



Data protection information

1. Preliminary remarks

Rothschild & Co Bank AG, Zollikerstrasse 181, 8034 Zurich (the “**Bank**”) has issued the below privacy statement (the “**Privacy Statement**”) in the light of the upcoming revision of the Swiss Federal Act on Data Protection (the “revFADP”).

With the following information, the Bank would like to give an overview of how personal data will be processed and of the data subject's rights according to data privacy laws. The details on what data will be processed and which method will be used depend significantly on the services applied for or agreed upon. Hence, not every element of this information may be applicable to all clients and data subjects (the “**Client**”, e.g. authorized representative, authorized signatory, holder of a power of attorney, director, beneficial owner, potential new client / prospect).

2. Who is responsible for data processing and who can the Client contact?

The Client can reach the Bank's responsible department and representative(s) for data protection matters at:

Rothschild & Co Bank AG
Data Protection Administration
Zollikerstrasse 181
8034 Zurich
Switzerland
E-Mail: data.protection@ch.rothschildandco.com

3. Which sources and which data do we use?

The Bank processes personal data that it obtains from the Clients in the context of the business relationship. The Bank also processes – insofar as necessary to render its service – personal data that it obtains from publicly accessible sources (e.g. debt registers, land registers, commercial and association registers, press, internet) or that is legitimately transmitted to it by other companies in the Rothschild & Co Group or from other third parties (e.g. a credit agency).

The Bank may collect various types of personal data about the Clients, depending on the particular services it provides, including, but not limited to:

- identification data (e.g., name, ID card, passport details and other national ID numbers, date and place of birth, nationality, gender, IP address);
- contact details (e.g., address and email address, phone number);
- family situation (civil status, number of children);
- authentication data (e.g., specimen signature);
- financial status (e.g., creditworthiness data, scoring/rating data, origin of assets);

- background checks;
- tax situation;
- banking, financial and transaction-related data with respect to the assets deposited with the Bank and investments made through the Bank (e.g. bank account details, payment orders, securities transactions, transaction history, investment advice);
- loan-relevant data (e.g. revenues and expenditures);
- marketing and sales data (including advertising scores);
- data from the interactions between the Bank and the Client (e.g. meetings, calls, emails, documents exchanged);
- data relating to the Clients' use of the Bank's services, in particular their internal and external IDs, information about how they use the Bank's website and applications and the pages they visit, the date and duration of use of the Bank's services, web pages and applications, the users of the services, web pages and applications and the approximate geographical location (city, country) of their devices, the websites visited by the users, and the type of service provided;
- cookie information (e.g., cookies and similar technologies on websites and in emails – for more information, please refer to our Cookies Policy <https://www.rothschildandco.com/en/cookies/>);
- and other data similar to the categories mentioned.

4. What does the Bank process the Clients' data for (purpose of processing) and on what legal basis?

The Bank processes personal data in accordance with the provisions of the revFADP (as well as the EU General Data Protection Regulation (**GDPR**) and applicable regulations like DFIC Data Protection regulations) as follows:

4.1 To fulfill its contractual obligations

Data is processed in order to provide banking and financial services in the context of carrying out the Bank's contracts with Clients or to carry out pre-contractual measures that occur as part of a client request.

The purposes of data processing are primarily in compliance with the specific product (e.g. bank account, credit, securities, deposits) and can include, among others, needs assessments, advice, asset management and support, as well as carrying out transactions.

The Bank may thus use personal data, *inter alia*:

- to manage its contractual relationship with the Clients (including, but not limited to: (i) to manage the Clients' account, as well as any products or services that the Clients have subscribed to; (ii) to manage contract-related communications with the Clients; (iii) to provide services, including the payment of fees and/or invoicing; and to advise and assist its Clients), as well as to execute any related transaction;
- to manage its pre-contractual relationship with the Clients and, subsequently, to open and manage an account and/or to start a business relationship with the Bank, including all formalities relating to the identification of the Clients;
- to comply with and enforce the applicable terms of contracts;
- to send administrative information (such as, for example, an update of the Bank's general terms and conditions or any report prepared by the Bank regarding its services); and
- to manage, administer and distribute collective investments funds, including any ancillary services related to such activities.

