course of the business relationship. If a data subject does not provide the Bank with the necessary information and documents, the Bank may not be able to enter into or continue the requested business relationship.

9. Is “profiling” or “automated decision-making” used?

In some cases, the Bank processes personal data of Clients, Connected Parties or Prospects with the aim of evaluating certain personal aspects (profiling). For instance, the Bank uses profiling in the following cases:

- Due to legal and regulatory requirements, the Bank must take anti-money laundering, counter-terrorist financing and fraud prevention measures. Data evaluations, including on payment transactions, are also carried out in this context. At the same time, these measures also serve to protect you.
- In order to provide you with targeted information and advice on products, the Bank may use evaluation tools. These enable demand-oriented communication and advertising, including market and opinion research.
- To assess any credit application that you may submit to the Bank, a profiling activity may be carried out with your personal data.

10. Changes to the Data Privacy Statement

You may request a copy of this Data Privacy Statement using the contact details set out in Section 1 above. The Bank may modify or update this Data Privacy Statement from time to time by providing a revised version to its clients or making such a revised version available on the Bank’s website at www.bil.ch.