Privacy Policy in the context of ING Wholesale Banking

1.

Our Privacy Policy: Who are we?

This is the privacy policy of ING Bank, a subsidiary of ING DiBa AG (hereinafter referred to as "ING", "we" or "our"). It applies to the processing of personal data stored in the context of ING Wholesale Banking.

As data controllers, we, the
ING Bank, branch of ING DiBa AG, Hamburger Allee 1
60486 Frankfurt
all measures required by law to protect your personal data.

If you have any questions about this privacy policy, please contact our data protection officer: INGDiBa AG
Data Protection Officer
TheodorHeussAllee 2 60486
Frankfurt am Main Email:
datenschutz@ing.de

We would also like to inform you that ING DiBa AG is a subsidiary of
ING Bank N.V. ING Bank N.V. is a European financial institution that is subject to the data protection regulations of the European General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). To comply with the GDPR, ING Bank N.V. has introduced global data protection principles through its Global Data Protection Guidelines (GDSR). The GDSRs are binding on all ING companies worldwide, i.e. subsidiaries, branches, agencies and branches, and have been approved by the European data protection authorities. Therefore, ING Bank N.V. has decided that all of its global companies, subsidiaries, branches, representative offices and subsidiaries – regardless of their location, target markets or customers – must comply with the GDSR in addition to national data protection laws and regulations.

2.

To whom does this privacy policy apply?

At ING, we understand how important your personal data is to you. This privacy policy explains in a simple and transparent way what personal data we collect, collect, store, use and process and how we do it. Our approach can be summed up as follows: The right people are using the right data for the right purpose.

This Privacy Policy applies to:

- All former, current and potential clients of ING who are natural persons ("you"), including sole proprietorships,
  agents or contact persons acting on behalf of our corporate clients.
- Non-ING customers, such as beneficiaries or payers, recipients, guarantors, beneficial owners,
  Managers and officers, legal representatives, shareholders, debtors or tenants of our clients, visitors to our WholesaleBanking website, auditors, consultants or other persons involved in a transaction.

We receive your personal data in the following ways:

- From your company, if you are a contact person .
- By yourself, when you register for our online services, fill out an online form, sign a contract, use our products and
  Services or contact us through one of our contact channels.
- From other available sources such as debtors land registers, commercial registers,
  Registers of associations, online or traditional media or other publicly available sources or other companies within ING or third parties such as payment or transaction processors, information agencies, other financial institutions, commercial companies or public authorities.

86.489/10.24/3001/03

3.

What personal data do we collect from you?

Personal data is any information that tells us something about you or that we can associate with you. This includes, but is not limited to, your name, address, date of birth, account number, IP address, or information about payments made from a bank account. By "processing" we mean the collection, recording, storage, adaptation, organization, use, disclosure, transfer or deletion.

You share personal information with us, for example, when you sign a contract on behalf of your company 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, association registers and the media, or that is lawfully provided by other companies within the ING Group or third parties such as credit reference agencies.

The personal data we collect includes, but is not limited to:

- **Identification data:** such as first name, last name, date and place of birth, your ID number, Nationality, physical and electronic signatures, address, social security number, (company) email address, (company) telephone number and the IP address of your PC or mobile device.
- **Financial data:** If you give us a guarantee, customer, we can take over your Check credit history, credit capacity, and other information regarding your creditworthiness and credit terms; furthermore, we may process your data from invoices or bonds.
- **Tax data:** personal tax identification tax residency and tax apportionment.
- **Trade-related data:** names of traders and those of the counterparty.
- **Know Our Customer (KYC) data:** Under the Know YourCustomerPrinciple (KYC) refers to the examination of the personal data and business data of new customers of a credit institution for the prevention of money laundering and terrorist financing on the basis of the Money Laundering Act. We process personal data as part of the so-called Customer Due Diligence (CDD). In the case of natural persons, the type of professional activity and the purpose of the business relationship must be recorded in particular. The details of the planned customer relationship, such as the scope of the or payment transaction types must be recorded.
- **Audiovisual data:** If necessary and permitted by law, we process surveillance videos in the respective ING locations, information from the video legitimation procedures, photos of ATM security devices in the event of suspected misuse, recordings of telephone conversations or chats.

As well as other data comparable to these categories.

4.

How do we handle your sensitive data?

Sensitive data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning a natural person's sex life or sexual orientation.

