bank zweiplus

Applicant Data Privacy Statement

In this Applicant Data Privacy Statement, bank zweiplus ltd. ("Bank") would like to outline how it collects, processes and protects personal data in connection with applicant's job application and its hiring process with the view to potentially enter into an employment relationship ("Applicants[1]"). Furthermore this Applicant Data Privacy Statement shall also inform Applicants of their rights in relation to personal data collected and processed by the Bank.

In this Data Privacy Statement:

- "you" or "your" means as a reference to an Applicant as defined herein;
- "personal data" means all information (whether business-related, private, public or confidential) relating to an identified or identifiable individual (e.g. name, gender and Curriculum Vitae). It includes any data that can be used to directly or indirectly identify a person; it also includes data where the individual at issue is identifiable only indirectly by use of secondary sources (e.g., the Internet or other databases) or through an identifier (namely an identification number, location data or an online identifier);
- "processing" means any operation with personal data, irrespective of the means and the procedures applied, and in particular the collection, recording, storage, use, modification, disclosure, archiving, deletion or destruction of personal data;
- "controller" means the Bank or any other private person (e.g. natural person, legal entity) or state bodies that alone or jointly with others decides on the purpose and the means of the processing. Please refer to section 1 below for further information about the Bank as controller;
- "processor" means private person (e.g. natural person, legal entity) that processes personal data on behalf of the controller.

If the Bank provides separate or further information about how it collects and uses Applicant's personal data for a particular purpose, those terms will also apply (e.g. consent forms, etc.).

If you provide the Bank with personal data of other persons (such as references, family members), you shall ensure that the respective persons are aware of this Data Privacy Statement and that you only provide the Bank with their data if you are allowed to do so.

This Data Privacy Statement is aligned with the Swiss Data Protection Act ("DPA") and the EU Data Protection Regulation ("GDPR"). However, the application of these laws depends on each individual case.
Please familiarize yourself with this Applicant Data Privacy Statement.

1. Who is responsible for the processing of your personal data and who can you contact in this regard?

The controller (and sometimes as joint controller) of data processing as described in this Data Privacy Statement is bank zweiplus ltd. (with registered address at Buckhauserstrasse 22, 8048 Zurich, Switzerland).

You can contact the Bank on any data protection related matters, using the following contact details of the Bank's Data Protection Officer:

bank zweiplus ltd
Data Protection Officer
Buckhauserstrasse 22
CH-8048 Zurich
Switzerland

E-Mail-Adresse: dataprotection@bankzweiplus.ch

The Bank's representative in the European Union is Banque J. Safra Sarasin (Luxembourg) SA, 17–21, Boulevard Joseph II, L-1840 Luxembourg.

2. What sources and personal data does the Bank collect and use?

In the context of your job application and the hiring process, personal data can be processed to assess and initiate a potential employment relationship with the Applicant, including, but not limited to, the Applicant's suitability for his/her job or whether it is necessary for the initiation of the employment contract.

The personal data the Bank collects or has about an Applicant come from different sources. This includes personal data provided to and collected by the Bank in order to take steps prior to entering into an employment contract and to prepare the employment contract, when initiating the employment relationship.

Some of the personal data will come directly from the Applicant. Some might be obtained from other third parties (such as headhunters). Personal data might also come from other J. Safra Sarasin Group[2]-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) Depending on the stage of the process the following information may be required to be provided from the Applicant 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 an Applicant given to the Bank by sending your application portfolio, filling in forms or by communicating with the Bank, whether face-to-face, by phone, e-mail, on-line or otherwise;
- Information concerning an Applicant's identity (e.g. passport information which does also contain a photograph) or which is relevant for authentication purposes (e.g. sample signature);
- Data with regard to an Applicant's education (diplomas, certificates, internships, special trainings etc.), language skills and professional experience (profile, data on previous employers, termination of last employments and work carried out, special projects etc.) including reference checks if provided to the Bank with references in an Applicant's CV or otherwise;
- If applicable, whether an Applicant possesses a working permit and details of this working permit;
- Any other personal data that an Applicant presents the Bank with as part of his/her application with the Bank;
- Extract from the criminal records register;
- Extract from the debt register.

b) Depending on the stage of the process the following information about the Applicant may be collected or generated by the Bank, such as:

