

Duties to provide information when collecting personal data pursuant to Articles 13 and 14 of the General Data Protection Regulation (GDPR)

The protection of your personal data is something of particular concern to us. We process your personal data solely on the basis of statutory provisions.

Below we provide you with information on the way we process your personal data and on your rights and remedies according to Articles 13 and 14 of the GDPR. Which data is processed in detail and in which way it will be used depends on the requested or agreed services. Therefore, not all parts of this information will apply to you.

Please also pass this information on to the current and future authorised representatives, trustees, beneficial owners, any co-debtors of a loan and, in the case of open third-party accounts, to the account holders. Should you transmit personal data of other individuals (e.g. of private tenants) within the scope of a business relationship, we would ask you to forward this information sheet to the persons in question too.

Data controller and contact person

Name and contact details of the controller

Aareal Bank AG
Paulinenstrasse 15
65189 Wiesbaden

Contact details of the company data protection officer

Aareal Bank AG
Data Protection Officer
Paulinenstrasse 15
65189 Wiesbaden
E-mail: datenschutz@aareal-bank.com

Processing framework

SOURCE. We process personal data that we receive from you in the course of our business relationship. In addition, to the extent necessary for the provision of our services, we process personal data that we have legitimately received from other companies or other third parties, e.g. a credit agency, (e.g. for the execution of orders, for the fulfilment of contracts or on the basis of a consent given by you). We also process personal data that we have legitimately obtained and may process from publicly accessible sources (e.g. debtor registers, land registers, commercial and association registers, press, media).

DATA. Relevant personal data are:

- personal details (name, address, date and place of birth, gender, marital status, nationality),
- contact details (e.g. phone, e-mail address),
- identification data (e.g. ID data) and authentication data (e.g. specimen signature),
- order data (e.g. payment order),
- tax information (e.g. tax ID, FATCA status, information on church tax liability),
- data from the fulfilment of our contractual obligations (e.g. payment transaction data, sales, credit lines, product data),
- information about your financial situation (e.g. creditworthiness data, scoring data, statements of income and balance sheets, business assessment, information / evidence on assets and liabilities, guarantees),
- information on any third-party beneficiaries, direct debit data, documentation data (e.g. consultation records, declarations of suitability),
- advertising and sales data,

- register data,
- contact information of customers and interested parties (e.g. information about the contact channel, date, occasion and result, information about participation in direct marketing activities),
- data about your use of the telemedia we offer (e.g. time of accessing our websites, apps or newsletter) as well as
- other data comparable with the above-mentioned categories.

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

1. For the performance of a contract (Article 6(1)(b) of the GDPR)

The processing of personal data takes place for the provision of banking transactions and financial services as well as for the brokerage of property deals as part of the performance of our contracts with our customers or for the performance of pre-contractual measures with you and the execution of your orders, as well as all activities required in the operation and administration of a credit and financial services institution.

The purposes of data processing are primarily guided by the specific product (e.g. account, loan, deposits, brokerage) and may include, among other things, needs assessments, advice, asset management and support as well as the execution of transactions.

Further details for the purpose of data processing can be found in the respective contractual documents and terms and conditions.

2. For the purposes of legitimate interests (Article 6(1)(f) of the GDPR)

If necessary, we process your data beyond the actual performance of the contract to protect the legitimate interests pursued by us or by a third party.

Examples:

- consultation and data exchange with credit agencies to determine creditworthiness and default risks,
- review and optimisation of procedures for needs analysis and direct approach of customers and interested parties,
- advertising or market and opinion research, as long as you have not objected to the use of your data,
- enforcement of legal claims and defence in legal disputes,
- ensuring the IT security and IT operation of the Bank;
- prevention and investigation of criminal offences,
- measures for building and system security (e.g. access control and video surveillance to safeguard house rights and to collect evidence in the event of criminal offences),
- measures for business management and further development of services and products,
- risk management within the Group.

3. On the basis of your consent (Article 6(1)(a) of the GDPR)

If you have given us your consent to process personal data for specific purposes (e.g. transfer of data within the Group, evaluation of payment transaction data for marketing purposes), the legality of such processing derives from your consent. A given consent can be revoked at any time. This also applies to the revocation of declarations of consent that were given to us before the GDPR was valid, i.e. before 25 May 2018. The revocation does not affect the legality of the data processed until the revocation.

4. For compliance with legal obligations (Article 6(1)(c) of the GDPR) or for the performance of a task carried out in the public interest (Article 6(1)(e) of the GDPR)

In addition, as a bank we are subject to various legal obligations, i.e. statutory requirements (e.g. German Banking Act, Money Laundering Act, tax laws) and requirements under banking supervisory law (e.g. of the European Central Bank, the European Banking Authority, the German Bundesbank and the German Federal Financial Supervisory Authority, BaFin). The purposes of processing include creditworthiness checks, identity and age checks, fraud and money laundering prevention, the fulfilment of tax control and reporting obligations and the assessment and management of risks in the Bank and within the Group.

Data transfer

Within the Bank, those departments that need your data to fulfil our contractual and legal obligations have access to it. Service providers and vicarious agents employed by us may also receive data for the aforementioned purposes if they observe banking secrecy and our written data protection instructions. These are companies in the categories of banking services, IT services, logistics, printing services, telecommunications, debt collection, consulting and sales and marketing.

