Julius Bär

# PRIVACY POLICY OF BANK JULIUS BAER & CO. LTD., GUERNSEY BRANCH
## ON THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE DATA PROTECTION (BAILIWICK OF GUERNSEY) LAW, 2017

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Guernsey Law") reflects the provisions of the EU General Data Protection Regulation but covers all individuals, regardless of whether they are EU citizens or not. The following information from Bank Julius Baer & Co. Ltd., Guernsey Branch ("the Bank") is intended to give you an overview of how your data is processed by the Bank and your rights under the Guernsey Law. In this notice we refer to "you" as a client, a business partner, or a prospect of the Bank. Which data is processed and how it is used depends upon the requested or agreed service(s).

If anyone represents you in dealings with the Bank, such as agents or attorneys for example, or you provide the Bank with information about other people that is relevant to the services the Bank provides, such as family members or additional cardholders for example, this Privacy Policy also covers how the Bank handles the personal data of those individuals. Please ensure that you provide those individuals with a copy of this Privacy Policy and obtain their agreement to providing the Bank with their data before you do so.

### 1 CONTACT DETAILS OF THE PERSON RESPONSIBLE FOR DATA PROTECTION AT THE BANK

Data Protection Officer
Bank Julius Baer & Co. Ltd., Guernsey Branch No 1, The Plaza
Elizabeth Avenue Admiral Park
P.O. Box 87
St Peter Port Guernsey GY1 4BS
E-mail: data.gg@juliusbaer.com

The Group Data Protection Officer can be contacted at:

Bank Julius Baer & Co. Ltd.
Data Protection Adviser
Bahnhofstrasse 36
PO Box 8010 Zurich
Switzerland
E-mail: dataprivacy@juliusbaer.com

### 2 WHICH DATA IS USED BY THE BANK?

The Bank processes data that it receives from its business relationship with you. This includes, among other data, personal data, i.e. data that directly identifies you as a client (e.g. name, address, telephone number, etc.), or data which leads to this identification when used in connection with other information (e.g. account number). In addition to data that the Bank receives directly from you, it also obtains and processes data on you from sources available in the public domain (e.g. Internet, social media, debtor directories, land registers, trade and association registers, company registries, the print media, etc.) or from other companies within the Julius Baer Group or authorised third parties.

The following personal data is processed:

- personal details (name and any former name(s), address and other contact data, date and place of birth, as well as nationality);
- identification data (e.g. passport and other identification document data or other legal identifiers);
- authentication data (e.g. specimen signature);
- still images of you with your identification documents (only for cases where your identity and address is verified by video conference);
- account data (e.g. contact notes), details relating to your personal background and financial situation (e.g. information on compliance and/or regulatory matters such as credit reports, origin of wealth and funds, financial knowledge and experience) and/or company-related data (e.g. business activities, purpose, ownership and organisational structure as well as number of employees);
- data arising from the fulfilment of obligations, in particular related to services or transactions (e.g. account and transaction data including details of the principal and the recipient);
- information on your financial situation (e.g. data on creditworthiness, scoring/rating data, taxation-related data);
- advertising and sales data;
- documentation data (e.g. minutes of consultation);
- data that is transmitted and automatically collected during the use of websites or other electronic services provided by the Bank (electronic services). This data includes date and time of access, name of file downloaded as well as the amount of data transmitted and the access result, your web browser, the browser language and the requesting domain and IP address. Further information can be found in the privacy policy or the legal provisions of the respective electronic service;
- data comparable with the above mentioned criteria.

For non-personal clients (e.g. corporates, trusts, partnerships, foundations, etc.) we will collect personal data on key individuals, such as controllers, shareholders, beneficial owners, partners, authorised signatories, trustees, settlors, enforcers, protectors, beneficiaries, foundation officials and underlying policyholders.

**Special category data**

This is defined as data revealing racial or ethnic origin, religious, political or philosophical beliefs, genetic, biometric, health data or data concerning an individual's sexual orientation. It also includes data relating to criminal offences committed or alleged to have been committed.

