Data privacy statements of Postbank – a branch of Deutsche Bank AG

The following data privacy statements provide an overview of the collection and processing of your data.

The following information is supposed to provide you with an overview of the manner in which we process your data, as well as your rights under the respective data privacy laws. The issue of which specific pieces of data are processed and the manner in which the said data is used is primarily determined on the basis of the requested or agreed-upon services.

1. Who is responsible for data processing and who can I contact?

The authority responsible is:

Deutsche Bank AG
Taunusanlage 12
60325 Frankfurt am Main, Germany
Tel.: +49 (0)228 920 – 0
Fax: +49 (0)228 920 – 35151
Email address: direkt@postbank.de

You can contact our corporate data protection officer at:

Postbank – a branch of Deutsche Bank AG
Data protection officer
Kennedyallee 62
53175 Bonn, Germany
Tel.: +49 (0)228 920 – 0
Fax: +49 (0)228 920 – 35151
E-mail address: datenschutz@postbank.de

2. Which sources and which pieces of data do we use?

We process the personal data that we receive within the framework of our business relationship from our clients. To the extent that such a course of action is necessary for us to be able to provide our services, we also process the personal data that we permissibly obtain from publicly accessible sources (e.g. lists of debtors, land registers, commercial registers, registers of associations, the press and the internet), as well as the personal data that is permissibly provided to us by other companies belonging to the Deutsche Bank AG (hereinafter referred to as "Bank") or other third parties (e.g. a commercial credit agency).

The relevant personal data consists of personal particulars (name, address and other contact data, date of birth, place of birth and nationality), legitimation data (e.g. identification data) and authentication data (e.g. specimen signature). Such data can also include job data (e.g. payment order), data that emerges as a result of the fulfilment of our contractual obligations (e.g. sales data in payment transactions), information regarding your financial situation (e.g. creditworthiness data, scoring/rating data, origin of asset values), advertising and sales data (including advertising scores), documentation data (e.g. minutes of consultations) and other data that is comparable to the specified categories.

3. Why do we process your data (objective of processing), and on what legal basis?

We process personal data in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG):

a. In order to fulfil contractual obligations (article 6 section 1 b of the GDPR)

Data is processed in order to facilitate banking transactions and provide financial services. This is done within the context of the execution of our contracts with our clients, or in order to implement pre-contractual measures that are implemented upon request.

The objective of such data processing is primarily geared towards the specific product in question (e.g. account, credit, building society savings, commercial papers, investments and arbitration). Among other things, the objectives of such data processing operations can relate to requirements analyses, consultations and the execution of transactions.

Further details of the data processing objectives can be found in the applicable contract documents and business conditions.

b. Within the context of the weighing of interests (article 6 section 1 f of the GDPR)

If necessary, we also process your data in a manner that extends beyond the actual execution of the contract, in order to protect our legitimate interests or the legitimate interests of third parties. Examples:

- Consulting and exchanging data with credit agencies (e.g. SCHUFA) in order to determine credit or default risks, or in order to determine requirements in situations involving garnishment exemption accounts or basic accounts,
- Checking and optimising requirements analysis procedures for the purpose of direct customer approach,
- Advertising or market and opinion research, if you have not objected to the use of your data,
- Raising legal claims and carrying out defence activities in case of legal disputes,
- Safeguarding the bank's IT security and IT operations,
- Preventing and solving criminal offences,
- Video surveillance for protecting domiciliary rights, for collecting evidence in situations involving muggings and fraud-related offences, or for providing evidence of dispositions and deposits, e.g. at ATMs (cf. §4 of the Federal Data Protection Act),
- Measures related to building security and system safety (e.g. access controls),
- Measures for safeguarding domiciliary rights,
- Measures related to business management and the further development of services and products,
- Risk control within the Postbank corporation.

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

If you have given your consent for the processing of personal data for specific purposes (e.g. forwarding of data within the corporation, evaluation of payment transaction data for the purposes of marketing), such processing is considered to be legal on the basis of your consent. Consent that has been granted can be revoked at any time. This also applies to the revocation of declarations of consent that were issued to us before the GDPR became valid (i.e. before 25 May 2018). The revocation of consent has no effect on the legality of the data that was processed before revocation.

d) On the basis of statutory provisions (article 6 section 1 c of the GDPR), or in the public interest (article 6 section 1 e of the GDPR)

Being a bank, we are also subject to diverse legal obligations, i.e. legal requirements (e.g. the Credit Services Act, the Money Laundering Act, the Securities Trading Act, tax laws) and banking supervisory regulations (e.g. the regulations issued by the European Central Bank, the European banking regulatory authority, the German Central Bank and the German Federal Financial Supervisory Authority). Among other things, the objectives of data processing relate to credit investigations, identity checks, age checks, the prevention of fraud and money laundering, the fulfilment of tax law-related monitoring and reporting obligations and the evaluation and management of risks within the bank and the Postbank corporation.

