

Privacy Statement
ING Bank, a branch of ING-DiBa AG

Contents

- 1. About this Privacy Statement 3
- 2. The types of data we collect 3
- 3. What we do with your personal data 4
- 4. Who we share your data with and why 4
- 5. Your rights and how we respect them..... 6
- 6. Your duty to provide data..... 8
- 7. How we protect your personal data..... 8
- 8. What you can do to help us keep your data safe..... 8
- 9. How long we keep your personal data 9
- 10. Scope of this Privacy Statement 9
- 11. Contact information 9

1. About this Privacy Statement

This Privacy Statement aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following people:

- Anyone involved in any transaction with ING Bank as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, etc.).
- Non-ING Bank customers such as payees or the contact persons of corporate clients.

Personal data refers to any information that tells us something about you or that we can link to you. This includes your name, address, date of birth, account number, IP address or information about payments made from a bank account. By processing we mean everything we can do with this data such as collecting it, recording, storing, adjusting, organising, using, disclosing, transferring or deleting.

You share personal information with us when you or your company become a customer, register with our online services, complete an online form, sign a contract, use our products and services or contact us through one of our channels.

We also use data that is legally available from public sources such as debtor registers, commercial registers, registers of association and the media, or is legitimately provided by other companies within the ING Group or third parties such as credit agencies.

2. The types of data we collect

The personal data we collect includes:

- **Identification data**, such as your name, surname, date and place of birth, ID number, signature, (company) email address, (company) phone number and the IP address of your PC or mobile device
- **Transaction data**, such as bank account number and transfers related to the account
- **Financial data**, such as invoices, credit notes, and credit history
- **Tax data**, such as personal tax identification number, tax residency and tax allocation
- **Trade-related data**, such as trader names and counterparty traders

Sensitive data

We are legally obliged to keep a copy of your ID card or passport. In individual cases – depending on the country of issuance – this may reveal sensitive data relating to your ethnicity, religious or political beliefs.

3. What we do with your personal data

We only use your personal data for legitimate business reasons. This includes:

- **Administration.** When we enter into a client relationship, we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport). We also need to know your address or phone number to contact you.
- **Service provision.** To provide the services specified in our contractual relationship, we may have to process your personal data, such as your name on a transaction or signature on an agreement.
- **Managing customer relationships.** We may ask you for feedback about our products and services and we might also use notes from conversations we have with you online, by telephone or in person for the customisation of products and services.
- **Preventing and detecting fraudulent/illegal activities:** We may use your personal data in order to comply with different regulations (e.g. against money laundering, terrorism financing and tax fraud).
- **Internal and external reporting:** We process your data for our banking operations and to help our management make better decisions about our operations and services.

In case that a link to a specific person is not necessary for the intended purpose, data is anonymised or we remove as much of the personal information as possible.

4. Who we share your data with and why

To be able to offer you the best possible services and remain competitive in our business, we share certain data internally and outside of ING Bank. This includes:

ING entities

In accordance with legal requirements, we transfer data across ING businesses and branches for operational, regulatory or reporting purposes, for example to screen new customers, comply with certain laws, secure IT systems or provide defined services. (See section 'What we do with your personal data' for the full list). We may also transfer data to centralised storage systems or to process it globally for more efficiency. To ensure an adequate level of protection, ING-DiBa and ING Group have adopted Binding Corporate Rules (BCR) within the meaning of the EU General Data Protection Regulation. These BCR were approved by the Data Protection Authorities in all EU Member States and allow ING Group entities to ensure that personal data exchanged or shared within the Group is protected. When the ING entities are outside the European Economic Area (EEA), we ensure similar personal data protection as in the EEA by usage of the BCR.

Government authorities

To comply with our regulatory obligations we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering. In some cases, we are **obliged by law** to share your data with external parties, including:

- **Regulators and supervisory bodies** such as the central banks of the countries where we operate.
- **Tax authorities** may require us to report assets.
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.
- **Lawyers**, for example, in case of bankruptcy, **trustees** who take care of other parties' interests, and **company auditors**.

Financial institutions

Other banks or specialized financial companies are involved in the execution of transactions on a regular basis.

We also share information with financial sector specialists who assist us with financial services like:

- exchanging secure financial transaction messages
- payments and credit transactions worldwide
- processing electronic transactions worldwide
- settling domestic and cross-border security transactions and payment transactions

Sometimes we share information with banks or financial institutions in other countries, for example in case of a foreign payment. And in specific cases we share information

with business partners such as insurance companies, for instance if we sell their financial products.

