

Data Privacy Statement

In this Privacy Statement, Privatbank Bellerive AG ("PBB") provides information on how it processes personal data and what rights persons whose personal data is processed ("data subjects") have under the Data Protection Act. Personal data is any data relating to an identified or identifiable natural person. PBB defines processing as the handling of personal data, regardless of the means and procedures used, in particular the acquisition, storage, retention, use, modification, disclosure, archiving, deletion and destruction of data.

1. Responsibility and Competence

Responsible for data processing:

Privatbank Bellerive AG
Mittelstrasse 6
8008 Zurich
Telephone: +41 44 388 6464
Email: info@bellerivebanking.ch
www.bellerivebanking.ch

Responsible for exercising the rights under the Data Protection Act:

Privatbank Bellerive AG
Legal, Compliance & Risk
Mittelstrasse 6
PO Box, 8034 Zurich
Telephone: +41 44 388 6467
Email: compliance@bellerivebanking.ch

Basic provisions on data protection are also contained in PBB's General Terms and Conditions. These govern the mutual relationship between PBB and the contracting party.

2. Sources and categories of personal data processed

PBB processes personal data from the following sources:

- Personal data received from customers, interested parties, visitors and suppliers for the purpose of conducting a business relationship, such as on the occasion of an information meeting or an e-mail exchange.
- Personal data legitimately disclosed to PBB by third parties for the purpose of providing a service, such as operators of settlement systems, managers of collective assets, asset managers, among others.
- Personal data disclosed to PBB by public authorities in the course of their activities, in particular by courts, public prosecutors, regulators (e.g. FINMA), child and adult protection authorities.
- Personal data obtained from publicly accessible sources, including the commercial register, land registers and media as well as the Internet.

The specific personal data that PBB processes depends in particular on the products and services that data subjects use. Customer data is divided into the following categories:

- Personal data: e.g. surname, first name, date of birth, nationality, gender, address and other contact data, tax ID number, identification data (e.g. identity card, passport) and authentication data (e.g. specimen signature).

- Portfolio data: e.g. contract numbers, information on the account, securities account or concluded transactions.
- Transaction, order and risk management data: e.g. payment order data, details on mandate issuance, risk, investment and customer profile, information on financial circumstances such as creditworthiness data.
- Market data: e.g. needs, wishes and preferences.
- Documentation data: e.g. correspondence.
- Registration data: e.g. in connection with certain offers such as newsletter delivery, free WLAN access and access controls to certain facilities, e.g. vault.
- Technical data: e.g. internal and external identifiers, IP addresses, records of access or changes.
- Other data: e.g. photos, videos, sound recordings of telephone calls, security cameras, occasions with official or legal proceedings, files or evidence.

PBB processes data of interested parties and visitors with regard to a possible conclusion of a product or service contract. In particular, the following personal data is processed:

- Personal and inventory data such as surname, first name, date of birth, nationality, gender, address and other contact data such as telephone number and e-mail address.
- Technical data such as internal and external identifiers, IP addresses, records of access or changes.
- Product, service development and marketing data such as needs, requests or preferences.

Personal data of business partners, their employees and agents are processed within the framework of the contractual business relationship. This includes in particular the following personal data:

- Personal and inventory data such as surname, first name, date of birth, address and other contact data such as telephone number and e-mail address, contract numbers and duration, information about the account or completed transactions.
- Technical data such as internal and external identifiers, IP addresses, business numbers, records of accesses or changes.

PBB may record telephone calls to the extent provided for by law or for training and quality assurance or evidentiary purposes. Video recordings are made for security reasons and for the purpose of investigating possible criminal acts, in particular in the area of the bank building and the bank facilities.

3. Purpose of and legal basis for the processing of personal data

PBB processes personal data in accordance with the applicable data protection provisions:

- For the fulfilment of contractual obligations: Personal data is processed for the purpose of providing financial services within the scope of pre-contractual measures, which are carried out upon request, or for the purpose of executing contracts with customers and business partners. The purpose of data processing depends mainly on the specific product (e.g. account, deposit, security, and loan) and may include, among other things, demand analyses, asset management and the execution of transactions. Further details on the purpose of data processing can be found in the contract and terms and conditions.
- In the context of balancing interests: To the extent necessary, PBB processes personal data beyond the actual performance of the contract in order to protect its legitimate interests or those of third parties, e.g.
 - Review and optimization of demand analysis procedures for direct customer approach or acquisition.
 - Assertion of legal claims and defence in legal disputes.
 - Ensuring IT security and IT operations.
 - Prevention and clarification of criminal offences.
 - Measures to ensure building security, including video surveillance, collection of evidence in the event of robberies and other crimes or to prove criminal acts.
 - Measures to ensure building and facility security, such as access controls.
 - Measures for business and risk management within PBB and for the further development of services and products.

PBB may also collect personal data from publicly available sources for the purpose of customer acquisition:

- Based on consent: If PBB receives consent to process personal data for specific purposes, it processes the personal data accordingly. Consent that has been given can be revoked. The revocation takes effect from the time of the revocation. Processing that took place before the revocation is not affected by the revocation.
- Due to legal requirements or in the public interest: PBB holds a license issued by the Swiss Financial Market Supervisory Authority FINMA as a bank within the meaning of the Federal Law on Banks and Savings Banks and is supervised by FINMA. PBB is therefore subject to strict legal and regulatory requirements and requirements of the Swiss Bankers Association and the Swiss National Bank SNB. The purposes for which personal data is processed include identity and age verification, fraud and money laundering prevention, the fulfilment of control and reporting obligations under tax law, and the assessment and management of risks within PBB.

