

Privacy policy for employees of ING-DiBa AG

Because we protect your personal data

This privacy policy has applied to all employees of ING-DiBa AG since 25 May 2018.

1. Introduction

Whether you are an employee, applicant, trainee, intern or former employee, we, ING-DiBa AG ("ING Germany" or the "Bank"), respect and protect your privacy. In practice, what does that mean for your personal data?

We will explain in the following. This privacy policy provides an overview of how we process your personal data and your rights under data protection law. The specific data we process and how we use it depends largely on the specifics of your employment relationship as per the employment contract between you and the Bank, and also on any additional benefits we provide to you. Therefore, some parts of this policy may not apply to you.

Who we are

We, ING Germany, are a German bank based in Frankfurt am Main.

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

As the controller, we,

ING-DiBa AG

Theodor-Heuss-Allee 2 60486 Frankfurt am Main, Germany, take all legally required measures to protect your personal data.

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

ING-DiBa AG

Data protection officer,

Theodor-Heuss-Allee 2

60486 Frankfurt am Main

Germany

E-mail: datenschutz@ing.de

2. To whom does this privacy statement apply?

This privacy statement applies to the following persons:

- Full-time and part-time employees as well as employees in fixed-term and in permanent employment relationships
- Retired employees
- Interns
- Vocational trainees
- Job applicants, and
- Temporary staff

Processing personal data refers to actions such as collecting, storing, using, transmitting and deleting personal data.

3. What kind of data do we, as an employer, use and where do they come from?

We process personal data that we receive or obtain from our employees or other comparable data subjects (e.g., applicants) in the course of our employment relationship. In addition, to the extent required for the employment relationship, we process personal data that we obtain from publicly accessible sources (e.g., professional networks on the Internet) or that other ING Group companies or other third parties (e.g. recruitment agencies) have lawfully provided to us. In certain situations, we also collect personal data from other agencies as prescribed by law. This includes tax-relevant information from the competent tax office and information regarding periods of incapacity for work from the relevant health insurer.

We process, for example, the following personal data:

- Personal details, such as salutation, title, first and last name, address, date and place of birth, nationality, photograph, identity document/passport number, e-mail address, telephone number, job, work permit if applicable, employee number
- Information about your family situation, e.g., marital status, details of your children

- Religious affiliation
- Health data (if relevant to the employment relationship, e.g., in the case of severe disability)
- Identification data (e.g., identity document data, signature)
- Tax identification number
- Social security number
- Pension insurance number
- Banking details
- Securities account number and holder
- Extract from the German Federal Central Register at the Federal Office of Justice
- Payroll data
- Information on professional qualifications and continuing professional development (e.g., CV, job references, training certificates, etc.)
- Former employers
- Data on the use of services (video chats, internal user ID, user name, language skills, video, audio, screen and chat recordings and transcripts of spoken language)
- Emergency contacts
- Other data that you voluntarily and proactively share with us, such as information about your interests, hobbies and memberships

These data may also include data that we receive by virtue of fulfilling our contractual obligations (e.g., salary payments), such as:

- Log data created during the use of IT systems
- Order data (e.g., from the application for remote working equipment)
- Information about the financial situation of an employee (e.g., loan liabilities, attachment of earnings)
- Data from the employment relationship (e.g., start and end dates, organizational affiliation, department, position, direct and indirect managers, pay scale group, time tracking data, vacation periods, periods of incapacity to work, skill data, social data, work-related performance data)
- Data comparable to the above categories

4. How do we handle sensitive data?

Certain types of personal data, e.g., regarding religious affiliation or the degree of a severe disability, are considered to be "sensitive data". We only process these types of data for the following purposes:

- Within the scope of the employment relationship
- For the purpose of exercising rights or fulfilling legal obligations under employment law, social security law and social protection (e.g., disclosing health information to health insurers, recording severe disability for the additional leave entitlements and determining disability contributions)

- To assess an employee's capacity for work, if necessary
- In addition, sensitive data may be processed with your consent (e.g., in connection with occupational health management).

5. What 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 for these purposes:

- Entry into the employment relationship
- Performance or termination of the employment relationship under the current contract
- Performance of pre-contractual measures upon request

This also includes processing personal data from the career profiles you voluntarily maintain in our HR systems.

For additional benefits such as childcare, we process your data as necessary to provide the additional services.

