Privacy Statement for ING Wholesale Banking

Privacy Statement for ING Wholesale Banking

Index

This is the Privacy Statement of ING Bank N.V. - Sucursal em Portugal ("ING WB", "we", "us" and "our") with address at Avenida da Liberdade, nº 200, 6º, 1250-147 Lisbon. It applies to us whenever we process personal data of representatives[1] and contact persons of our corporate banking and investment clients.

1 What is the scope of this Privacy Statement

This Privacy Statement explains in a simple and transparent way what personal data of our corporate clients' representatives and contact persons we collect, record, store, use and process, and how we do it. Our approach can be summarised as follows: the right people use the right data for the right purpose.

This Privacy Statement applies to:

- All representatives and contact persons of past, present, and prospective customers who are corporate bank clients of ING WB ("you") including one-person businesses, beneficial owners, legal representatives or contact persons acting on behalf of our corporate banking clients;
- Non-ING WB customers, such as our clients' representatives, shareholders, beneficial owners, and anyone involved in transactions conducted by ING.

We obtain your personal data in the following ways:

- From a prospective or existing customer that provides us with your personal data to help us contact your organisation;
- From other available sources, such as debtor registers, land registers, commercial registers, registers of association, online or traditional media, publicly available sources, or other companies within ING WB or third parties, such as payment or transaction processors, credit agencies, other financial institutions, commercial companies, or public authorities.

2 Which types of personal data we process

Personal data refers to any information that identifies or can be linked to a natural person. Personal data we process about you includes:

- **Identification data:** name, date and place of birth, ID or equivalent number, Passport number, other data contained in your ID card, postal mail or email address, telephone number, title, nationality, place of residence, and signature;
- **Financial data:** credit history, credit capacity, and other information on your income and credit conditions;
- **Know our customer data, as part of our customer due diligence:** origin of your funds, relationship between account holders, purpose of the account (savings, investing, and others);
- **Audiovisual data:** image and voice, video recorded for surveillance purposes on ING premises, or recording of telephone calls and video calls;
- **Sensitive data:** criminal or related security data, data related to your political role.

3 What we do with your personal data

Your personal data will be processed for the purposes and legal bases described below:

[1]Representatives: Beneficial Owners and/or attorneys-in-fact who may act on behalf of the client.

3.1 Purposes and legal bases for processing.

Processing means every activity that can be carried out in connection with personal data, such as collection, recording, structuring, storage, modification, consultation, organisation, use, disclosure, transmission, restriction, or erasure in accordance with applicable laws.

At ING WB, we process personal data for a variety of purposes, always based on a lawful basis that enables us to do so.

You can find the purposes, legal bases, sources, and categories of data used, whether profiling is carried out, and the categories of recipients for each personal data processing operation we carry out in the table below:

Purpose of the processing	Legal basis	Sources* and data categories	Profiling**	Categories of recipients (transferees)
Managing the contracting of banking products and services that you have requested as representative of a corporate banking client and delivering such products and services.	Processing is necessary for entering into a contract in relation to which you act as the representative of one of the parties or taking steps prior to entering into a contract (pre-contractual measures).	Identification, transactions, financial, sociodemographic, audiovisual, signatures of representatives and attorneys of corporate clients, ID .	No.	ING NV and other Group companies; Public Notaries, Mandated Lead Arrangers (MLAs), Coordinating Bank, Structuring Bank, Agent, Collateral Agent; Other entities (in the assignment of contractual position or credit rights).
Performing marketing activities and offering ING products and services.	We will process your data as you are a representative of our client based on our legitimate interest to manage and increase our commercial activity.	Identification, transactions, financial, sociodemographic, identifiers.		No.
Complying with all regulatory obligations to which ING WB is subject, such as requirements from administrative authorities, fraud alert systems, and other regulatory bodies.	Processing is necessary for complying with the legal obligations to which ING is subject.	Identification, transactions, financial, sensitive data (convictions and infringements). In addition, Know Your customer (KYC) data, as part of our due diligence. We may also obtain information from external sources for this purpose.	We analyse certain aspects for this purpose.	Authorities and public bodies. Law enforcement agencies .