Clients can find further details about the purposes of data processing in the relevant general terms and conditions and contract documents.

4.2 To pursue its legitimate interests

Where required, the Bank processes Client data for the purposes of the legitimate interests pursued by the Bank or a third party, including, *inter alia*:

- to consult and exchange data with information offices (e.g. debt register) so as to investigate creditworthiness and credit risks in credit business and the requirement in connection with exemption from seizure of assets;
- to review and optimize procedures for needs assessment for the purpose of direct client discussions;
- for marketing or market and opinion research purposes, unless a Client has objected to the use of its data;
- to establish, assert and/or defend actual or potential legal claims;
- to prove transactions;
- to ensure the security of the Bank's premises and infrastructures (such as access controls);
- to ensure IT security and IT operations of the Bank;
- to prevent, detect and investigate crimes (in particular fraud);
- to train the Bank's personnel (e.g. by recording phone calls);
- to improve the Bank's business, to improve the quality of its services, as well as to further develop its services and products;

- to develop its relationship with the Clients;
- to undertake data analytics to learn more about how the Clients interact with the Bank's websites, its applications and its advertising;
- to analyse and predict some of the Clients' personal preferences, interests and behaviours based on their use of the Bank's services, website, and applications (profiling); and
- for risk management purposes within the Rothschild & Co Group.

In addition, the Bank obtains personal data from publicly available sources for client acquisition purposes.

4.3 To comply with its legal and regulatory obligations

The Bank is subject to various legal and regulatory obligations and has to comply with other legal process and law enforcement requirements, which may include laws outside the country the Client is located in, including, *inter alia*:

- to check the Clients' identity and age;
- to set up measures to prevent abuse, fraud and money laundering (e.g. to detect transactions that deviate from usual patterns);
- to comply with regulations related to the prevention of money laundering, financial crime, financing of terrorism and market abuse;
- to comply with regulations related to sanctions and embargoes;
- to comply with regulations related to financial markets (in particular with respect to investor protection);
- to fight against tax fraud and to comply with any applicable tax supervision and reporting obligations;
- to comply with any applicable transaction reporting obligation; and
- to comply with the Bank's prudential obligations (e.g. in terms of risk identification, management and control).

4.4 As a result of Client's consent

Where the Bank would need to process personal data for purposes other than those listed in sections 4.1 to 4.3 above, it shall inform the Client, and, where necessary, request its consent.

In addition, the Client acknowledges that, as long as it has granted the Bank consent to process its personal data for certain purposes, this processing is legal on the basis of the Client's consent. Consent given can be withdrawn at any time. Withdrawal of consent does not affect the legality of data processed prior to withdrawal.

5. Who receives Client data?

Within the Bank, every unit which requires Client data to fulfill the Bank's contractual and statutory obligations will

have access to it, on a need-to-know basis. Service providers and vicarious agents appointed by the Bank may also receive access to data for the purposes provided in this Privacy Statement, if such third parties maintain banking confidentiality. These are companies which are active, mainly, in the categories of banking services, IT services, logistics, printing services, telecommunications, collection, advice and consulting, and sales and marketing.

The Bank is obliged to uphold banking secrecy with respect to all client-related matters and assessments of which the Bank acquires knowledge (banking confidentiality pursuant to the Bank's general terms and conditions).

The Bank may transfer information about a Client only: (i) if legal provisions require it (i.e. the provision of personal data would thus be mandatory); (ii) if a Client has given its consent (e.g. to process a financial transaction a Client has ordered the Bank to handle); or (iii) if the Bank has been authorized to issue an account inquiry. Under these circumstances, recipients of personal data can be, for example:

