

Data Privacy Statement

bank zweiplus Ltd ("**Bank**") has issued this Data Privacy Statement in light of the Swiss Federal Act on Data Protection ("**DPA**") and its upcoming revision as well as the EU General Data Protection Regulation ("**GDPR**") which is the new privacy regulation of the European Union ("**EU**"). Although GDPR is a regulation of the EU it is relevant for the Bank for a number of reasons. Swiss data protection legislation is historically closely tied to EU regulations and its future amendment will be substantially influenced by GDPR. Furthermore although GDPR is an EU-regulation, under certain circumstances it may apply to companies outside the EU such as the Bank (extraterritorial effect). This Data Privacy Statement is addressed to persons with their domicile in the EU or the European Economic Area (EEA).

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, (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 Individuals**"). A Connected Individual 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 Individuals and prospective clients of their rights in relation to personal data collected and processed by the Bank. Please note: Which 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 prospective client, a client and any Connected Individual as defined herein.

If the Bank provides separate or further information about how it collects and uses clients' or Connected Individuals' 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.

Please familiarize yourself with this Data Privacy Statement and also forward it to any Connected Individuals before the Bank is provided with personal data of such Connected Individual.

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

The controller for data processing purposes and the Bank's Data Protection Officer (according to GDPR) can be reached at:

bank zweiplus Ltd
Data Protection Officer
Bändliweg 20
P.O. Box
CH-8048 Zurich

dataprotection@bankzweiplus.ch

The Bank's representative (within the meaning of Article 27 GDPR) is Banque J. Safra Sarasin (Luxembourg) SA, 17–21, Boulevard Joseph II, L-1840 Luxembourg.

2. What sources and data does the Bank use?

The personal data the Bank collects or has about clients, Connected Individuals and prospective clients 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 Individual or prospective client has applied for or held previously.

Some of the personal data will come directly from the client, the Connected Individual 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 J. Safra Sarasin Group¹-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 that a client, a Connected Person or a prospective client provides to the Bank such as:
- Contact details (e.g. name, address and other contact details such as date and place of birth, and nationality);
 - Information about a client, a Connected Person or a prospective client given to the Bank by filling in forms or by communicating with the Bank, whether face-to-face, by phone, e-mail, on-line or otherwise;
 - Information concerning a client's, Connected Person's or prospective client's identity (e.g. passport information which does also contain a photograph) or which is relevant for authentication purposes (e.g. sample signature).
- b) Information that the Bank collects or generates about the client, a Connected Person or a prospective client, 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 Person's or a prospective client'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 relevant client files and client documentation and other comparable information;
 - Marketing and sales information (e.g. newsletters, documents received, invitations to and participations at events and special activities, personal preferences and interests, opt-in and opt-out declarations);

¹ This includes entities of J. Safra Sarasin Holding Ltd Group in Switzerland and abroad.

- 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.
- c) Information about the client, a Connected Person or a prospective client that the Bank collects from other sources, for example:
- Communication information (e.g., information contained in emails, 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 only collects special categories of personal data as defined in article 9 of the GDPR such as biometric data, data revealing political opinions or memberships, data concerning health, data revealing racial or ethnic origin, religious or philosophical beliefs or data relating to criminal convictions and offenses from a client, Connected Person or prospective client in exceptional cases ("**Special Categories of Personal Data**").

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 (purpose of the processing) and on what legal basis?

The Bank processes personal data of clients, Connected Individuals and prospective clients for various purposes in accordance with the provisions of the European GDPR and the Swiss DPA and only uses such personal data where the Bank has a lawful basis for using it. The lawful basis and purposes include processing:

a) For the fulfillment of contractual obligations (article 6 para. 1 b) of the GDPR)

The processing of personal data is carried out in order to perform banking transactions and financial services pursuant to contracts with the Bank's clients and their Connected Individuals or to take steps prior to entering into a contract (e.g. with prospective clients).

The purposes of data processing are primarily dependent on the specific product (e.g. bank account, credit, securities, deposits, payments) and can include needs assessments, advisory, asset management and other financial or support services, as well as the carrying out of transactions. Additional details about the purposes of data processing may also be included in the applicable contractual or product documentation.

b) In the context of balancing interests and the purposes of safeguarding legitimate interests respectively (article 6 para. 1 f) 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 J. Safra Sarasin Group). For Example:

- Reviewing and optimizing procedures for needs assessment for the purpose of direct client discussions;
- Keep track of the Bank's conversations with clients, Connected Individuals and prospective clients (by phone, in person, by email or by any other kind of communication);
- Asserting legal claims and mounting a defense in the event of legal disputes;
- Correspond with legal advisers and third party intermediaries;