- Application data;
- Information regarding an Applicant's financial situation such as debt data;
- Information the Bank collects or generates to comply with its obligations under the anti-money laundering regulatory framework and banking regulations (e.g. information on criminal records, Background screening);
- Information the Bank may collect through a digital assessment of information that is available on the internet (e.g. social media presence such as LinkedIn), insofar as this presence is open and publicly available;
- Geographic information;
- Information included in relevant Applicant files (e.g. education, work experience, reference letters, references, information) and any other comparable information provided by you;
- Information on salary and grade details, including data held on staff organigrams;
- Information generated in company documents, correspondence, e-mail, telephone calls (including audio or video recording) including Applicant's personal data in the course of carrying out the hiring process;
- Video recording in the context of surveillance of the Bank's premises ;
- Information used in 'cookies' and similar technologies on websites and in e-mails to recognize a data subject, remember a data subject's preferences and show a data subject content the Bank thinks he/she is interested in;
- Information related to telecommunications and internet and/or intranet data to the extent such information results from the use of

[1] In order to facilitate readability, "Employee" refers to all genders; the masculine form is used for male, female and diverse employees. To the extent justified by the context, the singular includes the plural and vice versa.

[2] This includes entities of J. Safra Sarasin Holding Ltd Group in Switzerland and abroad.

Applicant Data Privacy Statement

the company tools and resources, to the extent permissible under applicable laws and in compliance with internal policies and directives;

c) Information about the Applicant that the Bank collects from other sources, for example:

- Information available in registers (e.g. commercial registers and registers of associations, registers available on the Internet);
- Information from publicly available sources and combined information from external sources.

In certain limited circumstances, the Bank may collect sensitive data about you (also called "special category data"), such as for example information relating to your social security number, trade union affiliation, health or criminal record to fulfil its contractual or statutory obligations. Sensitive data includes different types of data relating to racial or ethnic origin, political opinions, religion or similar beliefs, trade union affiliation, physical or mental health data, criminal records, administrative proceedings and sanctions. Should you provide the Bank with sensitive data for any reason, the Bank acknowledges this as your explicit consent to process that data in the way as described in this Data Privacy Statement.

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

The Bank processes personal data of Applicants for various purposes in accordance with the provisions of the Swiss DPA and the European GDPR 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

The processing of personal data is carried out in order to take steps to initiate such an employment relationship.

The purposes of data processing relate to the initiation of such an employment relationship and internal directives, policies and guidelines and the applicable laws.

b) In the context of balancing interests and the purposes of safeguarding legitimate interests respectively

Where required, the Bank processes personal data beyond the actual fulfillment of its pre-contractual due diligence to initiate an employment relationship 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:

- Consulting and exchanging data with information offices (e.g. debt register, ZEK/IKO) to investigate creditworthiness, determine default risks;
- 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 and planning, insurance, audit and administrative purposes;
- 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;
- Complying with applicable Swiss and other legal statutory and regulatory requirements.

c) On the basis of your consent

Insofar as you have granted the Bank consent to process your personal data for specific 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 issuance of this Applicant Data Protection Statement. 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 or in the public interest

Furthermore, the Bank is subject to various legal obligations, i.e. statutory requirements (e.g. the Banking Act and labour law) as well as bank regulatory requirements. Purposes of processing include for example money laundering prevention measures, measuring and managing risks within the Bank and the J. Safra Sarasin Group (including for consolidated supervision purposes) and ensuring that the requirements in regard to good reputation of the Bank's administration and management as well as irreproachable conduct of the Bank's business operations can be met at all times.

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

4. Who does the Bank share your personal data with? Is your personal data disclosed abroad?

Within the Bank various units are given access to personal data of Applicants in order to conduct the hiring process and meet statutory obligations or as further described in this Applicant Data Privacy Statement.

In the context of the Bank's business activities and in line with the purposes and legal grounds of the data processing set out in section 3 above, the Bank may transfer data (incl. personal data) to third parties, insofar as such a transfer is permitted and the Bank deems it appropriate, in order for them to process data for the Bank or, as the case may be, their own purposes.

If a recipient is located in a country without adequate statutory data protection, the Bank requires the recipient to undertake to comply with data protection standards (for this purpose, the Bank namely uses the revised European Commission's standard contractual clauses which can be accessed here: https://eurlex.europa.eu/eli/dec_impl/2021/914/0j?), unless the recipient is subject to a legally accepted set of rules to ensure data protection or unless the Bank cannot rely on an exception, all in order to ensure that your personal data continues to receive appropriate protection. An exception may apply for example in case of a legal proceedings abroad, but also in cases of overriding public interest or if the performance of a contract requires disclosure, if you have consented or if data has been made available generally by you and you have not objected against the processing.