4. Recipient of personal data

Within PBB, access to personal data is granted to persons who need it to fulfil legal and contractual obligations. For this purpose, third parties employed by PBB (order processors) may also receive and process data. These are companies in the categories of banking services, marketing, IT services, logistics, printing services, telecommunications, sales. The involvement of third parties is subject to careful review and compliance with banking and data protection regulations. Persons who process personal data are obliged, among other things, to maintain banking secrecy, insofar as bank client data is concerned, and data protection.

PBB only passes on personal data to third parties if there is a legal basis for doing so, if the data subject consents (e.g. in order to be able to carry out a financial transaction) or if PBB is obliged or authorized to provide the information. Under these conditions, recipients of personal data may include:

- Authorities: e.g. law enforcement and supervisory authorities, courts, debt collection and bankruptcy offices, inheritance authorities, child and adult protection authorities if there is a statutory or other legal basis or order.
- Credit and financial services institutions or comparable institutions to which PBB transfers personal data in order to carry out the business relationship: e.g. correspondence and custodian banks, brokers, stock exchanges, information offices.
- Settlement agents for payment transactions and securities trading with an international dimension.
- Service providers in Switzerland and abroad who process personal data on behalf of PBB or under joint responsibility with PBB, or who receive data from us under their own responsibility. Third-party services include, for example, IT services, the dispatch of information, marketing, sales, communication or printing services, the organization and holding of events and receptions, anti-fraud measures and services provided by consulting firms, lawyers and telecommunications companies. The service providers involved provide information about their independent services in their own privacy statements.

5. Transfer of data to a third country or international organizations

A data transfer to bodies in countries outside of Switzerland (third countries) takes place, as far as this:

- is necessary for the execution of orders (e.g. payment and securities orders)
- is required by law (e.g. tax reporting obligations, administrative and legal assistance vis-à-vis foreign authorities)
- is necessary due to the involvement of service providers (order processors)
- appears necessary for reasons of IT security or for the purpose of detecting cyber attacks
- takes place on the basis of consent.

The recipients of personal data mentioned in section 4 may be located in Switzerland, but also abroad. Personal data may be processed anywhere in the world. If a recipient is located in a country without adequate data protection (e.g. USA), PBB shall oblige the recipient to comply with adequate data protection by concluding recognized standard contractual clauses (e.g. consent, conclusion or performance of a contract, protection of overriding public interests, enforcement of legal claims or if the data is generally accessible and the data subject has not objected to its processing).

6. Duration of data storage

PBB processes personal data for as long as is necessary for the fulfilment of its legal and contractual obligations, taking into account the fact that the business relationship with a data subject is usually a continuing obligation lasting several years. If the data are no longer required for the fulfilment of the obligations, they are - as far as technically possible - regularly deleted, unless their temporary further processing is required for the following purposes:

- Fulfilment of retention obligations under commercial and tax law, in particular under the Swiss Code of Obligations, the Value Added Tax Act, and the Federal Act on Direct Federal Taxes, the Federal Act on the Harmonization of Direct Taxes of the Cantons and Municipalities, the Federal Act on Stamp Duties, the Money Laundering Act and the Withholding Tax Act).
- Assertion, exercise or defence of legal claims or special storage regulations that require storage for a specific or indefinite period of time.

7. Protection of personal data

PBB uses appropriate technical and organizational measures to protect personal data. These include the use of authentication and encryption technologies, firewalls, anti-virus protection, physical and technical access restrictions, security controls for internal and external IT services, and training and awareness-raising for employees and service providers.

8. Rights of the data subjects

Every data subject has the right to information, correction, deletion, restriction of processing, revocation and the right to data portability with regard to the personal data concerning him or her within the scope of the applicable data protection law. In addition, the data subject has a right of appeal to the competent data protection supervisory authority.

The data subject may revoke the consent to the processing of personal data at any time vis-à-vis PBB. The revocation is effective for the future and does not affect the legality of the data processed until the revocation. Upon revocation, the personal data of the data subject will no longer be processed for the relevant purpose, unless overriding private or public interests or the law permit further processing. The same applies if the data subject objects to data processing.

The data subject may exercise the rights by e-mail or letter, enclosing a copy of the ID or passport, to the office mentioned above. These rights are subject to legal requirements and restrictions (e.g. personal data cannot be deleted if there is a duty to retain it). PBB will inform the data subject of any restrictions.

9. Obligation to provide personal data

Personal data required for the establishment and fulfilment of the business relationship must be provided. Without this personal data, PBB cannot conclude a contract with the data subject, provide the requested service or make products available. Furthermore, PBB may be required by law to collect personal data. In particular, PBB must comply with money laundering regulations, identify the data subject by means of an identification document prior to the establishment of the business relationship and collect and record details such as name, place of birth, date of birth, nationality, address and identification data. To enable PBB to comply with these legal obligations, the person concerned must provide PBB with the necessary information and documents in accordance with the Anti-Money Laundering Act and notify PBB immediately of any changes during the course of the business relationship. If the person concerned does not provide the documents and information, PBB cannot enter into or continue the business relationship.

10. Automatic decision making

As a matter of principle, PBB does not make any individual decisions that are based exclusively on the automated processing of personal data and that entail a legal consequence for the data subject or significantly affect him. Otherwise, PBB will inform the data subject in accordance with the legal requirements and grant the corresponding rights. Specifically, the data subject may then state his or her position and request that the decision be reviewed by a natural person.

11. Use of profiling

PBB processes personal data automatically in individual cases in order to evaluate certain personal aspects of the customer (profiling). For example, we use profiling in the following cases:

- Identification of risks, in particular in connection with risk management or the fight against money laundering, abuse and fraud and IT security.

12. Cookies and other tracking and analysis technologies

PBB does not use cookies and other tracking and analysis technologies.

Zurich, September 1, 2023