Purpose of the processing	Legal basis	Sources* and data categories	Profiling**	Categories of recipients (transferees)
Safety and security: Executing procedures and making decisions to ensure your safety and the Bank's safety. Protecting the assets of our corporate clients from online fraud. For example, if your username and password have been compromised, we may contact you if we detect any suspicious activity in your operations.	Processing is based on our legitimate interest to prevent losses from security incidents, such as fraud, and ensure the security and integrity of ING and the financial system. This helps us reduce risks and protect our corporate information for the correct functioning of bank services.	Identification, transactions, financial, sociodemographic, identifiers, preferences, and behaviour.	No.	Data will be communicated to the corresponding Supervising Authority.
Sending operational communications related to existing products and your usual banking activities.	Based on the contractual relationship that we maintain with you as the representative of an entity, we send communications that may be of interest to you for the proper use of the services.	Identification and contact data.	No.	No.
Managing Powers of Attorney.	Based on the contractual relationship that we maintain with your entity, we process the representative's data to formalise, verify, store, and revoke powers of attorney.	Identification, address, contractual.	No.	No.

* We process personal data provided by you. Any external data sources we may use are stated in the box above.

** For more information on profiling, please read section 3.3 of this Policy. Also, remember that you can request more detailed information about each profiling action at proteccion.datos@ing.es.

3.2. Legitimate interest

Where we rely on our legitimate interest to process your personal data, we have carried out an impact assessment to ensure that we are taking your interests and fundamental rights into account and that the processing we intend to carry out does not undermine them. Please contact us at dpo@ing.es if you would like to know about the outcome of this assessment.

3.3 Profiling

Your personal data may be used for profiling, i.e. ING may evaluate certain personal aspects to make predictions about you.

Fraud prevention, money laundering and terrorism financing

We have a duty to screen customers and transactions for potential criminal activity, with particular focus on suspicious transactions and transactions that, by their nature, may involve a relatively high risk of fraud, money laundering or terrorist financing. To this end, we create and maintain a risk profile on you in your capacity as representative of a corporate client. If we suspect that a transaction is related to money laundering or terrorist financing, we have an obligation to inform the authorities.

We consider there is a heightened risk of fraud or money laundering and terrorist financing when:

- There are deviations from normal spending and payment behaviour, such as unexpectedly transferring or debiting large amounts;
- There are suspicious payments between countries, commercial establishments, or addresses;
- You are included in an internal reference register. ING's internal reference register is a list of persons and institutions with whom we no longer wish to have a relationship. They are a risk to ING, its staff and/or its clients. Only employees of ING's security departments have access to this list;
- You are included in an external reference register. This external reference register is a list of banks in the Netherlands that includes persons and institutions that have committed fraud or pose a risk to the financial sector. Financial institutions in the Netherlands can check whether persons and institutions are on the list and can add them to the list;
- You are included in any national or international penalties list.

4 How long we retain data

ING WB will retain your data if necessary for the purpose for which it was collected or until required by a legal obligation, in accordance with its Internal Personal Data Retention and Deletion Policy.

When your personal data is no longer required for these purposes, ING will keep your data solely to take legal actions or conduct any action necessary for its defence, during the term legally established. Where applicable, your data will be blocked in accordance with current legislation and the period defined in the Policy.

Once these terms have expired, we delete or anonymise the data, in accordance with the regulatory provisions and legislation in force.

5 With whom and why we share your data

To fulfil the purposes set forth in Section 3, we share data with other ING Group entities and third parties. Sometimes data is shared with entities acting as processors for ING that process data to provide a service to us. Such entities should not use your information for any other purpose, and are required to delete or return it when the service is terminated.

In other cases, the entities that receive the data are assignees and become responsible for that data. In most cases, these entities are public bodies.