What else do we use your data for? To ensure you have access to the building, can use work equipment such as devices and applications, receive a payslip (this also includes the use of real data for testing purposes to update the payroll system) and to ensure that everything runs smoothly during the recruitment process.

5.2. We use your data for the balancing of interests

Your individual needs and requirements are important to us, and we always try to balance your interests with our own.

When necessary, we will process your data even after your employment with us has ended. We do this to safeguard our own legitimate interests or those of third parties. To give you a few examples:

- Measures to plan personnel development
- Conducting employee surveys
- Measures in connection with organizational changes
- Assertion of legal claims and defense in legal disputes

- Safeguarding of our IT security and IT operations, e.g., to protect company data from unauthorized access (data loss prevention measures)
- Prevention and investigation of criminal offenses or serious breaches of duty (see also section 26, (1) BDSG)
- Video surveillance to safeguard our right to exclude trespassers and to secure evidence in the event of robbery and fraud (see also section 4 BDSG)
- Recording of telephone conversations with customers to process customer complaints, to clarify misunderstandings as to the content of a telephone conversation, for training purposes and to meet banking supervisory requirements
- Measures to ensure building and technical security (e.g., access controls)
- Measures to safeguard our rights as the occupier of the premises
- Measures to ensure the appropriateness of remuneration
- Provision of specific services and offers (e.g., booking sports courses)
- Fitness and propriety screening (regular quarterly screening of employee data against sanctions, terrorist, extremist or similar lists)
- Measures to optimize the use of paid software licenses
- Transcriptions of spoken language (e.g., in MS Teams)

5.3. We use your data with your consent

If you have consented to the processing of personal data for specific purposes (e.g., extended storage of application documents, photographs and video recordings in the context of the Bank's events or marketing activities, newsletter distribution, personnel development initiatives), the processing of data on the basis of this consent is lawful.

You can withdraw your consent at any time. This also applies to consent that you gave us before the GDPR entered into force, i.e. before May 25, 2018.

Any such withdrawal of consent only takes effect for the future. It does not affect the lawfulness of any data processing that took place prior to the withdrawal of consent.

5.4. We process your data on the basis of legal requirements or in the public interest

As a bank, we are subject to various legal obligations. This means that we have to fulfill statutory requirements (e.g., relating to social security law, legislation on working hours and occupational health and safety, the German Dismissal Protection Act (KSchG), the German Banking Act (KWG), the German Money Laundering Act (GwG), the German Securities Trading Act (WpHG) and tax legislation). This also means that we are bound by the legal requirements of banking supervision (e.g., by the European Central Bank, the European Banking Authority, the Deutsche

Bundesbank and the Federal Financial Supervisory Authority (BaFin)). For this reason, we also process data for purposes such as identity checks, to prevent fraud and money laundering, to screen job applicants for fitness and propriety, to meet our monitoring, reporting and documentation obligations under social security and tax law, and to manage risks at our Bank and within the ING Group.

5.5. We process your data on the basis of collective agreements under labor law

We also process your data to ensure that your employee representatives can exercise their rights and meet their obligations (e.g., in connection with a works agreement governing the introduction and use of video surveillance). These rights and obligations arise from a collective bargaining agreement or a works agreement (collective agreement).

5.6. We process your data to protect the vital interests of 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 receives your data and why?

6.1. Your personal data within ING Germany

Within the Bank, your data can only be accessed by those persons who need it to meet our contractual and legal obligations. These include, for example, line managers, HR, the works council and the representative body for employees with severe disabilities.

6.2. Your personal data outside of ING Germany

Service providers and contractors engaged by us may also receive your data in the course of fulfilling their contractual duties. These may be companies in the categories of payroll accounting, pension calculation, tax consulting, insurance, training providers, management of company sports initiatives, IT services, logistics, printing services, occupational health management services and telecommunications.