- public entities and institutions (e.g. Swiss National Bank, FINMA) and other competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction upon request and to the extent permitted by law;
- other credit and financial service institutions or comparable institutions (including Rothschild & Co Group companies) to which the Bank transfers the Client's personal data in order to carry out a business relationship with a Client (depending on the contract, e.g. correspondent banks, custodian banks, brokers, stock exchanges, information offices, providers which perform banking, payment, investment management for the Bank);
- creditors or liquidators submitting queries in connection with a foreclosure;
- service providers (including Rothschild & Co Group companies) which perform services on the Bank's behalf, such as communication infrastructure providers, IT providers, distribution platforms and courier services or providers of monitoring and alert management related to certain activities on the Bank's information systems, development and/or operation and provision of a core business platform and other software, including internal and external communication interfaces (including with the Client);
- service providers in connection with credit or bank cards;
- certain types of professionals (e.g. legal advisors, accountants, auditors, insurers and tax advisors);
- facilitators and external asset managers;
- third parties in connection with the granting of a loan (such as Rothschild & Co Group companies, insurance

companies, investment companies, trustees, service providers carrying out value assessments);

- other companies belonging to the Rothschild & Co Group for the purpose of risk control due to statutory or official obligations (e.g. for group-wide monitoring of compliance, money laundering and other risks);

Other recipients of data can be any units for which a Client has given the Bank its consent to transfer data or for which a Client has released the Bank from banking confidentiality by means of a declaration or consent.

Irrespective of the above, the Bank reserves its right to make personal data accessible to other recipients, as disclosed to the Clients from time to time or where required by applicable laws or requested by a competent authority.

Where the transfer of personal data is mandatory (e.g. with respect to the Bank's legal and/or regulatory obligations), the Client understands that, should it withdraw or refuse its consent to such transfer, the Bank may be precluded from having a business relationship with the Client and/or from rendering (all or part of) its services to the Client, and/or performing certain transactions.

Finally, further information is set out in the Information Notice published by the Swiss Bankers Association "Information from the SBA regarding the disclosure of client data and other information in international payment transactions and investments in foreign securities", which is also available at the following link:
<https://www.swissbanking.ch/en/financial-centre/information-for-bank-clients-and-companies/information-for-bank-clients>

6. May data be transferred outside of Switzerland?

The Bank may transfer, communicate or store personal data to States outside Switzerland, the EU or the European Economic Area ("EEA"), where:

- it is necessary for the purpose of carrying out contractual obligations directly or indirectly related to the Banks relationship with the Client (e.g. payment and securities orders by the Client);
- it is required by law (e.g. reporting obligations under fiscal law or reporting obligations of certain stock exchange transactions);
- it is necessary to enable the Bank to establish, exercise or defend itself against a present or future claim, or to enable it to deal with an investigation by a public authority, in Switzerland or abroad;
- it is necessary to protect an overriding public interest; or
- Clients have granted their consent.

In the context of an international transfer, personal data may be transferred to:

- a State for which the local competent authority provides an adequate level of data protection (from a Swiss perspective).
- a State that does not offer an adequate level of data protection (from a Swiss perspective). In such a case, the Bank will either (i) obtain the Client's consent, or (ii) put in place appropriate contractual, technical and/or organizational safeguards (e.g., contract based on the standard contractual clauses "SCC" adopted by the European Commission, recognized by the Federal Data Protection and Information Commissioner "FDPIC" and adapted to Swiss data protection legislation) to ensure the protection of the Client's personal data.

The list of destination countries may be found under the following link:
https://www.rothschildandco.com/siteassets/publications/rothschildandco/wealth_management/legal/en_wm_list_of_countries_to_which_personal_data_may_be_transferred.pdf.

To obtain more details on international data transfers, the Clients may contact the Data Protection Officer, at the address provided for in section 11 below.

7. For how long will Client data be stored?

The Bank will process and store personal data of Clients for as long as it is necessary in order to fulfill its contractual and statutory obligations.

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

- fulfilling obligations to preserve records according to commercial and tax law: This includes, in particular, the Swiss Code of Obligations, the Federal Act on Value Added Tax, the Federal Act on Direct Taxation, the Federal Act on Harmonization of Direct Taxes of Cantons and Municipalities, the Federal Act on Stamp Duties and the Federal Act on Withholding Tax.
- The Bank can face legal holds, which requires keeping records for a defined or undefined period of time (e.g. US program for Swiss banks). A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.

