

DATA PROTECTION NOTICE ACCORDING TO EU GENERAL DATA PROTECTION REGULATION

The following Data Protection Notice provides an overview of how your data are collected and processed.

The following information is intended to provide you with an overview of our processing of your personal data and your rights under data protection law. The data processed in a particular case and the manner in which they are processed are described below.

The following Data Protection Notice applies especially to customers, prospective customers, applicants and authorized representatives/agents. Therefore it is possible that not all parts of this information will apply to you.

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

The responsible party is:

UniCredit Bank GmbH

Arabellastr. 12

81925 München

Tel.: +49 (0)89 378 – 0

E-mail address: info@unicredit.de

You can reach our Corporate Data Protection Officer at:

UniCredit Bank GmbH

Datenschutzbeauftragter

Postfach

80311 München

Tel.: +49 (0)89 378 – 0

E-mail address: datenschutzrechte@unicredit.de

2. What data sources and types of data do we use?

We collect your personal data when you contact us, for instance as a prospect, authorised representative or agent, applicant, or customer – in other words, especially if you are interested in our products, submit applications, or use our products and services as part of an existing business relationship. In addition, to the extent necessary to provide our services, we process the personal data that we permissibly obtain from public sources (e.g. records of debtors, land registers, commercial registers and registers of associations, as well as the press, the Internet) and data that are legitimately sent to us by other companies in the UniCredit Group or other third parties (e.g. credit bureaus).

Relevant personal data in the prospect process, when recording master data, when authorising an agent, etc. may be personal identifiers (name, address, and other contact information, date and place of birth, and citizenship), identification data (e.g. ID information), authentication data (e.g. signature specimen), and taxpayer ID. In addition, this can also include order-related data (e.g. payment orders), data based on the performance of our contractual obligations (e.g. data on turnover from payment transactions), information regarding your financial situation (e.g. data regarding creditworthiness, scoring/rating data, source of assets), statements and records concerning knowledge and/or experience as regards securities, interest-bearing and currency products/financial investments (MiFID status: suitability/appropriateness test), advertising and sales data (including advertising scores), documentation data (e.g. minutes of consultations) and other data comparable to the above categories.

3. Why do we process your data (purpose of processing the data) and on what legal basis do we do so?

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

a. For the purpose of meeting contractual obligations (Art. 6 para. 1 b GDPR)

Data are processed to conduct banking business and provide financial services under the contracts with our customers and to implement pre-contractual measures, upon request (e.g. by interested persons). The purposes for which data processing is used primarily depend on the specific product (e.g. account, loan, home-purchase savings account, securities, deposits, brokering) and can include requirements analysis, consulting, and the execution of transactions, among other things. You can find additional details regarding the purposes for which data processing is utilised in the relevant contract documents and standard terms of business.

b. As part of a balancing of interests (Art. 6 para. 1 f GDPR)

In addition to processing your data for the actual performance of the contract, we process your data to the extent necessary to protect our legitimate interests and those of third parties.

Examples:

- Consulting and exchanging data with credit bureaus (e.g. SCHUFA) to determine the credit risk or risk of default in the lending transaction and the need for an attachment protection account or a basic account,
- Examining and optimising requirements analysis procedures for the purpose of direct customer contact,
- Advertising or market and opinion research, to the extent that you have not objected to this use of your data,
- Asserting legal claims and mounting a defence in legal disputes,
- Ensuring IT security and the security of the Bank's IT operations,
- Regular, incl. tool-based review and update of IT systems, applications and services to learn how we can improve their functionality and our services, or what other products and services we may offer
- Preventing and investigating criminal offences,
- Using video surveillance to protect domiciliary rights, to collect evidence of robberies and fraudulent acts, or to document dispositions and deposits, e.g. at ATMs (cf. also § 4 BDSG),
- Taking measures to ensure building and system security (e.g. admission control),
- Taking measures to ensure domiciliary rights,
- Taking measures to manage the business and further develop services and products,
- Ensuring risk control in the UniCredit Group

c. With your consent (Art. 6 para. 1 a GDPR)

To the extent that you have given us your consent to process your personal data for specific purposes (e.g. sharing data within the UniCredit Group, evaluation of payment transactions for marketing purposes), such processing is lawful based on your consent. Once given, your consent can be revoked at any time. This also applies to declarations of consent provided to us before the GDPR takes effect, i.e. before 25 May 2018. The revocation of consent does not affect the lawfulness of data processed before the revocation.