In our capacity as an employer, we only disclose personal data to recipients outside the Bank on a need-to-know basis, and only in compliance with data protection rules. As a rule, we may only disclose information about our employees under certain circumstances: if this is required by law, if the relevant employee has consented to this or if we are, for other reasons, entitled to pass on this information. In such cases, personal data may be passed on to:

- Social security institutions
- Health insurers

- Pension schemes
- Tax authorities
- Professional associations
- Public authorities and institutions (e.g., the European Central Bank, European Banking Authority, Deutsche Bundesbank, Federal Financial Supervisory Authority (BaFin), tax authorities, law enforcement), if there is a statutory or regulatory requirement
- Other banks and financial services institutions or similar organizations to which we transfer personal data for the purpose of performing a contract (e.g., for salary payments)
- Chartered accountants and wage tax auditors
- Service providers for reviewing the appropriateness of remuneration
- Service providers we engage as processors in connection with data processing
- Third-party debtors in cases of wage or salary attachments
- Insolvency administrators in cases of private bankruptcy
- ING Bank N.V. as data controller for Group-wide reporting

We transfer your data to specific bodies if you have given us your consent to do so or if we are authorized to transfer personal data based on a balancing of interests.

6.3. Your personal data within the ING Group

In connection with your employment, we will in particular transmit the following personal data to ING Bank N.V.:

- First name
- Last name
- Date of birth
- Job title
- Organizational assignment
- Head of organizational unit
- Telephone number
- Mobile number
- E-mail address
- Corporate key
- Cost center
- Location
- ID number
- Status (internal/external)

These data will also be published on the worldwide intranet of the companies of the ING Group.

In addition, personal data will be processed as part of HR development activities within the ING Group, provided you have given your consent to participate in these processes. This includes in particular information relating to career development, qualifications and other relevant data.

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

Most importantly, under no circumstances do we sell personal data to third parties.

7. Will data be transmitted to a third country or an international organization?

Yes, that can happen.

We transmit data to recipients in countries outside the European Union and the European Economic Area (third countries) to the extent that

- It is required by law (e.g., due to tax reporting requirements)
- You have given us your consent
- Or it is in the Bank's legitimate interest and therefore permissible under data protection law, and your own protectable interests do not preclude this.

In addition, we also transmit personal data to recipients in third countries in the following individual cases:

- If you have given us your consent
- Statutory provisions need to be enforced for combating money laundering, terrorist financing and other criminal acts
- As part of the balancing of interests

In any of these cases, we will, of course, adhere to the data protection standards that apply within the European Union.

We only transfer personal data to service providers or Group companies outside the European Economic Area (EEA) if the European Commission has confirmed that the third country has an adequate level of data protection, or other appropriate data protection guarantees are in place (e.g., "binding corporate rules" as defined in Regulation (EU) 2016/679 or EU standard contractual clauses). Please contact our data protection officer for more detailed information on these requirements and the data protection standards at our service providers in third countries.

8. For how long do we store your data?

We process and store your personal data for as long as necessary to fulfill our obligations under the employment contract and our legal obligations.

The employment relationship is a continuing obligation, as it is geared towards a longer period. In terms of storing your data, this means that we delete

data on a regular basis as soon as they are no longer required for the fulfillment of contractual or legal obligations. Exceptions may be made if it is deemed necessary to further process the data for a limited period of time for the following purposes:

- **Compliance with statutory retention requirements**
These requirements may arise, for example, from Book Four of the German Social Security Code (SGB IV), the German Working Hours Act (ArbZG), the German Works Constitution Act (BetrVfG), the German Remuneration Transparency Act (EntgTranspG), 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). These laws generally stipulate retention or documentation periods from six to ten years.
- **Preservation of evidence in accordance with statutes of limitation**
In accordance with sections 195 *et seq.* of the German Civil Code (*Bürgerliches Gesetzbuch*, "BGB"), such periods may be up to 30 years, with the general statute of limitation being three years.
- **Transcription of spoken language**
Transcriptions of spoken language (e.g., in MS Teams) are stored for 90 days.

Whenever we process personal data in our own legitimate interest or that of third parties, we delete these data once such interest no longer exists. The above exceptions also apply in those cases. The same applies to the data that we process on the basis of your consent. As soon as you withdraw this consent for the future, we delete your personal data unless one of the exceptions referred to applies.

9. Your rights are important to us

We will respond to all your questions as quickly as possible. However, sometimes it may take up to a month before you receive a response from us. If we need more than a month to provide a final answer, we will of course let you know in advance how much longer it will take. However, in some cases we cannot or must not provide any information. In such cases, we will always let you know the reason for the refusal as soon as possible, provided this is legally permissible. What rights do you have as a data subject in terms of the processing of your data?

Your right of access

You have the right to request an overview of any personal data concerning you that we process. For

example, you can receive a copy of the personal data that we store about you.

