

Privacy Statement for Employees of ING-DiBa AG

We protect your personal
data

This Privacy Policy applies as of May 25, 2018
for all employees of ING-DiBa AG.

Table of contents

- 1** Foreword
- 2** To whom does this Privacy Policy apply?
- 3** Which data do we use as an employer – and where does it come from?
- 4** Sensitive data
- 5** What do we use your data for – and on what legal basis?
- 6** Who gets your data – and why?
- 7** Is data transferred to third countries or to international organizations?
- 8** How long do we store your data?
- 9** Your rights are important to us
- 10** What we need your data for
- 11** To what extent do automated individual case decisions or profiling measures take place?
- 12** How we protect your personal data
- 13** Changes to this Privacy Policy

1.

Foreword

Whether you are an employee, job applicant, trainee, or (former) employee: We, ING-DiBa AG ("ING Germany" or "Bank"), respect and protect your privacy. What does this mean for your personal data?

You will receive an overview of how we process your personal data – and your rights under data protection law. Which data we process in detail and how we use it depends on the components of your employment relationship (including the precontractual phase with us) as well as any additional employment benefits. Therefore, not all parts of this document will necessarily apply to you.

Who are we?

We, ING Deutschland, are a German credit institution based in Frankfurt am Main.

We are part of the Dutch ING Group, which operates through our parent company, ING Bank N.V., as an international financial services provider focused on the European market.

As the controller of the data, we, the

ING-DiBa AG
Theodor-Heuss-Allee 2
D-60486 Frankfurt am Main

undertake all measures required by law to protect your personal data.

If you have any questions about this privacy statement, please contact our data protection officer:

ING-DiBa AG
Data Protection Officer
Theodor-Heuss-Allee 2
D-60486 Frankfurt am Main
E-mail: datenschutz@ing.de

2.

To whom does the Privacy Statement apply?

The Privacy Policy applies to the following persons:

- Employees or workers in full and part-time, temporary and permanent employment relationships
- Retired employees
- Interns

- Trainees
- Job applicants as, well as
- Temporary staff („Zeitarbeitskräfte“)

The processing of personal data means inter alia the 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 data.

3.

Which types of data do we use as an employer – and where does it come from?

We process personal data that we receive or have obtained from our employees or other comparably affected persons (e.g. job applicants) within the scope of their employment relationship. In addition, we process – insofar as this is necessary for the employment relationship – personal data that we obtain from publicly accessible sources (e.g. professional networks on the internet) or which other companies of the ING Group or other third parties (e.g. recruitment agencies) are entitled to transmit. In certain situations, we also collect personal data from other bodies due to legal requirements. This includes tax-relevant information from the relevant tax office, as well as information on periods of incapacity to work from the relevant health insurer.

Among other things, we process the following personal data:

- Personal data, such as first and last name, address, date and place of birth, nationality, ID card/passport number, e-mail address, telephone number, work permit if applicable, personnel number.
- Information about your family situation, e.g. marital status and children
- Religious affiliation
- Health data (if relevant for the employment relationship, e.g. in case of severe disability)
- Authentication data (e.g. ID card data)
- Tax identification number
- Social insurance number
- Pension insurance number
- Bank details
- Data from pay receipts
- Information on professional qualifications and continuous training (e.g. curriculum vitae, certificates, etc.)

- Previous employers
- Emergency contacts
- Other data that you voluntarily and proactively share with us, such as information about your interests, hobbies, and memberships.

This data may also include data we receive from the performance of our contractual obligations (e.g. salary payments), such as:

- Log data generated during the use of the IT systems
- Order data (e.g. from the application for a teleworking station)
- Information about the financial situation of an employee (e.g. credit liabilities, salary garnishments)
- Data from the employment relationship (e.g. time recording data, vacation periods, periods of incapacity to work, skill data, social data, activity-related performance data)
- Other data comparable to the above categories.

4.

Sensitive data

Certain personal data, such as information on religious affiliation or degree of disability are considered as "sensitive data".

We process this data exclusively:

- Within the scope of employment
- To exercise rights or fulfill legal obligations arising from labor law, social insurance law and social protection law (e.g. health information to the health insurance company, recording of severe disability due to additional leave and determination of severe disability levy).
- To assess an employee's ability to work, if necessary.

In addition, the processing of sensitive data may be based on your consent (e.g. operational health management).