4. Who receives my data?

Access to your data is provided to the entities within the bank which need such access in order to fulfil our contractual and legal obligations. Service providers and sub-contractors employed by us can also receive data for these purposes, provided that they maintain banking confidentiality. Such entities are companies associated with the domains of credit-related services, IT services, logistics, printing services, telecommunications, collection operations, consultation and consulting and sales and marketing.

With regard to the forwarding of data to recipients outside our bank, it should first be noted that we are, as a bank, obligated to maintain the confidentiality of all customer-related matters and evaluations that become known to us (banking confidentiality as per no. 2 of our terms and conditions). We are only allowed to forward information about you if legal regulations mandate such a course of action, if you have given consent for such a course of action or if we are authorised to provide bank references. Under these conditions, personal data can be provided to (for example):

- Public sector entities and institutions (e.g. the German Central Bank, the German Federal Financial Supervisory Authority, the European Banking Authority, the European Central Bank, finance authorities, law enforcement agencies), if a corresponding legal or official obligation exists.
- Other credit and financial service institutes or comparable institutions to whom we send personal data in order to be able to execute our business relationship with you (e.g. (depending on the contract) correspondent banks, depositary banks, stock exchanges, credit agencies)
- Other companies within the Bank, for risk control and on the basis of legal or official obligations.

Other data recipients could be the entities for which you have given us consent to transfer data or, as the case may be, for which you have exempted us from banking confidentiality in accordance with an agreement or consent.

923 960 053 05.20

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

Data is transferred to entities located in countries lying outside the European Union (so-called 'third countries') if

- such a course of action is necessary in order to be able to execute your orders (e.g. payment and security orders),
- such a course of action is required by law (e.g. tax law-related reporting obligations) or
- you have given consent for such a course of action.

Except for these scenarios, the Bank does not transfer any personal data to international organisations or entities located in third countries. However, the Bank does engage service providers for certain tasks. These service providers usually engage other service providers, whose company headquarters, parent companies or computing centres may lie in a third country. A transfer is permissible if the European Commission has decided that the third country in question offers an appropriate level of protection (article 45 of the GDPR). If the Commission has not made such a decision, the Bank or the respective service provider may only transfer personal data to a third country or an international organisation if suitable guarantees are provided (e.g. standard data protection clauses that have been accepted for a specific procedure by the Commission or the regulatory authority), and if enforceable laws and effective legal remedies are available. The contracts that Postbank has signed with these service providers stipulates that an agreement shall always be reached between them and their contractual partners that ensures the adherence to fundamental data protection principles that are in line with the European level of data protection.

6. How long is my data stored?

We process and store your personal data as long as such a course of action is necessary for us to be able to fulfil our contractual and legal obligations. In this regard, it should be noted that our business relationship is a continuing obligation that remains in force for several years.

If the data is no longer required for the fulfilment of contractual or legal obligations, it is deleted on a regular basis, unless it needs to be processed further (over the short term) for the following purposes:

- The fulfilment of commercial law-related and tax law-related retention obligations: This scenario relates to the commercial code (HGB), the revenue code (AO), the Credit Services Act (KWG), the Money Laundering Act (GwG) and the Securities Trading Act (WpHG). The time limits for retention or documentation that are specified in these regulations amount to a period of time ranging from two to ten years.
- The preservation of evidence within the framework of the legal statutes of limitation. According to §§195 et seqq. of the Civil Code (BGB), these statutes of limitation can amount to up to 30 years, whereby the regular statute of limitation amounts to 3 years.

7. Which data privacy rights do I have?

Each person in question has the right to information as per article 15 of the GDPR, the right to amendment as per article 16 of the GDPR, the right to deletion as per article 17 of the GDPR, the right to limit processing as per article 18 of the GDPR, the right to raise objections as per article 21 of the GDPR and the right to transferability of data as per article 20 of the GDPR. The limitations associated with §§34 and 35 of the Federal Data Protection Act apply to the right to information and the right to deletion. The person in question also has the right to file a complaint with a responsible data protection supervisory authority (article 77 of the GDPR, in conjunction with §19 of the Federal Data Protection Act).

After you have given your consent for the processing of personal data, you can revoke this consent at any time. This also applies to the revocation of declarations of consent that were issued to us before the General Data Protection Regulation became valid (i.e. before 25 May 2018). Please note that such a revocation only applies to the future. Processing operations that were carried out before revocation are not affected by it.

8. Am I obligated to provide data?

Within the context of our business relationship, you are obligated to provide the personal data that is required for the commencement and execution of a business relationship and the fulfilment of the associated contractual obligations, or which we are legally obligated to collect. Without this data, we would normally be unable to conclude the contract with you or execute such a contract.

According to the regulations associated with money laundering laws, we are obligated to use your identification document to identify you before the business relationship is established; in this regard, we are also obligated to collect and record your name, place of birth, date of birth, nationality, address and identification data. In order to ensure that we can fulfil this legal obligation, you must, in accordance with the Money Laundering Act, provide us with the required information and documents; you are also obligated to promptly disclose any corresponding changes that may potentially be made over the course of the business relationship. If you do not provide us with the required information and documents, we will not be allowed to set up or continue the business relationship that you desire.