- Manage the Bank's internal operational requirements for credit and risk management, system or product development and planning, insurance, audit and administrative purposes;
- Consulting and exchanging data with information offices (e.g., debt register) to investigate creditworthiness, determine credit or default risks in the credit business and determine requirements for an account maintained with a basic non-seizable balance or a basic payment account;
- Ensuring Bank's IT security and IT operations;
- Prevention and solving of crimes;
- Video surveillance to safeguard Bank's premises against trespassers, for collecting evidence in the event of hold-ups or fraud, or to document disposals and deposits, e.g. at ATMs;
- Measures for building, site and systems security (e.g. access controls);
- Measures for ensuring the right of owner of premises to keep out trespassers;
- Measures for business management and further development and improvement of services and products;
- Risk control in the J. Safra Sarasin Group;
- Marketing or market and opinion research, to the extent that clients, Connected Individuals and prospective clients have not objected to having their personal data used;
- Gather insights from information through data analytics and for statistical purposes;
- Complying with applicable Swiss and other legal statutory and regulatory requirements.

c) On the basis of your consent (article 6 para. 1 a) of the GDPR)

Insofar as you have granted the Bank consent to process your personal data for specific purposes (e.g. analysis of transactional activities for marketing purposes), this processing is lawful on the basis of your consent. A consent given may be revoked at any time. This also applies to withdrawal of declarations of consent that were given to the Bank before the GDPR came into force, i.e. prior to May 25, 2018. Please be advised that a withdrawal of consent does not affect the lawfulness of the processing of data prior to revocation of such consent. Note however that the Bank may still be entitled to process your personal data if it has another legitimate reason for doing so.

d) Due to legal obligations (article 6 para. 1 c) of the GDPR) or in the public interest (article 6 para. 1 e) of the GDPR)

Furthermore, the Bank is subject to various legal obligations, i.e. statutory requirements (e.g. the Banking Act, Collective Investment Schemes Act, Anti-Money Laundering Act, Mortgage Bond Act, ordinances and circulars of regulatory authorities and tax laws) as well as bank regulatory requirements. Purposes of processing include for example assessment of creditworthiness, identity and age verification, fraud and money laundering prevention measures, fulfilment of control and reporting obligations under fiscal and other laws, and measuring and managing risks within the Bank and the J. Safra Sarasin Group (including for consolidated supervision purposes).

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

e) When processing Special Categories of Personal Data (article 9 para. 2 of the GDPR)

Special Categories of Personal Data can be processed by the Bank if this is necessary for the establishment, exercise or defence of legal claims of the Bank or if these data have manifestly been made public (article 9 para. 2 e) and f) of the GDPR). Otherwise the Bank only processes Special Categories of Personal Data with your explicit consent (article 9 para. 2 a) of the GDPR).

4. Who receives personal data?

Within the Bank those units are given access to personal data of clients, Connected Individuals and prospective clients which require them in order to perform the Bank's contractual and statu-

tory obligations or as further described in this Data Privacy Statement. Service providers and auxiliary persons appointed by the Bank may also receive data for these purposes if they observe banking secrecy. These could mainly be companies in the categories of banking services, IT services, logistics, printing services, telecommunications, debt collection, advice and consulting, as well as sales and marketing.

With regard to transferring data to other recipients outside the Bank, to begin with, it is to be noted that, as a bank, the Bank is generally obliged to maintain secrecy about any customer-related facts and evaluations which the Bank may acquire or have knowledge of (banking secrecy). The Bank may pass on information about you only if legal provisions demand it, if you have given your consent (e.g. to process a financial transaction a client or Connected Individual has ordered the Bank to perform), and/or if the Bank is authorized to provide information. Under these requirements, recipients of 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 the J. Safra Sarasin Group for risk control purposes due to statutory or official obligation or for the purpose of outsourcing data processing activities within the J. Safra Sarasin Group mainly in the categories of banking services, IT services, logistics, printing services, telecommunications, advice and consulting, as well as sales and marketing;
- Joint account holders, trustees, beneficiaries, power of attorney holders 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.

Additional recipients of personal data may be those for which you have given your consent to transfer your personal data or with respect to which you have exempted the Bank from banking secrecy by agreement or consent.

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

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. for example in the context of an outsourcing project).

Transfer of personal data to recipients in countries outside Switzerland, the EEA and the EU (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 your 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 46 para. 2 (c) 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 Individuals or prospective clients for as long as it is necessary in order to fulfil the Bank's contractual and statutory obligations. It should be noted here that the business relationship with the Bank is a continuing and long term obligation, intended to last for several years.