5.

Wha do we use your data for – and on what legal basis?

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

5.1

We use your data to fulfill the contractual obligations arising from the employment relationship between you and us.

The data are processed to:

- Establish the employment relationship
- Implement or terminate the employment relationship within the framework of the existing contract
- Implement pre-contractual measures, which are carried out upon request

For additional services, such as childcare, we process your data if necessary, to provide the additional services. What else do we use your data for? So that you have access to the building, can use work equipment, such as terminals and applications, receive a salary slip, and to ensure that everything runs smoothly in the job application process.

5.2.

We use your data within the framework of the legitimate interest

To the extent necessary, we process your data beyond the actual performance of the contract with you. We do this to protect our legitimate interests or those of third parties. Here are some examples:

- Measures for personnel development planning
- Measures in the event of organizational changes
- Assertion of legal claims and defense in legal disputes
- Securing our IT security and our IT operations, e.g. to protect the company's data from unauthorized access (data loss prevention measures)
- Prevention and investigation of criminal acts or serious breaches of duty (cf. also Section 26 (1) BDSG)
- Video surveillance for safeguarding house rights, collecting evidence in the event of robberies and fraud (cf. also Section 4 BDSG)

- Recording of customer conversations for processing customer complaints, clarifying misunderstandings about the content of a telephone call made, e.g. for training purposes or to meet banking supervisory requirements
- Measures for building and plant security (e.g. access controls)
- Measures to ensure the right of domicile
- Provision of certain services and offers (e.g. booking of sports courses)

5.3.

We use your data with your consent

Insofar as you have consented to the processing of personal data for certain purposes (e.g. extended storage of application documents, photographs as well as video recordings in the context of events or advertising measures of the bank, newsletter dispatch), the processing of data on the basis of this consent is lawful. You may withdraw any consent given at any time. This also applies to declarations of consent that you gave to us prior to the validity of the GDPR, i.e. prior to May 25, 2018. The withdrawal of consent only takes effect for the future. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

5.4.

We process your data based on legal requirements or for the public interest

As a bank, we are subject to various legal obligations. This means that we have to comply with legal requirements (e.g. from social insurance, working hours and occupational safety laws, from employment protection, banking, money laundering and securities trading laws, and from tax laws).

It also means that we are bound by legal requirements of banking supervision (e.g. the European Central Bank, the European Banking Authority, the German Bundesbank and the German Federal Financial Supervisory Authority). In this context, we therefore process data, among other things, for identity verification, for fraud and money laundering prevention, for the fulfillment of social insurance and tax law monitoring, reporting or documentation obligations, and for the management of risks at the bank and in the ING Group.

5.5.

We process your data on the basis of

collective agreements under German labor law We also process your data to ensure that the Works Council can exercise its rights and fulfill its obligations (e.g. for a company agreement such as the one on the introduction and use of camera surveillance). The

rights and obligations arise from a collective agreement or a works agreement (collective bargaining agreement). We also process your data if this is covered by a relevant collective agreement under labour law.

5.6.

We process your data to protect the vital interests of the data subjects or other natural persons

It may be necessary to process personal data to protect your vital interests, for example in a medical emergency.

6.

Who gets your data – and why?

6.1.

Your personal data within ING Germany

Within the bank, your data can only be accessed by those who need the data to fulfill our contractual and legal obligations. These include, for example, supervisors, the Human Resources department, the Works Council and the representative for severely disabled employees.

6.2.

Your personal data outside ING Germany

Service providers and vicarious agents hired by us may also receive your data within the scope of fulfilling the contractual relationship.

These may include companies for payroll accounting, pension calculation, tax consulting, insurance, training providers, management of the company sports program, IT services, logistics, printing services, company health management services and telecommunications.

As an employer, we only pass on the necessary personal data to recipients outside the bank in compliance with data protection regulations. We only disclose information about our employees under certain conditions: if required by law, if the employee has consented, or if we are otherwise authorized to disclose the information. Recipients of personal data may include:

- Social insurance agencies
- Health insurance companies
- Pension funds
- Tax authorities

- Professional associations
- Public bodies and institutions if a legal or regulatory obligation exists (e.g. European Central Bank, European Banking Authority, Deutsche Bundesbank, German Federal Financial Supervisory Authority, financial authorities, law enforcement agencies)
- Other credit and financial service institutions or comparable institutions to which we transmit personal data for the purpose of implementing the contractual relationship (e.g. for salary payments)
- Business and payroll tax auditors
- Service providers that we use in the context of order processing relationships
- Third-party debtors in the case of wage and salary garnishments
- Insolvency administrators in the event of personal insolvency

We transmit your data to certain bodies if you have given us your consent to do so, or if we are authorized to transfer personal data due to a balancing of interests.

