

General Data Protection Policy

General Data Protection Policy

1. Information on collecting personal data

We provide information below on how we collect personal data and your entitlements and rights under data protection legislation. Personal data refers to any information relating to an identified or identifiable natural person. Processing personal data includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of such data.

2. Controller

The data controller is Bayerische Landesbank, Institution established under public law, Brienner Straße 18, 80333 Munich.

You can contact the data protection officer at:

Bayerische Landesbank
Institution established under public law
Data Protection Officer
Brienner Straße 18
80333 Munich, Germany
Tel: +49 89 2171-01
E-Mail: Datenschutz.BayernLB@bayernlb.de

3. Source and type of data

We process data of clients and other data subjects obtained as part of the business relationship and data received from other companies or third parties (e.g. SCHUFA) or, for clients of BayernLabo, from the government awarding authorities. We also process as part of business relationships personal data reliably obtained from public sources and which we are permitted to process (e.g. the debtor's register, the register of companies and associations, the press, the media).

As part of the relationship with a supplier or service provider or as part of employment, data provided by suppliers, service providers or employees is processed, as is data captured owing to the supply/service relationship or employment. There is also a small amount of data in special categories (e.g. data relating to health, absences due to sickness).

Relevant personal data includes, for example: personal details, identification data, authentication data, order data, register data, data on the use of our telemedia and advertising and sales data.

4. Purpose for processing personal data and legal basis for processing

We process the data of our clients and other data subjects as part of the customer relationship to meet contractual obligations, especially to provide and distribute banking transactions, financial services and insurance and real estate transactions. We also process personal customer data to protect our legitimate

interests and those of third parties, e.g. as part of consulting and exchanging data with information agencies to determine credit and default risk, for market research and opinion surveys, to enforce legal claims and defend legal disputes and to check and optimise procedures for analysing needs and contacting clients directly.

The personal data of clients is only processed with their consent. Consent may be withdrawn at any time. Processing may also take place as a legal requirement or in the public interest. This mainly applies to various legal obligations to which we are subject as a bank, e.g. statutory requirements arising from the Banking Act, the Anti-Money Laundering Act, the Securities Trading Act, tax law and banking supervision. The purposes for processing include credit checking, checking identity and age, preventing fraud and money laundering, meeting control and reporting requirements under tax law and assessing management and risk.

The processing of personal data of our suppliers, service providers and other third parties is carried out as part of general data processing to calculate remuneration and comply with the requirements to record, provide information and report and as necessary under law and regulation. It can also sometimes be necessary to process the data of suppliers, service providers and other third parties to ensure access to buildings or premises.

In addition, under the existing statutory data protection provisions data is processed to administer and protect systems, e.g. to manage user IDs, provide hardware and software for system users and for systems security.

In the event of a dispute in court during a service relationship or after one has ended, the data required to legally pursue the case appropriately in law will be transferred to legal representatives and courts.

The processing and transfer of data as part of **current employment** is carried out to calculate compensation or invoicing and to comply with the obligations to record, provide information and report, to the extent necessary under labour law or regulation or as a result of contractual obligation.

A series of employee data is processed under existing statutory data protection provisions to manage IT systems and keep them secure, e.g. to manage user IDs, provide hardware and software for system users and for systems security.

Professional contact data is published in internal and external media to allow colleagues to get in touch. We do this as we have a legitimate interest in ensuring seamless business processes. Employees may object to publication at any time.

If a legal dispute arises during an existing employment relationship or after it has ended, the data required for the purposes of prosecution will be passed on to legal representatives and courts.

Health data is processed by the Medical section to keep people fit for work, prevent occupational diseases and work-related sickness, support preventive healthcare, assist rehabilitation, cooperate with family doctors and allow personal consultation.

Religious denomination is given voluntarily with the consent of employees if they wish to claim associated rights or have church tax deducted by their employer. Private emergency contact details and information on employees' children and family (e.g. for voluntary social benefits or welfare calculations, etc.) are also given on the basis of consent. The same applies to the publication of photos of employees on the Intranet and the company's website.

The data of **former employees** for alumni purposes is only processed with express consent. Data of former employees with retirement benefit entitlements and their surviving dependants is processed in order to implement the respective retirement benefit systems. The data of former employees who are not entitled to retirement benefits is only processed to the extent required to meet obligations under German or EU law (Article 17 (3) b GDPR).

Data of job applicants is only processed for that specific purpose and is restricted to people involved in the application process. Once the purpose of the application process has been achieved (the position advertised

has been filled) applicant data is deleted, unless the applicant has given express consent to it being saved longer.

All consents can be withdrawn at any time independently of one another. Withdrawal means that the data may no longer be processed from that time onwards and the relevant rights, benefits etc. may no longer be claimed.

5. Data recipients

Within the Bank, those units which need access to the data of clients, employees and service providers to meet their contractual and legal obligations receive it. The contract data processors we use (Article 28 GDPR) or other recipients may receive data for the purposes stated above.

Personal data may only be transferred to recipients outside the Bank where it is relevant in the specific individual case on the basis of legal provisions or contractual agreement or consent, e.g. to the following bodies:

- Public bodies and institutions, where there is a legal or official obligation
- Other banking and financial services institutions or similar entities to carry out the relevant business relationship
- Professional representative bodies
- The authorities
- Courts
- Customers and interested parties of the controller
- Legal representatives

Please note when transferring client data to recipients outside the Bank that, under the General Business Conditions agreed between us and the client, we are required to observe confidentiality concerning all client-related matters and evaluations we learn about (banking confidentiality).