d. Based on legal obligations (Art. 6 para. 1 c GDPR) or in the public interest (Art. 6 para. 1 e GDPR)

Moreover, as a bank, we are subject to various legal obligations, i.e. statutory requirements e.g. the German Banking Act (Kreditwesengesetz), the Whistleblower Protection Act (Hinweisgeberschutzgesetz), the Supply Chain Due Diligence Act (Lieferketten-sorgfaltspflichtengesetz), the Money-Laundering Act (Geldwäschegesetz), the Securities Trading Act (Wertpapierhandelsgesetz), and the tax laws as well as bank regulatory requirements (e.g. those imposed by the European Central Bank, the European banking regulator, the German Central Bank and the German Federal Financial Supervisory Authority). The purposes for which processing is used include credit checks, identity and age checks, fraud and money-laundering prevention, the fulfilment of control and reporting obligations under tax laws and the assessment and control of risks to the Bank and the UniCredit Group.

4. Who receives my data?

Within the Bank, those parties that need access to your data to meet our contractual and statutory obligations receive such access. Service providers and agents utilised by us can also receive data for these purposes if they maintain banking secrecy. The latter are companies in the categories of credit services, IT services, logistics, printing services, telecommunications, collection, advising and consulting as well as sales and marketing.

With respect to the disclosure of data to recipients outside of our Bank, it should first be noted that, as a bank, we are obliged to maintain confidentiality with respect to all customer-related facts and assessments of which we obtain knowledge (banking secrecy in accordance with No. 2 of our Standard Terms of Business). We may only disclose information regarding you when statutory provisions so require or when you have consented to this or we are authorised to issue a bank reference. Under these conditions, the following parties may receive your personal data, e.g.:

- Public bodies and institutions (e.g. the German Central Bank, the German Federal Financial Supervisory Authority, the European Banking Authority, the European Central Bank, financial authorities, prosecuting authorities) if there is a statutory or regulatory obligation.
- Other banks and financial services institutions or comparable institutions to which we send personal data in the pursuit of our business relationship with you (depending on the contract, e.g. correspondent banks, custodian banks, stock exchanges, credit bureaus)
- Other companies in the UniCredit Group for risk control based on statutory or regulatory obligations.

Additional recipients of personal data can be those bodies to which you gave us your consent to transfer data or for which you released us from banking secrecy by agreement or consent.

5. Are data sent to a third country or an international organisation?

Data are transferred to locations in countries outside of the European Economic Area (so-called third countries) to the extent that

- this is necessary to fulfil your orders (e.g. payment orders and orders for securities),
- it is prescribed by law (e.g. notification obligations under tax law), or
- you have given us your consent.

Beyond this, UniCredit Bank GmbH transmits no personal data to locations in third countries or international organisations.

However, UniCredit Bank GmbH uses service providers for certain tasks, many of which also use service providers that may have their headquarters, parent companies or data centres in a third country. Data transfer is permissible if the European Commission has decided that there is an adequate level of protection in the third country (Art. 45 GDPR). If the Commission has not made such a decision, UniCredit Bank GmbH or the service provider may only transfer personal data to a service provider in a third country if suitable guarantees have been provided (standard data protection clauses, which have been accepted by the Commission or the supervisory authority in a specific proceeding) and enforceable rights and effective legal remedies are available. In addition, UniCredit Bank GmbH has contractually agreed with its service providers that basic data protection, which complies with the European level of data protection, must always be ensured by their contract partners.

Upon request, UniCredit Bank GmbH will provide you with a copy of the standard data protection clauses with the aforementioned providers.

6. For how long are my data stored?

We process and store your personal data for as long as is necessary to meet our contractual and statutory obligations, or as long as you are authorised to represent the particular (natural or legal) person to us. It should be kept in mind that our business relationship is a continuing obligation designed to last for years.

If the data are no longer necessary to meet contractual or statutory obligations, they are deleted on a regular basis, unless there is a need to further process the data – for a limited period of time – for the following purposes:

- To meet retention obligations under commercial and tax law: Such laws include the German Commercial Code (HGB), the Tax Code (AO), the Banking Act (KWG), the Money-Laundering Act (GwG) and the Securities Trading Act (WpHG). These laws prescribe two- to ten-year retention or documentation periods.
- To preserve evidence under the provisions of the statute of limitations. Under §§ 195 et seq. of the German Civil Code (BGB), statutes of limitations can last for up to 30 years. However, the most common statute of limitations is for three years.