6.3.

Your personal data within ING Group

Within the scope of the employment relationship, we forward in particular the following personal data to ING Bank N.V. :

- Name
- Job title
- Organizational assignment
- Head of the organizational unit
- Phone number
- Mobile phone number
- E-mail address
- Corporate Key
- Cost center
- Location
- ID number
- Status (internal/external)

This data is also published on the worldwide intranet of the companies that belong to the ING Group.

We ensure that when transferring personal data to companies within the ING Group, data protection is guaranteed, and your personal data is protected.

Very important: Under no circumstances do we sell personal data to third parties.

7.

Is data transferred to third countries or to international organizations?

Yes, this can happen.

We transfer data to bodies in countries outside the European Union and the European Economic Area (so-called third countries) if:

- It is required by law (e.g. due to reporting obligations under tax law),
- You have given us your consent, or
- It is legitimized by the legitimate interest of the bank in terms of data protection law and there are no higher interests worthy of protection on your part that conflict with this.

We also transfer personal data to entities in third countries in these individual cases:

- We have your consent
- Statutory regulations to combat money laundering, terrorist financing and other criminal acts take effect
- Within the framework of a balancing of interests (legitimate interest)

Of course, we comply with the data protection level of the European Union.

If we transfer personal data to service providers or group companies outside the European Economic Area (EEA), we will only do so if the EU Commission has confirmed that the third country has an adequate level of data protection – or if other appropriate data protection guarantees (e.g. binding corporate data protection rules as defined in Regulation (EU) 2016/679 (so-called Binding Corporate Rules) or EU standard contractual clauses) are in place. You can also request detailed information on this and on the level of data protection at our service providers in third countries from our data protection officer.

8.

How long do we store your data?

We process and store your personal data for as long as it is required for the fulfillment of our contractual and legal obligations.

The employment relationship is a so-called continuing obligation, i.e. it is designed for an extended period. For the storage of your data this means:

As soon as the data is no longer required for the fulfillment of contractual or legal obligations, we regularly delete the data. Unless – for a limited period – further processing of the data is necessary for the following purposes:

- **Compliance with legal record keeping requirements**

These obligations may arise, for example, from the German Social Code (SGB IV), the German Working Hours Act (ArbZG), the German Works Constitution Act (BetrVfG), the German Remuneration Transparency Act, the German Commercial Code (HGB), the German Banking Act (KWG), the German Money Laundering Act (GwG), the German Securities Trading Act (WpHG) and the German Fiscal Code (AO). The periods specified there for storage or documentation are generally six to ten years.

- **Preservation of evidence according to statutory limitation provisions**

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 3 years.

If we process personal data in our legitimate interest or that of a third party, we delete the data as soon as this interest no longer exists. The aforementioned exceptions also apply here.

The same applies to data that we process on the basis of your consent. As soon as you revoke this consent for the future, we delete the personal data. Unless one of the aforementioned exceptions applies.

9.

Your rights are important to us

We want to respond to all your questions as soon as possible. However, sometimes it can still take up to a month before you get an answer from us. If we need more than one month for a final clarification, we will of course let you know beforehand how long it will take. In some cases, we cannot or may not provide information. If permitted by law, we will always inform you in a timely manner of the reason for the refusal in each case. What rights do you have as an affected person when it comes to the processing of your data?

Your right of access

You are entitled to request from us an overview of your personal data that we process. For example, you can obtain a copy of the personal data we stored which concerns you.

Your right to rectification

If your information is not (or is no longer) correct, you can request a correction/update. If your data is incomplete, you can request that it be amended. If we have disclosed your information to third parties, we will inform these third parties about any corrections – if required by law.

Your right to deletion

You may request the immediate deletion of your personal data for the following reasons:

- If your personal data is no longer needed for the purposes for which it was collected
- If you revoke your consent and there is no other legal basis
- If you object to processing by providing conclusive justification and there are no overriding legitimate grounds for processing
- If your personal data have been processed unlawfully
- If your personal data must be deleted to comply with legal requirements.