The Bank is required under Guernsey financial crime legislation to:

- identify individuals through use of identity documents containing a photograph, which may reveal the person's racial or ethnic origin;
- verify certain information in relation to parties to an account with the Bank, including their source of wealth. The Bank may utilise open source intelligence available using public search engines, information recorded on public media sites as well as other commercially available subscription based sources in order to do this. This open source information may contain special category data such as references to, for example, political opinions and affiliations, religious or philosophical beliefs, physical or mental health or to offences committed or alleged to have been committed;
- screen the names of parties to an account against international sanctions lists.

The Bank does not require your consent for collecting and processing this special category data in relation to the above obligations because it is necessary to do so in order for the Bank to comply with financial crime legislation.

The Bank may also collect information on:

- your health, because you may choose to provide information on specific medical because you think it is relevant to your financial objectives and you want the Bank to take this into account when it advises you;
- your political opinions or religious or philosophical beliefs where you choose to provide the Bank with information on these because you think it is relevant to the choice of investments the Bank should be able to make for you.

The Bank will collect this information if you choose to give it to the Bank, and if it is directly relevant to the services the Bank provides you with. You are not obliged to provide the Bank with it and the Bank will ask you for your consent to use it. However, if you do not allow the Bank to collect it, the Bank's services may not meet your needs because the Bank cannot take that information into account. As explained later in this Privacy Notice, you may withdraw your consent to the Bank using this information at any time by writing to the Bank. If you do, the Bank will cease to use it from then on.

Occasionally the Bank may be made aware of health conditions which may affect your ability to make decisions about your financial affairs and you are unable to give your consent to the Bank using it or the Bank cannot reasonably be expected to obtain it. This might be, for example, if you have been in an accident or suffered a medical event that has temporarily affected your ability to make your wishes known. In such a case, the Bank may keep a record of this information to help it act in ways aimed at protecting your economic wellbeing, for example making sure the Bank knows that your attorney will be acting for you or adjusting how the Bank provides its services to account for the impact of your health condition. But if circumstances change so the Bank can obtain your consent the Bank will only continue to collect and use that information if you do give your consent.

Biometric data is personal data of a particularly sensitive nature. Therefore, where necessary, the Bank will obtain separate, express consent before, for example, using your fingerprint or any other biometric identification feature for accessing certain applications or uses.

## 3 FOR WHAT PURPOSE AND ON WHAT LEGAL BASIS DOES THE BANK USE YOUR DATA?

a) For the fulfilment of contractual obligations

The processing of your data allows the Bank to establish and manage its client relationship with you and provide you with its services. The particular purpose for which the data will be processed is primarily governed by the products and services you have requested which may involve operating your bank accounts, safeguarding and administering your assets, providing financial advice, wealth management, wealth planning, financing & credit services, and arranging or executing payments and transactions in and transfers of your assets). Your data will also be used to analyse your preferences, needs and objectives and to assist the Bank with providing you with a tailored and comprehensive offering of services and improving the Bank's relationship with you.

b) On the basis of statutory requirements or in the public interest

The Bank will process data to ensure compliance with the legal and regulatory obligations to which it and other members of the Julius Baer Group are subject and to respond to enquiries of and otherwise satisfy the requirements of the judicial, regulatory, tax and other governmental authorities to whose jurisdiction it or they are subject (such as undertaking "know your client" procedures, the verification of creditworthiness as well as identity and age, the prevention of fraud and money laundering or terrorist financing, the fulfilment of monitoring and reporting obligations, as well as the assessment, investigation, analysis and management of risks in the Bank and within the Julius Baer Group).

c) Within the context of the legitimate interest of the Bank and Julius Baer Group

To protect its own legitimate interests or interests of third parties, the Bank will also process your data for the following purposes, provided that these interests are not overridden by your rights and freedoms:

- preventing and investigating criminal acts;
- testing and optimising processes for needs analysis or client contact;
- for the proper management and supervision of the Bank's business, including conducting financial management, system management, legal and regulatory compliance monitoring, physical and technology security monitoring, litigation, internal audits and investigations, business continuity management, reputation management and other tasks related to the management of the risks to which members of the Julius Baer Group are exposed, and obtaining professional advice in this context; safeguard and enforce the interests and rights of the Bank or other members of the Julius Baer Group, including recovery of fees and debts due to the Bank;
- responding to and defending the Bank, Julius Baer Group companies and their officers and employees against any allegations, in any legal disputes with clients and third parties and in any investigations undertaken by any judicial, regulatory, tax or other governmental authorities to whose jurisdiction it or they are subject;

- for the purpose of conducting international supervision and oversight of the business of the Julius Baer Group as a whole, including by consolidation and maintenance of the data relating to you that the Bank and Julius Baer Group companies possess (single-client view);
- consultation and exchange of data with information agencies (e.g. debt recovery registers) for determining creditworthiness and/or default risks in the credit business;
- advertising, market and opinion research or surveys, provided you have not objected to this use of your data;
- safeguarding the Bank's IT security and IT operation;
- for maintaining the security of the Banks' premises and systems, such as by video surveillance entry controls;
- for the development of its business and that of the Julius Baer Group as a whole, including the development of new services and products;
- collection of personal data from sources available in the public domain for the purpose of market research and business development.

**Recording and storage of communications**

The Bank may record, store and otherwise process communications involving clients, prospective clients, business partners and other relevant third parties. Such communications may include:

- electronic communications (e.g. emails, instant messages and chat messages);
- telephone conversations;
- video conferences and virtual meetings; and
- related metadata, including telephone numbers, email addresses, meeting identifiers and the date, time and duration of communications.

Such recording, storage and processing may occur where required to comply with legal or regulatory obligations to which the Bank or other members of the Julius Baer Group are subject and/or where necessary for the legitimate interests of the Bank or the Julius Baer Group.

The Bank may process recorded communications for purposes including:

- documenting interactions with clients, prospective clients and business partners;
- creating records of meetings and communications, including minutes, notes, transcripts and summaries, whether produced manually or through the use of automated technologies, including artificial intelligence tools;
- evidencing instructions, decisions, transactions and other communications relating to products and services provided by the Bank;
- complying with legal, regulatory and risk management requirements;
- preventing, detecting and investigating fraud, financial crime, market abuse and other unlawful or improper conduct;
- monitoring service quality and staff training;
- investigating and resolving complaints, disputes and enquiries; and
- establishing, exercising or defending the rights and interests of the Bank and other members of the Julius Baer Group, including in connection with litigation, regulatory investigations and other proceedings.

Recorded communications may be accessed by authorised personnel of the Bank, other members of the Julius Baer Group and relevant service providers where necessary for the purposes described in this Privacy Policy.

For further information regarding the disclosure, international transfer, retention and other processing of recorded communications, please refer to the relevant sections of this Privacy Policy.

**Marketing**

The Bank may use your personal information to tell you about products and services that the Bank thinks may be of interest to you, taking into account the services the Bank already provides you with and the Bank's knowledge of your financial circumstances and interests, as the Bank believes that this supports the provision of a tailored and high-quality service to its clients. Where the Bank carries out such activities, it will do so in a proportionate way, and will not use your personal data for marketing purposes where your rights and interests outweigh those interests.

**You have the right at any time to object to the use of your personal data for direct marketing purposes. If you do so, the Bank will stop using your personal data for such purposes. To do this please contact your relationship manager or contact the Bank's Data Protection Officer using the details given in paragraph 1 of this policy.**

## 4 WHO CAN ACCESS YOUR DATA?

Within the Bank and other Julius Baer companies, access is only granted to those personnel who require your data for purposes for which it is collected and processed by the Bank (need-to-know principle).