The Bank may disclose your personal data, in particular, to the following categories of recipients:

Types of third parties receiving data	Purpose of the transfer	Location of the third parties receiving data
Other companies within the J. Safra Sarasin Group	For risk control purposes due to statutory or other 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	See list of companies and their location on the Group's website[3]

[3] https://jsafrasarasin.com/content/jsafrasarasin/language-masters/en/company/locations.html

Applicant Data Privacy Statement

Types of third parties receiving data	Purpose of the transfer	Location of the third parties receiving data
Various headhunters, recruiting firms, referees, and background checks firms	To assist the Bank in recruiting you	Mainly in Switzerland & Europe
Third parties involved in specific activities, particularly those relating to information and communication technologies (e.g. phone, email, chat, videoconferencing, co-browsing).	To provide services and operate the Bank's business activities (your personal details may be accessible to such third parties during the chat/videoconference, phone or email-exchange etc. and for a limited time thereafter).	The countries where you and the third parties are located at the time of the communication (including the US in connection with the use of Webex)
Law firms/entities providing legal advice	To obtain professional legal advice in respect of the hiring process	The countries where the legal or dispute issue arises or has a connection with, but primarily Switzerland and Europe
Other parties in possible or pending legal proceedings	To comply with any legal or regulatory obligations as well as defend the legitimate interests of the Bank	The countries where the concerned other parties are located, but primarily Switzerland and Europe
Domestic and foreign authorities, courts or arbitral tribunals (e.g. the Swiss National Bank, Swiss Financial Market Authority (FINMA), other financial authorities, tax authorities, criminal prosecution authorities)	To comply with any legal or regulatory obligations the Bank has as well as defend the legitimate interests of the Bank	The countries where the concerned authorities, court or arbitral tribunals are located

The aforementioned table is a general description of the various scenarios where the Bank may share data. Additional recipients of personal data may also 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 privacy obligations by agreement or consent. All these categories of recipients may involve third parties, including sub-processors of personal data, so that your data may also be disclosed to them. The Bank can restrict the processing by certain third parties (for example IT providers), but not by others (for example authorities).

As indicated in the above table, certain recipients may be within Switzerland but some may be located in other countries, including countries in Europe and the USA.

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.

5. How long will personal data be stored?

The Bank will process and store personal data of Applicants for as long as it is necessary to fulfil the Bank's Human Resources process, after which they will be deleted.

If an Applicant becomes an effective employee of the Bank, the Employee Data Privacy Statement and applicable data retention periods will further apply.

6. What data protection rights do you have?

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

- Right of **access**
- Right to **rectification**
- Right to **erasure**
- Right to **restriction of processing**
- Right to **object to the data processing**
- Right to **data portability**.

The right of access and the right to erasure are subject to certain restrictions. In case you exercise your right to restrict or object to the processing, 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.

You shall address any request in that regard to the Bank's Data Protection Officer as mentioned under section 1 above.

Furthermore, if applicable on a person, there is also a right to lodge a complaint with an appropriate data privacy supervisory authority.

7. How is personal data kept secure?

The Bank implements internal technical and organisational measures to keep personal data of Applicants safe and secure which may include encryption, anonymization, access limitations (e.g. limitation of user rights or use of passwords) 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.

8. Is there an obligation to provide data?

In the context of the initiation of a potential employment relationship with the Bank an Applicant must provide all personal data which is necessary for the establishment of such employment 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 any employment contract or employment relationship without collecting and processing personal data.

Applicants are responsible to make sure the information provided to the Bank is accurate and up to date.

In particular, provisions in the bank law and regulatory authority's regulations in regard to the "proper and rightful conduct of business" requirement each bank has to comply with, implies that the Bank verifies a data subject's personal data by means of a document of evidentiary value (e.g. excerpts of the debt register and the criminal records register) and that the Bank collects and records certain data (e.g. subject's name, place of birth, date of birth, nationality, residential address and other data for that purpose) in order to establish their Applicants' suitability for their jobs. 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 bank law and the regulatory authority's regulations and notify the Bank without undue delay of any changes. If a data subject does not provide the Bank with the necessary information and documents, the Bank may not be allowed to enter into the employment relationship.

9. Is "profiling" or "automated decision-making" used?

Automated decisions are defined as decisions about individuals that are based solely on the automated processing of data and that produce legal effects or that significantly affect the individuals involved. As a rule, the Bank does not make use of automated decision-making as described above in relation to the initiation of employment agreement. In particular, the Bank does not base its decision whether or not to hire you solely on automated processing of your personal data.

Should the Bank use automated decision-making in the future, the Bank will inform you accordingly and 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.

In some cases, the Bank uses profiling to process assessments in the hiring stage with the aim of

Applicant Data Privacy Statement

evaluating certain personal aspects of an Applicant. The Bank may further also process data to develop predictive analytics. If such analytics are done the results are whenever possible anonymized to ensure no conclusions can be made on individuals.

10. Changes to the Applicant Data Privacy Statement

You may request another copy of this Applicant Data Privacy Statement from the Bank using the contact details set out in section 1 above. The Bank may modify or update this Applicant Data Privacy Statement from time to time by making such a revised version available on the Bank's website.

Issue Date: 1st September 2023