Your right to restrict processing

You have the right to request a restriction of the processing of your personal data for one of the following reasons:

- If the accuracy of your personal data is disputed by you and we have had the opportunity to verify its accuracy

- If the processing is not lawful and you request restriction instead of deletion
- If we no longer need your data for the purposes of processing, but you need it to assert, exercise or defend against legal claims
- If you have filed an objection, as long as it has not yet been determined whether your interests prevail

Your right to data portability

You have the right to receive a copy of the data that concerns you in a structured and commonly used transferable format and to forward this data to other organizations. You also have the right to request us to transfer your personal data directly to other organizations you have named. We will transfer your personal data to the extent technically possible and permitted by relevant national legislation.

Your right to object

If we process your data only based on legitimate interests or in the public interest, you have the right to object to the processing of your data in the event of an exceptional situation. If we use your data for direct marketing or advertising activities, you may object to the processing without giving a reason. However, you cannot ask us to delete your personal data if

- We are still legally obligated to store it
- Its storage is necessary for the fulfillment of a contract with you

Please refer to our separate note in the section "Information about your right to object".

Your right of appeal

In individual cases, you may not be satisfied with our response to your request. In this case, you are entitled to file a complaint with ING's data protection officer and with the competent data protection supervisory authority.

You may assert these above-mentioned rights through your colleagues at the Service Point Personal (servicepoint-personal@ing-diba.de).

You can withdraw your consent to the processing of personal data at any time. The withdrawal only takes effect from that point on. It therefore does not affect any processing that took place before the revocation.

10.

What we need your data for

As part of our employment relationship, we require the following personal data:

- Data needed for the commencement, implementation and termination of the employment relationship
- Data required for the fulfillment of the related contractual obligations
- Data that we are obliged to collect by law or on the basis of a collective agreement

Without this data, we are usually not able to conclude, fulfill and terminate a contract with you.

In some cases, you may suffer disadvantages if you do not provide certain personal data. In the case of a severe disability, for example, you will not be able to use facilitating work equipment, or if you are childless, you will not be able to make an additional contribution to long-term care insurance.

Without the necessary information and documentation from you, we may not be able to start an employment relationship at all. Or we may not be able to maintain it.

11.

To what extent do automated individual case decisions or profiling measures take place?

As a matter of principle, we do not use fully automated decision-making to establish, implement and terminate an employment relationship. If we do use this procedure in individual cases, we will inform you about it and about your rights in this regard, insofar as required by law.

12.

How we protect your personal data

We take appropriate technical and organizational measures (policies and procedures, IT security, etc.) to ensure the confidentiality and integrity of your personal data and how it is processed. We apply an internal framework of policies and minimum standards

throughout the company to protect your personal data. These policies and standards are regularly updated to reflect current legislation and market developments. In addition, all ING employees are bound by confidentiality agreements and must not disclose your personal data unlawfully or unnecessarily. If you suspect that your personal data has fallen into the wrong hands, you should always contact ING to help us protect your personal data in the long term.

13.

Changes to this Privacy Statement

We may change this Privacy Statement to comply with changes in the law and/or to reflect how our company processes personal data. We will then change the revision date at the bottom of this page accordingly. However, we recommend that you review this statement regularly to stay informed about how we process and protect your personal data.

This version was created in June 2022

Information about your right to object according to Article 21 GDPR

1.

Right to object on a case-by-case basis

You have the right to object to the processing of your personal data on grounds relating to your particular situation. The prerequisite for this is that the data processing is carried out in the public interest or on the basis of a balancing of interests. This also applies to profiling.

In the event of an objection, we will no longer process your personal data, unless we can demonstrate compelling legitimate grounds to process such data that override your interests, rights and freedoms, or if your personal data is used for the assertion, exercise or defense of legal claims.

2.

Objection to the processing of your data for our direct marketing purposes

Important: We do not use your personal data for direct marketing purposes.

Where to send your objection

There is no special form for an objection – use the subject line "Objection", then provide your name, address as well as your date of birth in the message. Send it to:

ING-DiBa AG
Data Protection Officer
Theodor-Heuss-Allee 2
D-60486 Frankfurt am Main
E-mail: datenschutz@ing.de