Whenever we share your personal data externally with third parties located in countries outside the European Economic Area (EEA), we ensure that the necessary safeguards are in place to protect it. For this purpose, we rely amongst others on:

- Requirements based on applicable local laws and regulations;
- EU standard clauses, when applicable, we use standardised contractual clauses in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with GDPR provisions. We carry out an assessment beforehand regarding the transfer and the legislation of the receiving country to ensure that all the necessary guarantees

are in place. If an adequate level is not guaranteed, we take the necessary organisational and/or technical mitigating measures (i.e. pseudonymisation or encryption) to ensure an adequate level of data protection;

- Adequacy decisions by the European Commission, establishing whether a country outside of the EEA ensures personal data is adequately protected;
- Binding Corporate Rules (BCRs) for transfers to ING Group companies located in a country without an adequate level of data protection.

ING entities

ING is part of the ING Group, which provides financial services in more than 40 countries (www.ing.com). ING Group is committed to data protection and has adopted strong data protection principles through its Global Data Protection Policy (GDPP). The GDPP has been approved by the Dutch Data Protection Authority, which is the lead supervisory authority of ING Bank NV, and is binding on all ING Group entities worldwide with respect to (i) the processing of personal data within the scope of the GDPR and (ii) the transfer of personal data from ING Group companies established in the EU to other ING Group companies established outside the EU. In addition, when we share data with other ING Group entities, we always sign a data processing agreement regulating the specific conditions to be considered in that processing.

To standardise and simplify its core banking processes, ING Group has centralised certain operations for efficiency purposes such as:

- Back-office activities, such as IT services (IT security, hosting, remote administration, and application services), payment and other transaction operations, fraud alerts or customer information analysis derived from our Know Your Customer obligation, which are centralised in ING Business Shared Services entities located, among others, in Slovakia, Poland and the Philippines;
- Development of other models related to the improvement of processes, communication with customers and quality of our products or services. This processing will be carried out by the Group's Analytics Department, and your personal data will be pseudonymised when transferred for this purpose;
- Development of models related to our Know Your Customer (KYC) requirement to protect ING Group against financial economic crimes. Group-wide models are being developed for the screening of customers and transactions with a view to detecting potential criminal activity. These models incorporate mandatory requirements derived from, among others, EU Directives and Regulations in the field of prevention of money laundering and terrorist financing, the Basel Committee on Banking Supervision (BCBS) Guidelines and EU, US, and UN criminal laws and regulations;
- Filing of internal and external reports, to be shared with authorities, such as the European Central Bank (ECB), the European Banking Association (EBA) or the Financial Stability Board (FSB). This data will be aggregated so that individualised information is not shared with these regulators.

Please note that ING will remain responsible for ensuring that the processing of your personal data, including any processing carried out by other ING entities on our behalf, follows the applicable data protection regulations. For example, we will ensure that your data is only processed for a specific purpose based on appropriate legal bases (considering any effects that such processing may have on you), and that appropriate operational and technical measures are in place to protect your rights.

Government, Supervisory and Judicial authorities

To comply with legal obligations, we may disclose data to the relevant government, supervisory and judicial authorities, such as:

- **Public authorities, regulators, and supervisory bodies,** such as central banks and other financial sector supervisors in the countries where we operate;
- **Tax authorities** may require us to report customer assets or other personal data, such as your name and contact details and other information about your organisation;
- **Judicial/investigative authorities,** such as the police, public prosecutors, courts, and arbitration/mediation bodies on their express and legal request.

Financial institutions

To process certain payment and withdrawal services, we may have to share information about customers or their representatives with another bank or a specialised financial company. 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.

Service providers and other third parties

Service providers support us with activities like:

- Designing, developing and maintaining internet-based tools and applications;
- IT service providers who may provide application or infrastructure (such as cloud) services;
- Marketing activities or events and managing customer communications;
- Preparing reports and statistics, printing materials and designing products;
- Placing advertisements on apps, websites and social media;
- Having legal, auditing or other special services provided by lawyers, notaries, trustees, company auditors or other professional advisors;
- Identifying, investigating or preventing fraud or other misconduct by specialised companies;
- Performing specialised services like postal mail by our agents, archiving of physical records, contractors and external service providers;
- Carrying out securitisation arrangements (such as trustees, investors, and advisers).