If the personal data are no longer required in order to fulfil contractual or statutory obligations, they are regularly deleted, unless their further processing – generally for a limited time - is required for the following purposes:

- Compliance with records retention periods under commercial and tax law: this includes for example the Swiss Code of Obligations (CO) and its related relevant ordinances, the Federal Act on Value Added Tax (VATA), the Federal Act on Direct Taxation (DTA), the Federal Act on Harmonization of Direct Taxes of Cantons and Municipalities (THA), the Federal Act on Stamp Duties (SDA) the Federal Act on Withholding Tax (WTA), the Swiss Bankers Association's Guidelines on the treatment of assets without contact and dormant assets held at Swiss banks (Guidelines on Dormant Assets).
- Preservation of evidence in accordance with statutes of limitations.
- Compliance with special retention constellations, such as «legal holds», i.e. processes put into effect by the Bank in order to preserve all forms of relevant information when litigation is reasonably anticipated or ongoing. In such cases the Bank might be required to keep the information for an undefined period of time.

7. What data protection rights do you have?

Under the applicable data protection laws you may have the following rights: the right of **access** (as defined in article 8 DPA and 15 GDPR), the right to **rectification** (as defined in article 5 DPA and 16 GDPR), the right to **erasure** (as defined in article 5 DPA and 17 GDPR), the right to **restriction of processing** (as defined in articles 12, 13, 15 DPA and 18 GDPR), the right to **object** to the data processing (as defined in article 4 DPA and 21 GDPR) and, if applicable, the right to **data portability** (as defined in article 20 GDPR). The right of access and the right to erasure are subject to certain restrictions (under articles 9, 10 and 13 DPA and, in particular, 23 GDPR). Furthermore, if applicable on a person, there is also a right to **lodge a complaint** with an appropriate data privacy supervisory authority (article 77 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. This also applies to the revocation of declarations of consent that were granted to the Bank prior to the entry into

force of the GDPR, i.e. before May 25, 2018. Please be advised that the revocation will only take effect in the future. Any processing that was carried out prior to the revocation shall not be affected thereby. Please note however that the Bank may still be entitled to process your personal data if it has another legitimate reason for doing so.

8. How is personal data kept secure?

The Bank implements internal technical and organisational measures to keep personal data of clients, Connected Individuals and prospective clients safe and secure which may include encryption, anonymization, access limitations and physical security measures. The Bank requires its employees and any third parties who carry out any work on the Bank's behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of personal data.

9. Is there an obligation to provide data?

In the context of a business relationship with the Bank a client or a Connected Individual, must provide all personal data which is necessary for the establishment and maintenance of such business relationship and the performance of the associated contractual obligations or which the Bank is legally obliged to collect. 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 law 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 the Anti-Money Laundering Act 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 will not be allowed to enter into or continue the requested business relationship.

If you give the Bank any information about another person connected to your account (such as a Connected Individual), you must inform such person about what personal data you have given to the Bank, and make sure they are informed of the content of this Data Privacy Statement.

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

In some cases, the Bank processes personal data of clients, Connected Individuals or prospective clients automatically 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 is obliged to take anti-money laundering, anti-terrorist-financing, anti-fraud and anti-financial crime 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.

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

When providing you with services, the Bank may make decisions about you by automated means. The Bank will ensure that a suitable contact person is available if you wish to express a view on any automated individual decision where such opportunity to express a view is required by law. In such event, please refer your request to the address contained in section 1 above.

11. Changes to the Data Privacy Statement

You may request a copy of this Data Privacy Statement from the Bank 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.bankzweiplus.ch/dataprotection.

Information on your right to object under article 21 of the EU General Data Protection Regulation (GDPR)

1. Ad hoc right to object

In case GDPR is applicable to you, you have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on article 6 para 1 e) GDPR (processing in the public interest) and article 6 para.1 f) GDPR (processing for the purposes of safeguarding legitimate interests); this includes any profiling based on those provisions within the meaning of article 4 para. 4 GDPR.

If you lodge such an objection, the Bank will no longer process your personal data, unless the Bank can demonstrate mandatory legitimate grounds for the processing which override your interests, rights and freedoms or unless the processing is for the establishment, exercise or defense of legal claims. Please note, that in such cases the Bank will not be able to provide services and maintain a business relationship with you either.

2. Right to object to the processing of data for direct marketing purposes

In individual cases the Bank processes your personal data for direct marketing purposes, If GDPR is applicable to you, you have the right to object at any time to processing of personal data concerning yourself for such marketing, which includes profiling to the extent that it is related to such direct marketing.

If you object to processing for direct marketing purposes, the Bank will no longer process your personal data for such purposes.

There are no formal requirements for lodging an objection. It should ideally be in writing and addressed to:

bank zweiplus Ltd
Data Protection Officer
Bändliweg 20
P.O. Box
CH-8048 Zurich
dataprotection@bankzweiplus.ch