Service providers

When we use other service providers we only share personal data that is required for a particular assignment. Service providers support us with activities like:

- performing certain services and operations
- designing and maintenance of internet-based tools and applications;
- marketing activities or events
- preparing reports and statistics, printing materials and designing products.

In all of these cases, we ensure the third parties can only access personal data that is necessary for their specific tasks.

Whenever we share your personal data internally or with third parties in other countries, we ensure the necessary safeguards are in place to protect it. For this, ING Bank relies on:

- Binding Corporate Rules as defined in EC Regulation (EU) 2016/679. These are known as the ING Global Data Protection Policy (GDPP) and have been approved by the data protection authorities in all EU member states.
- [EU Model clauses](#), which are standardised contractual clauses used in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with EU data protection law.
- [Privacy Shield](#) framework that protects personal data transferred to the United States.

5. Your rights and how we respect them

We respect your rights as a data subject to determine how your personal information is used. These rights include:

Right to access information

You have the right to ask us for an overview of your personal data that we process.

Right to rectification

If your personal data is incorrect, you have the right ask us to rectify it. If we shared data about you with a third party that is later corrected, we will also notify that party.

Right to object to processing

You can object to ING Bank using your personal data for its own legitimate interests. We will consider your objection and whether processing your information has any undue impact on you that requires us to stop doing so.

You cannot object to us processing your personal data if we are legally required to do so; if it is necessary to fulfil a contract with your company; or if there are security issues with the account.

Right to restrict processing

You have the right to ask us to restrict using your personal data if

- you believe the information is inaccurate
- we are processing the data unlawfully
- ING Bank no longer needs the data, but you want us to keep it for use in a legal claim
- you have objected to us processing your data for our own legitimate interests

Right to erasure

You may ask us to erase your personal data if:

- we no longer need it for its original purpose,
- you object to us processing your data for our own legitimate interests
- ING Bank unlawfully processes your personal data, or
- a law of the European Union or a member state of the European Union requires ING Bank to erase your personal data.

Right to complain

Should you not be satisfied with the way we have responded to your concerns you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the ING Data Protection Officer. You can also contact the data protection authority in your country.

Exercising your rights

If you want to exercise your rights or submit a complaint, please contact us. There is a list of contact details at the end of this Privacy Statement.

Your rights can be exercised on different ways. It could be through our website, in person or by telephone. We aim to respond to your request as quickly as possible. In some instances this could take up to one month (if legally allowed). Should we require more time to complete your request, we will let you know how much longer we need and provide reasons for the delay.

In certain cases, we may deny your request. If it's legally permitted, we will let you know in due course why we denied it.

6. Your duty to provide data

There is certain information that we must know about you so that we can commence and execute our duties as a bank and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this data we may not be able to provide our services.

7. How we protect your personal data

We apply an internal framework of policies and minimum standards across all our business to keep your data safe. These policies and standards are periodically updated to keep them up to date with regulations and market developments. More specifically and in accordance with the law, we take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it's processed.

In addition, ING Bank employees are subject to confidentiality and may not disclose your personal data unlawfully or unnecessarily.

8. What you can do to help us keep your data safe

We do our utmost to protect your data, but there are certain things you can do too:

- Install anti-virus software, anti-spyware software and a firewall. Keep them updated.
- Do not leave equipment and tokens (e.g. bank card) unattended.
- Report the loss of a bank card to ING and cancel the lost card immediately.
- Log off from online banking when you are not using it.
- Keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures.
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing emails requesting personal information.

9. How long we keep your personal data

We are only allowed to keep your personal data for as long as it's still necessary for the purpose we initially required it. Furthermore we are required to adhere to legal retention periods.

10. Scope of this Privacy Statement

This is the Privacy Statement of ING Bank, branch of ING DiBa AG. It is applicable to the services provided as part of ING Wholesale Banking.

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created on 16 May 2018. The most recent version is available at ingbank.de.

11. Contact information

Responsible for the processing of your data is:

ING Bank, branch of ING DiBa AG
Hamburger Allee 1
60486 Frankfurt am Main

In case of questions regarding the content of this Privacy Statement and/or an individual right with respect to it you can contact our Data Protection Officer ('DPO'):

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