7. What are my data protection rights?

Every data subject has the right to information under Article 15 GDPR, the right to rectification under Article 16 GDPR, the right to erasure under Article 17 GDPR, the right to restriction of processing under Article 18 GDPR, the right to object under Article 21 GDPR and the right to data portability under Article 20 GDPR. The restrictions in §§ 34 and 35 BDSG apply to the right to information and the right of erasure. In addition, there is a right to lodge a complaint with a competent data protection authority (Article 77 GDPR in conjunction with § 19 BDSG).

You can revoke consent to the processing of personal data at any time. This also applies to declarations of consent provided to us before the GDPR takes effect, i.e. before 25 May 2018. Please keep in mind that the revocation is only effective prospectively and does not affect any processing done before the revocation.

8. Do I have an obligation to provide data?

Within the framework of our business relationship, you must provide the personal data that are necessary to initiate and conduct the business relationship and meet the related contractual obligations, as well as the personal data we are required to collect by law. Without this, we would generally not be able to conclude or implement a contract with you.

If you are an authorised representative, you must provide us with the personal information that is necessary to commence and implement representation/authorisation and to fulfil the associated contractual duties, or that we are legally required to collect. Without these data, we would generally be obligated to reject you as an authorised representative/agent or cancel any existing authorised representation/agency, as applicable.

In particular, we are required by anti-money laundering regulations to identify you using your identification document before establishing the business relationship or before setting up the representation/authorisation, and in so doing to collect and record your name, place and date of birth, nationality, address, and identification information. For us to meet this statutory obligation, you must provide us with the information and documents required by the Money-Laundering Act and promptly notify us of any changes that occur in the course of the business relationship. If you do not provide us with the necessary information and documents, we may not initiate or continue the business relationship you desire or establish or continue the authorised representation/agency desired by the respective legal entity.

9. To what extent do we use automated decision-making?

In accordance with Article 22 GDPR, we generally do not use fully automated decision-making to establish and conduct the business relationship. If we use this process in individual cases, we will give you separate notice, to the extent prescribed by law.

10. Is profiling carried out?

At times, we use automated processing of your data with the goal of evaluating certain of your personal aspects (profiling). For example, we use profiling in the following cases:

- Under statutory and regulatory provisions, we are required to combat money-laundering, terrorist financing and crimes that endanger assets. Therefore, data analyses are conducted (with respect to payment transactions, etc.). These measures are also for your protection.
- We use evaluation tools to inform and advise you of our products in a targeted manner. These enable demand-oriented communication and advertising, including market and opinion research.
- We use scoring to assess your creditworthiness. Thereby, we calculate the probability that a customer will meet his or her payment obligations in accordance with the contract. For example, this calculation can be based on income level, expenses, existing liabilities, occupation, employer, length of employment, experiences in the business relationship to date, repayment of earlier credits in accordance with the contract, and information from credit bureaus. The scoring is based on a recognised and proven mathematical and statistical procedure. The scores calculated assist us in making decisions on completing products and are used in the ongoing risk management process.

Information regarding your right to object under Article 21 of the General Data Protection Regulation (GDPR)

1. Right to object in individual cases

Under Article 6 paragraph 1 letter e GDPR (data processing in the public interest) and Article 6 paragraph 1 letter f GDPR (data processing based on a balancing of interests), you have a right to object to the processing of your personal data at any time for reasons arising from your particular situation. This also applies to any profiling based on this provision within the meaning of Article 4 No. 4 GDPR.

If you lodge an objection, your personal data will no longer be processed, unless we can prove that there are compelling legitimate reasons for processing the data, which override your interests, rights and freedoms, or that processing serves the purpose of asserting, pursuing or defending against legal claims.

2. Right to object to the processing of data for purposes of direct advertising

In some cases, we process your personal data to engage in direct advertising. You have the right to lodge an objection against the processing of your personal data for the purpose of such advertising at any time. This also applies to profiling, to the extent that profiling is connected to such direct advertising.

If you object to processing for purposes of direct advertising, we will no longer process your personal data for these purposes. The objection can be informal and should, if possible, be sent to:

UniCredit Bank GmbH
Datenschutzbeauftragter
Postfach
80311 München
E-mail address: datenschutzrechte@unicredit.de