We only process your sensitive data:

- where we have your explicit consent;
- if we are legally obliged or entitled to do so;
- If you choose to use fingerprint recognition for identity verification when accessing mobile apps and when performing certain processes in the apps.

We process your sensitive data, for example, in connection with:

- Know Your Customer (KYC) Regulations: We are required by law to provide a copy of your personnel or your passport. In individual cases – depending on the country of issue – they may collect sensitive data on your ethnic origin or your religious or political beliefs contain.
- Money laundering or terrorist financing monitoring: We monitor your activities and may report them to the relevant regulators. announce.
- Face and fingerprint recognition: If permitted by law and if you choose to do so, we may use your face and fingerprint to Use identity verification when signing in to mobile apps and during certain operations.

5.

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

We will only use your personal information for lawful business purposes.

These include:

- **Execution of contracts to which you are a party or measures within the framework of contract initiation:** If you are acting as a representative of a company
  We may use your personal data to enter into the contract with the corporate client or to contact the corporate client if necessary. If you are a private individual,
  or a beneficiary of payment instruments, we may use your personal data to enter into a contract or execute a payment order in connection with our agreements with the customer. We may also exercise your powers on the basis of commercial registers or legal regulations.
  information on the performance of your duties.
- **Provision of services:** In order to provide the services described in our contract, we may process personal data, such as a
  Names on a wire transfer or a signature on a contractual agreement.
- **Customer management and marketing:** We can help you as a representative of our corporate customer for your opinion
  about our products and services or record your conversations with us – online, by phone or at our locations. We may share this information with certain employees in order to improve our offerings or tailor our products and services to you. We may send you newsletters informing you about these products and services. If you do not want to receive these offers, you can of course object or withdraw your consent.
  revocation.
  - **Provision of the most appropriate products, services:** If you visit our website as a representative of a customer, our
    Call customer service, speak to an ING employee, we may collect information about the customer.
  - **Improvement and development of our products and services:** When we analyse how we
    As you use and interact with our products and services, we can better understand you and where and what we can improve.
- **Execution of business processes, internal Management and ManagementReports:** We process your data for our banking operations and to help our management make better decisions about our operations and services.
- **Security and Protection:** We are committed to protecting your personal information and preventing, detecting, and preventing data breaches
  Curb. Not only do we want to protect you from fraud and cybercrime, but we are also committed to ensuring the security and integrity of ING and the entire financial system by taking action against crimes such as money laundering, terrorist financing and tax fraud.
  - Process your personal data in order to
    Your company's assets from fraud
    Protect your business activities, e.g. in the event that your identity (e.g. username and password) is compromised.
  - We may have certain information about you (e.g. Name, account number, age, nationality
    IP address, etc.) for profiling purposes, to identify fraudulent activities and the offenders.
  - We may use your personal data
    to make you aware of the
    that we detect suspicious activity on your company's account, for example, if a transaction takes place from an atypical location.
- **Compliance with legal obligations:** We process personal data for fulfilment
  a number of legal obligations and requirements (anti-money laundering legislation and tax legislation, etc.). For example, KYC regulations require ING to verify the identity of its customers before accepting you as a customer. At the request of authorities, ING can report the transactions carried out by customers.

If the processing is not compatible with any of the purposes mentioned, we will ask for your explicit consent, which you can refuse or withdraw at any time.

6.

How long do we store your data?

We will retain your personal information throughout our business relationship with you as your company's representative. After the termination of our business relationship with you, we may retain your data as well as legally binding documents issued by the competent authorities, etc., for up to ten years in accordance with the German Commercial Code (HGB), the Federal Tax Code (BAO), the Banking Act (BWG), the Money Laundering Act (AMLA) and the Securities Supervision Act (WAG).

Once your personal data is no longer
are needed for the process or activity for which they were originally collected, we delete or anonymise them and dispose of them in accordance with relevant laws and regulations.

7.

Who we share your information with and why

In order to provide you with the best possible services and to strengthen competitiveness in our industry, we share certain data internally (to other ING companies) and externally (to companies other than ING) to third parties.