8. What data protection rights does a Client have?

Each Client has the following rights:

- the right to access its personal data: i.e. the right to obtain information with respect to the data the Bank processes (article 25 revFADP, article 15 GDPR and article 33 of DFIC DP Law);
- the right to object at any time to the processing of its personal data, on grounds relating to its particular situation (article 32 revFADP, article 21 GDPR and article 32 of DFIC DP Law);

- the right to withdraw its consent: where the Client has granted its consent to the Bank processing its personal data, the Client has the right to withdraw its consent at any time. The Client notes that the withdrawal only applies to the future. Processing that was carried out before the withdrawal is thus not affected by it;
- the right to rectify its personal data, where such data is inaccurate or incomplete (article 32 revFADP, article 16 GDPR and article 33 of DFIC DP Law);
- the right to erase its personal data: i.e. the right to have its personal data deleted to the extent permitted by law (article 32 revFADP, article 17 GDPR and article 33 of DFIC DP Law);
- the right to restrict the processing of its personal data (article 32 revFADP, article 18 GDPR and article 33 of DFIC DP Law);
- and if applicable – the right to data portability (article 28 revFADP, article 20 GDPR and article 37 of DFIC DP Law). Furthermore, if applicable to a Client, there is also a right to lodge a complaint with an appropriate data protection regulatory authority (article 77 of the GDPR).

The Bank draws the Client's attention to the fact that, even if the Client objects to the processing of its personal data, the Bank is entitled to continue the processing if it is:

- required by law;
- necessary for the performance of a contract to which the Client is a party;
- necessary for the performance of a task carried out in the public interest; or
- necessary for the Bank's overriding legitimate interests, including the establishment, exercise, or defense of legal claims. The Bank will not use for direct marketing purposes personal data of Clients who object to such processing.

9. Does a Client have to provide the Bank with data?

In the context of the Bank's business relationship with a Client, a Client must provide all personal data that is required for accepting and carrying out a business relationship and fulfilling the accompanying contractual obligations that the Bank is legally obliged to collect.

In particular, anti-money laundering regulations require the Bank to identify Clients on the basis of the Client's identification documents (e.g. passport, ID card) before establishing a business relationship and to collect and put on record e.g. name, address and other contact details, place and date of birth, nationality, and identification details for this purpose.

In order for the Bank to be able to comply with these statutory obligations, a Client must provide the Bank with the necessary information and documents in accordance with the Swiss Anti-Money Laundering Act, and to

immediately disclose any changes over the course of the business relationship.

If a Client does not provide the Bank with the necessary information and documents, the Bank cannot enter into or continue the business relationship with a Client as desired.

10. Will profiling take place?

The Bank processes some of the Client data automatically, with the goal of assessing certain personal aspects (profiling). The Bank uses profiling for the following cases, for instance:

- Due to legal and regulatory requirements, the Bank is obligated to combat money laundering, terrorism financing, and offenses that pose a danger to assets. Data assessments (including on payment and securities transactions) are also carried out for this purpose. At the same time, these measures also serve to protect Clients.
- The Bank uses assessment tools in order to be able to specifically notify Clients and advise those regarding products. These allow communications and marketing to be tailored as needed – including market and opinion research. In individual cases, the Bank processes personal data of Clients in order to conduct direct marketing. A Client has the right to object to the processing of 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 a Client objects to processing for the purpose of direct marketing, the Bank will no longer process a Client's personal data for this purpose.
- The Bank can use scoring for example as part of the assessment of a Client's creditworthiness. This calculates the probability that a Client will meet the payment obligations pursuant to the contract. This calculation may be influenced by the Client's earning capacity, expenses, pending liabilities, occupation, employer, term of employment, experience from the business relationship thus far, contractual repayment of previous credits, and information from credit information offices, for instance. Scoring is based on a mathematically and statistically recognized and established process. The calculated scores help the Bank to make decisions in the context of product sales and are incorporated into ongoing risk management.

11. Contact

In case of questions on this Privacy Statement, please contact:

Rothschild & Co Bank AG
Data Protection Administration
Zollikerstrasse 181
8034 Zurich
Switzerland
E-Mail: data.protection@ch.rothschildandco.com