Privacy Statement for ING Wholesale Banking

Index

This document contains the **Privacy Statement for corporate banking clients** of ING BANK NV – Sucursal em Portugal (with address at Praça Marquês de Pombal, 14 1250-162 Lisboa).
To make reading easier, we will use the following abbreviations:

- «You» refers to representatives of our corporate clients.
- «ING», «ING WB», «we» o «our» refers to ING BANK NV – Sucursal em Portugal.
- «Privacy Statement» o «Policy» refers to this Privacy Statement.

1. What is the scope of this Privacy Statement

This Privacy Statement explains in a simple and transparent way how and what personal data we process in relation to representatives and contact persons of our ING WB clients.
This Privacy Statement applies to:

- All representatives and contact persons of former, current, and prospective corporate banking clients of ING WB (“you”), including one-person businesses, beneficial owners, legal representatives, or contact persons acting on behalf of our corporate clients.
- Non-ING WB clients. This may include representatives of our corporate clients, shareholders, guarantors, beneficial owners, and generally, any individual involved in transactions carried out through ING.

2. Which types of personal data we process

Personal data refers to any information that identifies you directly or indirectly as a natural person.
We obtain your data:

- From you, when you provide it directly as a representative or contact person of a prospective or existing corporate client.
- From other available sources such as beneficial ownership registers, land registries, commercial registries, association registries, online or traditional media, publicly available sources, other ING WB entities, or third parties such as payment or transaction processors, credit agencies, other financial institutions, commercial companies, or public authorities.

The personal data we may process about you include:

- **Identification data:** name, surname, date and place of birth, national ID number or equivalent, passport number, other data from your identity document, postal or email address, phone number(s), nationality, country of residence, and signature.
- **Transactional data:** deposits, withdrawals, and transfers made to or from the bank account of the client you represent, transaction identifiers, and associated information.
- **Financial data:** credit history, creditworthiness, and other information related to your financial standing and credit conditions; data from electronic payment instruments such as card number, expiration date, or card verification code (CVV/CVC) for cards linked to banking products of the corporate client where you have been designated as a user.
- **Sociodemographic data:** employment status and occupation, the company you work for and your position, education and employment information of shareholders, CEO, CFO, or other individuals in similar roles acting on behalf of a corporate client, for the evaluation, monitoring, and review of corporate credit risk.
- **Know Your Customer (KYC) data as part of our due diligence:** origin of funds, relationships between account holders, purpose of the account (saving, investing, etc.).
- **Identifiers, preferences, and online behavior data:** online user or mobile device identifier, including encrypted user data, IP address of the computer or mobile device you use, and the pages you visit on our app and websites. This includes information collected through cookies and other tracking technologies.
- **Data about your interests and needs:** data you share with us when contacting our customer service or completing an online survey, and data we infer from your interactions with us, such as how often and why you contacted us.
- **Audiovisual data**: image and voice, videos recorded for surveillance purposes at ING premises or ATMs, or recordings of phone and video calls.
- **Sensitive data:** criminal conduct or related security measures, data related to your political role.

We **do not process any sensitive data that may be inferred from transactions** you carry out on behalf of the entity you represent. For example, if you make a payment to a political party, trade union, religious institution, or healthcare entity, we will process this information solely for the purpose of executing the transaction you requested.

3. What We Do with Your Personal Data

a. Purposes and Legal Bases for Processing

At ING WB, we carry out various personal data processing activities for different purposes, always based on a lawful basis that allows us to do so. Below. you will find a detailed overview of the processing activities we may carry out with your personal data, including the purpose, legal basis, categories of data processed, and recipients. For cases where profiling is involved, please refer to the section "Profiling and Automated Decisions" in this Policy. You may also request more specific information about profiling at dpo@ing.es

We obtain your personal data directly from you. If we use other data sources, this will be explicitly indicated in the table below.

1. Contracting Products and Services

Purpose of the processing	To manage the contracting of banking products and services you have requested as a representative of a corporate banking client, and to execute them.
Legal Basis	Performance of a contract in which you represent one of the parties, or to take necessary steps prior to entering into the contract (pre-contractual measures).
Categories of data	Identification, transactional, financial, sociodemographic, audiovisual.
Profiling	No profiling.
Categories of recipients	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).

2. To comply with regulatory obligations

Purpose of the processing	Comply with regulatory obligations to which ING WB is subject and respond to information requests from Comissão Nacional de Protecção de Dados, Banco de Portugal, fraud alert systems and other regulatory bodies.
Legal Basis	**Compliance with legal obligations applicable to ING.**
Categories of data	Identification, transactional, financial, sensitive data (criminal convictions and offenses). Also, Know Your Customer (KYC) data as part of our due diligence, including information obtained from external sources for this purpose.
Profiling	Profiling is applied. We assess certain personal aspects for this purpose.
Categories of recipients	Public authorities and law enforcement agencies.

3. Sending communications

Purpose of the processing	Send informative and operational communications related to contracted products and regular banking activities, including sending newsletters and educational/informative communications, and requesting feedback on our products and services.
Legal Basis	**Performance of the contract** as a representative of the entity that has contracted our products or services. We may also send communications to **comply with legal obligations** applicable to ING. Additionally, we rely on our **legitimate interest** to contact you and maintain the commercial relationship with the corporate client you represent.
Categories of data	Identification data.
Profiling	No profiling.
Categories of recipients	No data sharing.

4. To maintain the relationship with our clients

Purpose of the processing	· Contact our clients. · Record online or phone conversations for quality purposes. · Manage the customer complaints inbox and the exercise of individual rights. · Handle suggestions or operational issues raised via our social media channels.
Legal Basis	**Performance of the contract** as a representative of the entity that has contracted our products or services, and to comply with legal obligations applicable to ING in case of complaints or rights requests.
Categories of data	Identification data.
Profiling	No profiling.
Categories of recipients	No data sharing.