The Bank may appoint other Julius Baer Group companies and third-party service providers to perform functions on the Bank's behalf or to provide services to the Bank and they may in turn use the services of subcontractors (the Julius Baer Group companies, the third-party service providers and the subcontractors, each a "Service Provider"). The relevant functions and services may include IT functions (e.g. data hosting and processing, IT development, support, operation, including the use of "cloud"-based IT services), the usage of internet-based services (e.g. online commercial register), the processing of transactions and services (e.g. payments), reporting and output services), wealth management services and ancillary activities, services related to the safeguarding, administration, trading, execution and processing of financial instruments and other financial assets, compliance and risk management functions, accounting (financial accounting and controlling), financing and credit services, marketing and sales-related activities and reporting and output services as well as other back-office and middle-office activities.

The Bank ensures that the Service Providers with access to or otherwise processing your personal data are contractually bound to comply with appropriate confidentiality, data protection and data security obligations.

The Bank may also transmit data to other external recipients for the purposes described above, who may include:

- judicial, regulatory, tax or other governmental authorities (e.g. Guernsey Financial Services Commission, Guernsey Revenue Service, law enforcement authorities);
- other credit and financial services institutions or similar institutions with whom the Bank deals in the course of providing its services to you (e.g. correspondent banks, custodian banks, brokers, stock exchanges, securities commissions, information agencies);
- other companies within the Julius Baer Group;
- the Bank's professional advisers, such as lawyers and auditors;
- other data recipients for which you have given your consent.

The Bank may exceptionally share information with the public or media in circumstances where you or your representatives have made inaccurate or misleading statements to the public or media that the Bank considers are damaging to the Julius Baer brand, including by damaging the Bank's reputation or that of other members of the Julius Baer Group or their respective officers and employees. But the Bank will only do so to the extent reasonably necessary to correct the factual record.

## 5 DOES THE BANK TRANSMIT THE DATA ABROAD?

The Bank may disclose your data to jurisdictions where Julius Baer Group Companies are established or located or to any other jurisdiction around the world where any Service Provider is located or where the Bank executes transactions or provides services.

Your data may be transmitted to entities in other countries outside Guernsey if:

- the data is transferred to other Julius Baer Group entities;
- the data is transferred to Service Providers;
- this is required for the execution of your orders (e.g. payment and securities orders);
- it is a statutory requirement (e.g. disclosure obligations under tax law);
- it is provided for in your agreements with the Bank or in the General Banking Conditions or you have given your consent in another way.

Furthermore, recipients of your personal data may forward the information to their branches or group entities, service providers or to other market participants or authorities within and/or outside its jurisdiction.

Data may therefore be disclosed to countries which include Switzerland, the United Kingdom and other members of the European Economic Area. These countries are considered to have data protection laws that are equivalent to those in Guernsey.

Data may also be disclosed to other countries, where it will be governed by the local laws and regulations of that country which may offer a lower level of data protection and client secrecy protection than the laws and regulations applicable in Guernsey. In these cases, the Bank will generally ensure an adequate level of data protection by concluding data transfer agreements with the recipients of your personal data in third countries.

By way of an exception, your personal data may also be transferred to countries without an adequate level of protection in other cases, e.g. based on your consent, in connection with legal proceedings abroad or if the transfer is required in order to execute a contract.

Please contact the Data Protection Officer if you would like more information on this topic.

## 6 HOW LONG WILL YOUR DATA BE STORED?

The Bank processes and keeps your data only for as long as is necessary to fulfil its contractual, regulatory and legal obligations.

If the data is no longer required for the fulfilment of these obligations, it will be deleted at regular intervals, unless it is still required for further processing. This requirement could be:

- on instruction from a public body in the context of an ongoing enquiry or investigation (e.g. an ongoing law enforcement, regulatory or tax matter);
- in the event of anticipated litigation;
- if the Bank is unable to delete it for technical reasons (in which case, the Bank will seek to put your data beyond use).