Your right to rectification

If the information you have provided is no longer accurate, you can request that it be corrected. If your data are incomplete, you can request that they be completed. If we have passed on your details to third parties, we will inform these third parties of your correction, to the extent this is required by law.

Your right to erasure

You can request the erasure of your personal data without undue delay for the following reasons:

- When your personal data are no longer needed for the purposes for which they were collected
- If you withdraw your consent and there is no other legal basis
- If you object to the processing on reasonable grounds and there are no overriding legitimate grounds for the processing
- If your personal data have been unlawfully processed
- If your personal data have to be erased for compliance with a legal obligation

Your right to restriction of processing

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

- If you contest the accuracy of your personal data and we have had the opportunity to verify their accuracy
- If the processing is not lawful and you request a restriction on use instead of erasure
- If we no longer need your data for the purposes of processing, but you need them for the establishment, exercise or defense of legal claims
- If you have filed an objection, pending the verification of whether your interests override ours

Your right to data portability

You have the right to receive a copy of any data concerning you in a structured, commonly used and machine-readable format and to transmit those data to other organizations. You also have the right to request that we transmit your personal data directly to other organizations you have named. We transmit your personal data where technically feasible and where permitted by relevant national law.

Your right to object

If we process your data based solely on legitimate interests or in the public interest, you have the right to object to the processing of your data in a particular situation. If we use your data for direct marketing or advertising activities, you can object to the processing

without providing a reason. However, you cannot request that we delete your personal data if:

- We are still legally required to store them
- The data are necessary for the performance of a contract with you

Please refer to the separate notice at the end of this privacy policy in the section "Information about your right to object".

Your right to lodge a complaint

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

You can assert these by contacting Servicepoint Personal (servicepoint.personal@ing-diba.de).

You can withdraw your consent to the processing of your personal data at any time. This also applies to withdrawing any consent you gave us before the GDPR came into force on May 25, 2018. Withdrawal of consent is only effective for the future. It therefore does not apply to any processing that took place before withdrawal.

10. What we need your data for

In connection with your employment, we require the following personal data:

- Data required for the commencement, performance or termination of the employment relationship
- Data needed to meet the associated contractual obligations
- Data that we are required to collect by law or under a collective agreement

Without these data, we are generally unable to enter into, perform or terminate a contract with you.

In some cases, you might be disadvantaged if you do not provide certain personal data. For example, in the case of a severe disability there may be a lack of special work equipment, or it may be that no additional contribution is made to your long-term care insurance if you have no children.

In fact, without the necessary information and documents from you, it is possible that no employment relationship can be entered into at all. Or we may not be able to maintain your employment.

11. To what extent do we use automated case-by-case

decision-making processes or profiling?

As a matter of principle, we do not use fully automated decision-making to enter into, perform or terminate an employment relationship. Should we use this procedure in individual cases, we would inform you accordingly, including of any rights you may have in this regard, to the extent required by law.

Information on your right to object under 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 personal situation. This requires that the data processing is carried out in the public interest or on the basis of a balancing of interests. The same applies to profiling.

If you object, we cease to process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms. This also applies if your personal data serve for the establishment, exercise or defense of legal claims.

2. Objection to the processing of your data for our direct marketing

Please note: We do not use your personal data for direct marketing.

Addressee of objection

Your objection can be made without observing any formal requirements – simply write "Objection" in the subject line and include your name, address and date of birth in the text. Send your objection to:

ING-DiBa AG
Data protection officer
Theodor-Heuss-Allee 2
60486 Frankfurt am Main
Germany
E-mail: datenschutz@ing.de

12. How we protect your personal data

We use appropriate technical and organizational measures (guidelines and procedures, IT security, etc.) to ensure the confidentiality and integrity of your personal data and their processing. We apply an

internal framework of policies and minimum standards across the organization 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 subject to a duty of confidentiality and may not disclose your personal data unlawfully or unnecessarily. If you suspect that your personal data have fallen into the wrong hands, you should always contact ING to help us ensure that your personal data are permanently protected.

13. Changes to this privacy policy

We may amend this privacy policy to reflect changes in the law and/or how our company processes personal data. We will then change the revision date on the first page accordingly. However, we recommend that you regularly review this policy to stay up-to-date with how we process and protect your personal data.