Independent agents, brokers, and business partners

We may share your personal data with independent agents, brokers or business partners who act on our behalf, or who jointly offer products and services with us, such as insurance. They are registered in line with local legislation and operate with due permission of regulatory bodies.

6 Your rights and how we respect them

If your personal data is processed, you have privacy rights.

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 to ask us to rectify it. If we shared data about you with a third party and that data is later corrected, we will also notify that party accordingly.

Right to object to processing

You can object to ING using your personal data for its own legitimate interests if you have a justifiable reason. We will consider your objection and whether processing your information has any undue impact on you that would require us to stop processing your personal data.

You can also object to receiving personalised marketing messages by opting out, using the **'unsubscribe'** link at the bottom of marketing emails or by contacting us at proteccion.datos@ing.es

In addition, even if you opt out of receiving personalised offers, we will alert you to unusual activity on your account, such as:

- When your credit or debit card is blocked;
- When a transaction is requested from an unusual location;

- When there is an informative communication that you should be aware of because it affects the products and services you have contracted with ING.

Right to object to automated decisions

Even though the regulations recognise this right, at ING we do not make automated decisions based on the personal information of our corporate banking and investment clients, so this right to object this type of processing is not applicable.

Right to restrict processing

You have the right to ask us to restrict the use of your personal data if:

- You believe the personal data is inaccurate;
- We are processing the data unlawfully;
- We no longer need the data, but you want us to keep it for use in a legal claim;
- You have objected to ING processing your personal data for our own legitimate interests.

Right to data portability

You have the right to ask us to transfer your personal data directly to you or to another company. This applies to personal data we process by automated means with your consent or based on a contract with you. Where technically feasible, based on applicable local law, we will transfer your personal data.

Right to erasure

You may ask us to erase your online personal data. ING will analyse the request and carry it out if appropriate. In any case, ING will retain your blocked data until the end of the defined data retention period.

Right to withdraw consent

You may withdraw the consent you have given us at any time.

Exercising your rights

To exercise these rights, please send your written request, enclosing a photocopy of your ID card or similar document, to proteccion.datos@ing.es or to the postal address Ing Bank N.V. - Sucursal em Portugal, Avenida da Liberdade, nº 200, 6º, 1250-147 Lisbon. You may also do so by visiting our offices.

When exercising your rights, the more specific you are with your application, the better we will be able to assist you.

We may ask you for a copy of your ID or additional information to verify your identity. In some cases, we may deny your request and, if permitted by law, we will notify you of the reason for denial. If permitted by law, we may charge a reasonable fee for processing your request.

We strive to address requests as quickly as possible within the statutory timeframes. However, based on applicable laws, response times may vary. Should we require more time (than what is normally permitted by law) to complete your request, we will notify you immediately and provide reasons for the delay.

If you are unhappy with the way we handle your personal data, you have the right to complain to ING's Data Protection Officer by sending an email to dpo@ing.es. If you are not satisfied with their response, you can also submit a complaint to the Portuguese Data Protection Agency (https://www.cnpd.pt).

7 How we protect your personal data

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 is processed.

We apply an internal framework of policies and minimum standards across all our businesses to keep your personal data safe. These policies and standards are periodically updated to keep them consistent with existing regulations and market developments.

In addition, ING employees are subject to confidentiality obligations and may not disclose your personal data unlawfully or unnecessarily. To help us continue to protect your personal data, you should always contact ING if you suspect that your personal data may have been compromised.

8 Changes to this Privacy Statement

We may amend this Privacy Statement for it to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created on 30TH November 2022.

9 Contact and questions

To learn more about ING's data privacy policies and how we use your personal data, you can send us an email to proteccion.datos@ing.es or contact the Data Protection Officer of ING at dpo@ing.es

ING