If we transfer your personal data externally to third parties (companies other than ING) in countries outside the European Economic Area (EEA), we will ensure that the necessary safeguards have been put in place. To this end, we use the following, among others:

- Requirements based on relevant national laws and regulations;
- **EU standard clauses:** If necessary, we will standardised procedures for agreements with service providers include contractual clauses to ensure that the GDPR is complied with when transferring personal data outside the European Economic Area;

INGGecompanies

In accordance with legal requirements, we transfer data between ING business fields and stores for operational, legal or reporting purposes, for example to screen new customers, comply with laws, secure IT systems or provide certain services. For greater efficiency, we can also transfer data to centralized storage systems or process it worldwide. In order to ensure an appropriate level of security, INGDiBa AG and the ING Group have adopted binding corporate rules (BCR) within the meaning of the EU General Data Protection Regulation. These BCRs have been approved by the data protection authorities in all EU member states. With the help of the BCR, ING Group companies can ensure that personal data exchanged or shared within the group remains protected. If an ING Group company is located outside the European Economic Area (EEA), we guarantee the same protection of your personal data as within the EEA through the group-wide application of our BCRs.

Public bodies, supervisory and judicial authorities

In order to comply with our legal obligations, we may disclose data to the relevant authorities, for example to combat terrorism and prevent money laundering.

In some cases, we are required by law to share your information with, for example:

- **public bodies, supervisory authorities and bodies** such as the national banks and public bodies as well as supervisory authorities of the financial sector of the federal states, in which we operate.
- **Tax authorities** that may require us to provide information on client assets or other personal data Data such as your name, contact details. To do this, we may process your identification data such as your social security number, tax identification number or other national identification marks in accordance with the relevant regulations. national laws.
- **Judicial authorities and similar institutions** such as the police, prosecutors, courts and arbitration/mediation rely on their explicit and lawful Inquiry.

Financial institutions

In order to process certain deposits and withdrawals, we may need to transfer information about the customer or their representative to another bank or specialist financial services company. We also share information with specialists in the financial industry who support us with financial services, such as:

- Exchange of secure messages on financial Operations;
- Payments and transfers worldwide;
- Processing electronic transactions worldwide;
- Handling local and cross-border securities transactions and payment transactions;
- Provision of services by other financial services companies, including Banks, pension funds, stockbrokers, custodian banks, fund managers and portfolio service providers.

Service providers and other third parties

If, in the course of our normal business activities, we engage service providers or other third parties to carry out certain activities, we may need to transfer personal data for certain tasks. Service providers support us in activities such as

- Design, development and maintenance of the internet based tools and applications;
- Provision of application or infrastructure services (e.g. cloud services);
- Marketing activities or events, and Managing communication with customers;
- Preparation of reports and statistics, printing of materials and product design;
- Advertising in apps, websites and social media Media;
- specialist services, including legal and auditing services, by lawyers, notaries, trustees, accountants or other specialist advisers;
- Detecting, detecting, or preventing fraud or other unlawful conduct by special companies such as KSV or CRIF;

- Provision of specialised services such as mailing or file filing by our agents, contractors and external service providers.

Account information and payment initiation service providers within the EU

The revised EU Payments Services Directive (PSD2) allows you to instruct a third-party service provider to retrieve information or initiate payments on your behalf regarding your accounts with the ING account. The third-party provider may only act if you have expressly consented to these services.

If we receive a request from a third-party service provider on your behalf, we are required to process the requested payment or provide the account information.

You can also use the PSD2 services to manage your accounts with other banks through your ING channels or apps. You can use apps or ING's channels,

- to request account information about your current accounts with other banks;
- To make online payments from your current accounts with other banks.

In this case, we act as a third-party service provider and can only provide these services if we have received your explicit consent to do so. If you decide that you no longer want to use these PSD2 services, you can simply deactivate this function in ING's OnlineBanking.

Independent contractors, brokers and business partners

We may share your personal information with our independent contractors, brokers or business partners who act on our behalf or co-operate with us in products and services. These contractors are registered in accordance with national legislation and have proper authorisation from the relevant supervisory authorities.

8.

Why do we care about your rights?

We want to respond to all your questions as quickly as possible. However, sometimes it can take up to a month before you get a response from us – if this is legally permissible. If we need more than a month for a final clarification, we will of course let you know in advance how long it will take.

In some cases, we cannot or may not provide information. If permitted by law, we will always inform you of the reason for the refusal in a timely manner. You have the right to lodge a complaint.

What rights do you have as a data subject when it comes to the processing of your data?

Details can be found in the respective regulations of the General Data Protection Regulation (Articles 15 to 21 GDPR).