9. To what extent are decisions made automatically?

As a matter of principle, we do not use any fully automated automatic decision-making procedures as per article 22 of the GDPR to establish and execute the business relationship. If we do use such procedures in individual cases, we shall separately notify you to that effect, inasmuch as such a course of action is legally mandated.

10. Is profiling done?

To some extent, we do process your data automatically, with the goal of assessing certain personal aspects (profiling). For example, we use profiling in the following cases:

- Statutory and regulatory provisions obligate us to combat money laundering, terrorism financing and asset-jeopardising criminal offences. Data is also analysed in this context (in payment transactions etc.). These measures also serve to protect your safety.
- We use analysis instruments in order to be able to inform and advise you about products in a targeted manner. These instruments facilitate need-based communications and advertising (including market and opinion research).
- We use the scoring system while evaluating your creditworthiness. This involves calculating the probability that a client will fulfil his payment obligations in accordance with the contract. For example, these calculations could consider earning capacities, expenses, existing liabilities, professions, employers, the duration of employment, experiences from previous business relationships, the contract-oriented repayment of earlier loans and information obtained from commercial credit agencies. The scoring is based on an accepted and proven mathematical-statistical procedure. The calculated score values help us make decisions within the context of product sales, and they are also factored into the current risk management mechanism.

Right of objection

Information about your right of objection as per article 21 of the General Data Protection Regulation (GDPR)

1. Case-by-case right of objection

You have the right, at any time and for reasons related to your specific situation, to lodge an objection against the processing of personal data that relates to you [which takes place on the basis of article 6 section 1 sub-paragraph e of the GDPR (data processing in the public interest) and article 6 section 1 sub-paragraph f of the GDPR (data processing on the basis of a weighing of interests)]; this also applies to profiling that is based on this provision and which is associated with article 4 no. 4 of the GDPR. If you lodge such an objection, we shall no longer process your personal data, unless we can demonstrate urgent reasons worthy of protection for such processing which outweigh your interests, rights and freedoms, or unless the processing makes it possible to raise, exert or defend legal claims.

2. Right to lodge an objection against data processing for the purposes of direct advertising

In individual cases, we process your personal data in order to conduct direct advertising.You have the right to lodge an objection at any time against the processing of personal data that relates to you for the purposes of such advertising; this also applies to profiling, if the profiling is associated with such direct advertising.
If you lodge an objection against processing that is carried out for the purposes of direct advertising, we shall no longer process your personal data for these purposes.
Such an objection is not subject to any form-related requirements, and should, if possible, be addressed to:

Postbank – a branch of Deutsche Bank AG
Friedrich-Ebert-Allee 114-126
53113 Bonn, Germany

923 960 053 05.20

Postbank Luxembourg – a brand of
Deutsche Bank AG, Luxembourg Branch

Data protection – supplementary information for Luxembourg

On 25 May 2018, the EU General Data Protection Regulation (GDPR) comes into effect and replaces the previously valid Directive 95/46/EC from the year 1995. The new Regulation means that there are uniform rules throughout the whole of the EU governing handling personal data. Along with the GDPR and the Federal Data Protection Act, the legal basis for the processing of data by Postbank Luxembourg are the two following Luxembourg laws of 1 August 2018: Gesetz zur Gründung der CNPD und zur Einführung des allgemeinen Datenschutzrahmens (*"Law for the foundation of the CNPD and for the implementation of general data protection conditions"*) and Gesetz über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in Angelegenheiten, die das Strafrecht oder die nationale Sicherheit betreffen *("Law on the protection of naturals persons during processing of personal data in affairs concerning criminal law or national security")*.

The GDPR contains provisions on the free movement of data in the European Union and is intended to protect natural persons on processing of personal data. In the framework of the business relations with its customers, Postbank Luxembourg receives data on customers' beneficiaries and representatives and, where applicable, from third-party guarantors.
The rights of persons affected during data processing, therefore, apply to this group of persons.

At Postbank Luxembourg, the purposes of data processing and other information can be seen in the relevant contract documents and terms and conditions in the derivatives, credit and deposit business. With regard to storage of personal data, along with statutory provisions in Germany, the retention periods that apply in Luxembourg must also be taken into account, whereby the time limit is in principle ten years, but may be longer in individual cases because of specially regulated retention obligations, or for preservation of evidence.

In addition to the responsible agency and the company data protection officer in Germany, you can also contact the coordination office for data protection at Postbank Luxembourg:

Coordination office for data protection Luxembourg:
Postbank Luxembourg – a brand of
Deutsche Bank AG, Luxembourg Branch
18-20, rue Gabriel Lippmann
L-5365 Munsbach
Telephone: +352 / 34 95 31 -382 or +352 / 34 95 31 - 205
Email address: fma.pbnl-datenschutz@postbank.lu

Status: Mai 2020