6. Duration of storage of personal data

We process and save your personal data as necessary for the duration of employment or the business relationship with the client or supplier/service provider.

Please note that the business relationship is an ongoing obligation extending over years.

We are subject to obligations to retain and document under, amongst others, the Commercial Code (HGB), the Tax Code (AO), the Banking Act (KWG), the Anti-Money Laundering Act (GwG) and the Securities Trading Act (WpHG). The retention and documentation periods stipulated are generally between two and ten years.

External tax audits (section 193 AO) can result in retention periods in excess of ten years.

Application documents as part of the application procedure are stored for up to six months after the end of the application process.

The duration of processing also takes account of the legal limitation periods. Under section 195 ff. of the Civil Code (BGB) these generally run for three years but can be as long as 30 years in some cases.

7. Transferring data to a third country or international organisation

Data is only transferred to a third country (a country outside the European Economic Area or EEA) where this is necessary to execute client instructions, for the purposes of a service relationship or for potential/current/former employment, is required by law or you have given us your consent. Where service providers in a third country are used, these must be required to comply with the level of data protection in the EU by agreeing to standard EU contractual clauses, in addition to written instructions.

We will inform you separately of details where legally required.

8. Data protection rights

Every data subject has the **right of access** 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 data portability** under Article 20 GDPR and the right to object under Article 21 GDPR. The right of access and right of erasure are subject to the limitations in sections 34 and 35 BDSG. There is also a **right to object** by lodging a complaint with a data protection supervisory authority under Article 77 GDPR in conjunction with Section 19 BDSG.

You may withdraw consent granted to us to process personal data at any time. This also applies to withdrawing declarations of consent which were granted to us before the GDPR came into effect, i.e. before 25 May 2018. Please note that the withdrawal only applies in the future. Data processing that was performed before the withdrawal remains unaffected.

9. Obligation to provide data

As part of a service agreement, business relationship or potential or actual employment you are only required to provide data needed to establish, execute and end the relationship in question or data we are legally obliged to collect.

In particular, we are required under anti-money laundering regulations to confirm the identity of our clients by means of an official identity document, for example, and record their name, date of birth, place of birth, nationality and home address. Under the Anti-Money Laundering Act our clients must provide us with the necessary information and documents to allow us to perform our legal obligation and notify us of any changes over the course of the business relationship immediately. If our clients do not provide the information required, we are not able to open the business relationship requested.

In connect with former employment, only the data needed to meet an entitlement to retirement benefits is required.

10. Information on automated decision-making in individual cases

We generally do not use automated decision-making as specified in Article 22 GDPR as the sole method for establishing and implementing a contractual relationship, business relationship or employment. If we use this procedure in individual instances we will inform you separately as legally required.

11. Use of data for scoring

We do not use profiling as specified in Article 22 GDPR to establish and implement a contractual relationship with suppliers, service providers or other third parties, or to establish and execute employment. If we use this procedure in an individual instance we will inform you separately as legally required.

We use profiling in some cases in business relationships with clients to evaluate certain personal aspects. This applies to the following cases in particular:

- Legal and regulatory requirements oblige us to combat money laundering, terrorist financing and criminal offences which endanger assets; as part of this, data (e.g. on payment services) is reviewed.

- When assessing the creditworthiness of our clients we carry out a credit check for retail clients and a rating for corporate clients. This is used to check whether a customer will meet their payment obligations as contractually agreed. The calculation includes, for example, income, expenses, forthcoming liabilities, profession, employer, length of employment, experience of the business relationship to date, punctual repayment of previous loans and information from credit reference agencies. Additional data is taken into account for corporate customers, such as sector, annual net profit and financial situation. The rating is based on a recognised and proven mathematical/statistical procedure. The ratings support us in making decisions regarding product sales and are incorporated into ongoing risk management.
- Personal data of BayernLB clients are is used to inform them of products in a focused manner and to advise them.

12. Right to object

You have the right to lodge an objection at any time based on grounds relating to your particular situation to the processing of personal data about you being carried out under Article 6 (1) e GDPR (processing in the public interest) and Article 6 (1) f GDPR (processing on a balance of interests).

If you object, we will no longer process your personal data unless we can provide compelling legitimate reasons for the processing which override your interests, rights and freedoms, or the processing serves the assertion, exercise or defence of legal claims.

In specific cases we process your personal data to engage in direct marketing. You have the right at any time to object to your personal data being processed for the purpose of such marketing; this also applies to profiling if it is connected with direct marketing.

If you object to your data being processed for the purposes of direct marketing, we will no longer process your data for this purpose.

The objection does not require any specific form and, if possible, should be addressed to:

Bayerische Landesbank
Institution established under public law
Brienner Straße 18
80333 Munich, Germany
Tel.: +49 89 2171-01
E-mail: kontakt@bayernlb.de

Your contact

Bayerische Landesbank
Brienner Straße 18
80333 Munich, Germany
www.bayernlb.de

Data Protection Officer
Tel: +49 89 2171-01
Datenschutz.BayernLB@bayernlb.de