Your right to information

You have the right to request an overview of the personal data we process from us. For example, you may receive a copy of the personal data we hold about you.

Your right to rectification

If your information is not (or no longer) accurate, you can request that it be corrected. If your data is incomplete, you can request that it be completed. If we have shared your information with third parties, we will notify those third parties of your correction – where required by law.

Your right to object

We may process your data on the basis of legitimate interests or in the public interest. In these cases, you have the right to object to the processing of your data. This also applies if we use your data for our direct marketing.

However, you cannot ask us to delete your personal data if:

- we are legally obliged to do so;
- this for the performance of a contract with you is required.

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

Your right to restriction of processing

You have the right to request restriction of processing of your personal data on one of the following grounds:

- If the accuracy of your personal data disputed by you and we have the opportunity to to check the accuracy
- If the processing is not lawful and you request restriction of use instead of erasure
- If we no longer use your data for the purposes of the processing, but you need it for the purposes of to make, exercise or defend against legal claims

- If you have lodged an objection, as long as it is not yet clear whether your interests prevail

Your right to data portability

You have the right to receive a copy of the data concerning you in a structured and commonly used format and to transmit this data to other organisations. You also have the right to ask us to forward your personal data directly to other organisations you have designated. We transfer your personal data to the extent technically possible and permitted by relevant national law.

Your right to erasure

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

- If your personal data is used for the purposes of: for which they were collected is no longer needed become
- If you withdraw your consent and there is no other legal basis
- If you object to the processing and it is no overriding reasons worthy of protection for a processing
- If your personal data has been unlawfully processed
- If your personal data is deleted in order to meet legal requirements conform

Please note that a right to erasure depends on whether there is a legitimate reason that requires the processing of the data.

Your right to lodge a complaint

In individual cases, you may not be satisfied with our response to your request. If so, you are entitled to lodge a complaint with ING's data protection officer and the responsible data protection supervisory authority.

Exercising your rights

If you wish to exercise your rights or have any other questions about how we use your personal data, you can contact us by sending an email to info@ing.de . You can also contact our Data Protection Officer by sending an email to datenschutz@ing.de .

The more specific your request is in exercising your rights, the better we can respond to your question. We may ask you for a copy of your ID or other information in order to establish your identity. It may happen that we reject your application. If permitted by law, we will inform you of the reason for this. Where permitted by law, we may be responsible for the processing of your application. We strive to process all applications in a timely manner.

9.

Your obligation to provide data

In some cases, we are required by law to collect personal data; we may need your personal data before we can provide certain services and deliver products. We undertake to request only those personal data that we absolutely need for the purpose in question. Failure to provide the required personal information may result in delays in the delivery of certain products and services.

10.

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 its processing. We apply an internal framework of policies and minimum standards across the company to protect your personal information. These guidelines and standards are regularly updated to adapt them to current legislation and market developments.

In addition, ING's employees are subject to confidentiality and may 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 on a permanent basis.

11.

What you can do to help us protect your information

We do our best to protect your data, but there are also some things you can do yourself: install antivirus software, spyware protection, and a firewall. Keep these programs up to date. Do not leave devices and tokens (e.g. bank cards) unattended. Report the loss of a bank card to ING and have the lost card blocked immediately. Log out of online banking if you are not currently using it. Keep your passwords top secret and use strong passwords, i.e. avoid obvious combinations of letters and numbers. Be vigilant on the Internet and learn how to avoid unusual

Detect activity, such as new website addresses or phishing emails that request personal information.

12.

Changes to this Privacy Policy

We may amend this Privacy Policy to reflect changes in the law and/or to reflect how our company processes personal data. We then change the revision date on the first page accordingly.
However, we recommend that you make this statement regularly. To check in order to always be informed about how we process and protect your personal data.

Information about your right to object

1. Case-by-case right of objection

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 for processing this data that outweigh your interests, rights and freedoms. Or your personal data is used to assert, exercise or defend legal claims.

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

In individual cases, we use your personal data for our direct marketing. You have the right to object to this at any time; this also applies to profiling if it is related to direct advertising.

In the event of an objection, we will no longer process your personal data for these purposes. The objection can be made in any form and should be addressed to: ING DiBa AG
Data Protection Officer
TheodorHeussAllee 2 60486
Frankfurt am Main Email:
datenschutz@ing.de