With regard to the transfer of data to recipients outside the Bank, please note that, in accordance with the General Terms and Conditions agreed between us, we are obliged to maintain confidentiality about all customer-related facts and assessments of which we become aware (banking secrecy). We may only disclose information about you if required to do so by law, if you have given your consent, if we are authorised to disclose banking information, and/or, where the processing is carried out on behalf of us, the processor has provided sufficient guarantees to comply with the

banking secrecy and the requirements of the EU – General Data Protection Regulation / the German Federal Data Protection Act. Subject to these requirements, recipients of personal data may include, for example:

- public bodies and institutions (e.g. Deutsche Bundesbank, German Federal Financial Supervisory Authority, European Banking Authority, European Central Bank, financial authorities) in the event of a legal or official obligation.
- other credit and financial services institutions, comparable institutions or contract processors to which we transfer personal data in order to carry out the business relationship with you (e.g. correspondent banks, custodian banks, stock exchanges, credit agencies, depending on the contract).

Other recipients of data may be those bodies for which you have given us your consent to the transfer of data or for which you have exempted us from banking secrecy in accordance with an agreement or declaration of consent.

Storage

We will process and store your personal data as long as required to fulfil our contractual and statutory duties. It should be noted that our business relationship is a long-term obligation that is intended to continue for years.

If the data are no longer required for the fulfilment of contractual or legal obligations, they are regularly deleted, unless their - limited - further processing is necessary for the following purposes:

- fulfilment of commercial and tax storage obligations: these include the German Commercial Code (HGB), the Fiscal Code (AO), the German Banking Act (KWG), the German Money Laundering Act (GwG) and the German Securities Trading Act (WpHG). The periods

for storage and documentation specified there range from two to ten years.

- Preservation of evidence within the framework of the statutory limitation periods. According to sections 195 et seq. of the German Civil Code (BGB), these limitation periods can be up to 30 years, with the regular limitation period being three years.

Data transfer to third countries

Data are only transferred to third countries (countries outside the European Economic Area (EEA)) if this is necessary for the execution of your orders (e.g. payment orders), if it is required by law (e.g. tax reporting obligations) or if you have given us your consent. If service providers are used in third countries, your data will be processed there in compliance with the European data protection level. We will inform you separately about details, if required by law.

Rights of the data subject

Any data subject has the right of **access** (Article 15 of the GDPR), the right to **rectification** (Article 16 of the GDPR), the right to **erasure** (Article 17 of the GDPR), the right to **restriction of processing** (Article 18 of the GDPR), the right to **object** (Article 21 of the GDPR) and the right to **data portability** (Article 20 of the GDPR). With regard to the right of access and the right to erasure the restrictions of sections 34 and 35 of the BDSG apply. In addition, there is a right to lodge a complaint with a competent data protection supervisory authority (Article 77 of the GDPR in conjunction with section 19 of the BDSG).

You can revoke your consent to the processing of personal data at any time. This also applies to the revocation of declarations of consent that were given

to us before the General Data Protection Regulation was valid, i.e. before 25 May 2018. Please note that the revocation will only take effect in the future. Processing that took place before the revocation is not affected by this.

Obligation to provide data

In the context of our business relationship you only have to provide those personal data which are necessary for the establishment, execution and termination of a business relationship and the fulfilment of the associated contractual obligations or which we are legally obliged to collect. Without these data we will usually not be able to conclude or execute the contract with you.

In particular, we are obliged under money laundering regulations to identify you before establishing the business relationship, e.g. on the basis of your identity card and to collect your name, place of birth, date of birth, nationality as well as your address and identification data. In order for us to comply with this statutory provision, you must provide us with the necessary information and documents in accordance with the Money Laundering Act and notify us immediately of any changes arising in the course of the business relationship. If you do not provide us with the necessary information and documents, we are not permitted to establish or continue the business relationship you have requested.

Automated decision-making

We do not generally use fully automated decision-making in accordance with Article 22 of the GDPR for the establishment and implementation of the business relationship. Should we use these procedures in individual cases, we will inform you separately, insofar as this is required by law.

Profiling

We process some of your data automatically with the aim of evaluating certain personal aspects (profiling). For example, we use profiling in the following cases:

Due to legal and regulatory requirements, we are obliged to combat money laundering, terrorist financing and asset-endangering crimes. In this process, data is also evaluated (for example, in payment transactions). These measures are also designed to protect you.

Supervisory authority/right to lodge a complaint

If you believe that your data are not being processed properly, you have a right to lodge a complaint with the competent supervisory authority. Please address your complaint to:

The Data Protection Officer of Hesse
PO Box 3163
65021 Wiesbaden

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

If you have given your consent to the processing, you have the right to revoke your consent to the processing for the future at any time. This does not affect the lawfulness of the processing carried out up to that point.

1. Right of objection on a case-by-case basis

Where personal data concerning you was processed on the basis of Article 6(1)(e) (processing of data for the performance of a task carried out in the public interest) or (f) (processing of data for the purposes of legitimate interests), you have the right to object to such processing at any time for reasons arising from your particular situation. If you object, we will no longer process your personal data, unless we can provide compelling legitimate grounds for the processing which override your interests, rights and freedoms, or if the processing serves to establish, exercise or defend legal claims.

2. Right of objection to the processing of data for direct marketing purposes

In individual cases we process personal data for direct marketing purposes. You have the right to object at any time to the processing of personal data concerning you for the purpose of such advertising.

If you object to the processing for direct advertising purposes, we will no longer process your personal data for these purposes.

Your revocation can take place form-free and should be directed if possible to:

Aareal Bank AG
Informationssicherheit und Datenschutz
(Information security & data protection)
Paulinenstrasse 15
65189 Wiesbaden