## 7 WHAT ARE YOUR RIGHTS UNDER THE GUERNSEY LAW?

Under the Guernsey Law you have the following rights. You can:

- request access to your personal information which enables you to receive a copy of the personal information the Bank holds about you and to check that the Bank is lawfully processing it;
- request that this be corrected if it is incorrect;
- request that this data be deleted if the Bank is not permitted or does not have a reason to store this data;
- request that the processing of this data be restricted. This enables you to ask the Bank to suspend the processing of personal information about you, for example if you want the Bank to establish its accuracy or the reason for processing it;
- object to the processing by the Bank:
  - if the Bank only processes the data on the basis of its legitimate interests; in this case it will cease the processing unless this is outweighed by its own interests or it needs to process the data in order to exercise its rights;
  - if the processing is carried out with a view to direct advertising;
  - request that your personal data which you have provided to the Bank be transmitted to another party in a generally available, machine-readable, and standard format;
  - object to a decision made purely on the basis of automated processing.

You also have a right to complain to the Data Protection Commissioner at the Office of the Data Protection Authority in Guernsey if you believe that the Bank has breached the above rights or any other provision of the Guernsey Law. The Commissioner can be contacted on +44 (0)1481 742074 and its website, which includes details of how to make a complaint, is www. odpa.gg

## 8 IS DECISION-MAKING AUTOMATED?

You have the right to object to a decision made purely on the basis of automated processing. However, as a basic principle, the Bank does not use fully automated decision-making for commencing and conducting the business relationship. If the Bank does apply this procedure as an exception in individual cases, it will inform you separately of this.

## 9 WILL YOUR DATA BE AUTOMATICALLY PROCESSED?

In specific areas, the Bank will process your data on a semi-automatic basis, the aim being to evaluate certain personal criteria (profiling), for example, in the following cases:

- In order to combat money laundering, the financing of terrorism, and criminal acts such as fraud, the Bank also conducts data assessments (e.g. in payment transactions). The aim of these measures is to protect you.

- The Bank uses assessment tools to provide you with interesting and appropriate information on its products. This enables it to carry out demand-based communication and advertising, including market and opinion research.

- As part of its assessment of your creditworthiness, the Bank uses an algorithm based on a mathematical-statistical process. This is how it calculates the likelihood of clients fulfilling their payment obligations. The algorithm can, for example, include income ratios, expenditure, existing liabilities, occupation, employer, duration of employment, experience from the previous business relationship, the contractual repayment of previous loans as well as information from credit rating agencies. The results of the analysis assist the Bank in making decisions within the context of product sales and are also incorporated into the ongoing risk management.

## 10 WHAT DATA DO YOU HAVE TO SUPPLY?

The Bank requires you to provide the data necessary for the acceptance and execution of a business relationship and the fulfilment of the associated contractual and/or legal obligations.

Under Guernsey financial crime legislation, the Bank is obligated to verify your identity on the basis of your identification document and in this context to collect and store your full name and any former names, your address, nationality, place of birth, date of birth, occupation and identification data prior to the commencement of a business relationship. In order for the Bank to comply with this legislation, you are obligated to supply it with the necessary information. Unless it has this data, the Bank is usually unable to conclude or implement the contract with you. If this information changes during the course of the business relationship, you are obliged to notify the Bank without delay. If you do not provide the Bank with the necessary information, it will not be able to commence or continue a business relationship with you.

## 11 WHERE CAN YOU FIND THE CURRENT PRIVACY POLICY?

This Privacy Policy can be adapted at any time in accordance with the corresponding regulations.

You can find the respective current version at
www.juliusbaer.com/en/legal/privacy-notices-for-clients

## 12 HOW CAN YOU CONTACT THE BANK?

If you have any questions about how your data is treated, your relationship manager as well as the Bank's Data Protection Officer mentioned in paragraph 1 of this document will be happy to assist you.

Guernsey, October 2026