5. To manage our internal operations

Purpose of the processing	**Generate internal reports, aggregated data analytics, and statistics to analyze ING's commercial operations and support business decision-making.** Analyzing how you use and interact with our products and services helps us improve our corporate and product strategy. This includes audience measurement and statistical analysis of your use of our website and mobile app, provided you have given prior consent for cookie installation.
Legal Basis	**Legitimate interest in managing and increasing our commercial activity and properly managing ING WB's commercial operations.**
Categories of data	Identification, transactional, financial, sociodemographic, identifiers, preferences and online behavior, interests and needs, and interactions with ING on social media.
Profiling	No profiling.
Categories of recipients	No data sharing.

6. To offer ING products and services

Purpose of the processing	Carry out marketing activities and offer ING products and services intended for the company you represent.

6. To offer ING products and services

Legal Basis	We process your data as a representative of our corporate banking client based on our **legitimate interest** in managing and increasing our commercial activity.
Categories of data	Identification, transactional, financial, sociodemographic, identifiers, preferences.
Profiling	No profiling.
Categories of recipients	No data sharing.

7. To ensure the security of ING's assets and protect our clients

Purpose of the processing	**Execute procedures and make decisions to ensure your safety and ING's.** Protect your assets and ING's through the implementation of security tools for the prevention and management of attacks and security incidents.
Legal Basis	We process your data based on our **legitimate interest** in preventing losses due to data security incidents and ensuring the security and integrity of ING and the financial system. This helps reduce business risk, protect organizational information, and ensure proper functioning of banking services. **Compliance with legal obligations** in the case of video surveillance for the security of premises and ATMs, in accordance with the Private Security Regulation.
Categories of data	Identification, transactional, financial, sociodemographic, identifiers, preferences and online behavior.
Profiling	No profiling.
Categories of recipients	Relevant Supervisory Authority.

8. Fraud prevention, detection, control, and investigation

Purpose of the processing	We use your data to carry out activities that allow us to prevent, detect, investigate, and control fraud, thereby avoiding financial losses for both ING and our clients.
Legal Basis	**Legitimate interest** in detecting and preventing fraud, protecting our clients whose accounts may be affected by fraud committed by third parties
Categories of data	Identification, transactions, financial, location, audiovisual, and sensitive data.

8. Fraud prevention, detection, control, and investigation

Profiling	Profiling is applied. Profiling in this processing activity is related to fraud prevention.
Categories of recipients	Financial institutions, Supervisory Authority for anti-money laundering (Banco de Portugal).

b. Legitimate Interest

When we rely on our legitimate interests to process your personal data, we always carry out a prior assessment to ensure that your interests and fundamental rights are respected and that the intended processing does not cause you harm.

If you would like to know the outcome of the legitimate interest assessment for a specific processing activity, please contact us at dpo@ing.es

c. Profiling

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

Fraud prevention, money laundering, and terrorism financing

We are required to analyze clients and transactions to detect potential criminal activities, paying special attention to unusual transactions and those that, by their nature, may carry a relatively high risk of fraud, money laundering, or terrorist financing. To this end, we create and maintain a risk profile about you, as a representative of a corporate banking client.

If we suspect that a transaction is related to money laundering or terrorist financing, we are legally obligated to report it to the authorities.

Factors we consider that may indicate a higher risk of fraud, money laundering, or terrorist financing include:

- Deviations from a person's normal spending and payment behavior, such as the transfer or debit of unexpectedly large amounts.
- Payments to or from suspicious countries, merchants, or addresses.
- Being listed in an internal reference register. ING's internal reference register is a list of individuals and institutions with whom we no longer wish to maintain a relationship. They pose a risk to ING, its staff, and/or its

clients. Only employees from ING's security departments have access to this list.
- Being listed in an external reference register. This external register is maintained by banks in the Netherlands and includes individuals and institutions that have committed fraud or pose a risk to the financial sector. Financial institutions in the Netherlands can check whether someone is on the list and may add new entries.
- Being listed on any national or international sanctions list.

4. Use of Artificial Intelligence by ING

ING may test and implement Artificial Intelligence (AI) systems to improve the efficiency and effectiveness of our workflows. For example, our relationship managers may use AI tools to respond to client inquiries. Personal data of representatives or contact persons of our corporate clients may be processed within these systems.
These personal data will be processed by Artificial Intelligence solutions in order to improve ING's financial crime and fraud prevention processes, based on its legitimate interest of using state of the art technology to ensure prevention, detection and containment of financial crime and fraudulent activities and to contribute to the security and stability of the financial system

5. How long we retain data

We will retain your data for as long as necessary to fulfill the purpose for which it was collected or to comply with a legal obligation, in accordance with our internal Personal Data Retention and Deletion Policy.
When your personal data is no longer needed for these purposes, we will keep it blocked for the period established by applicable legislation, solely to initiate legal action or defend ourselves in case of claims or demands, and to respond to requests from competent authorities. Where applicable, your data will remain blocked for the retention period defined by our internal policy.

Once these periods expire, we will delete or anonymize the data, in accordance with regulatory provisions and applicable legislation.

6. With whom and why we share your data

To fulfill the purposes described in the section "What We Do with Your Personal Data," we share data with other ING Group entities and third parties.
Sometimes, we share data with entities acting as data processors for ING, who process this information to provide a service to us. These entities are not allowed to use the data for other purposes and must delete or return the data once the service ends.
In other cases, the entities receiving the data become data controllers and are responsible for the information. In most cases, these entities are public authorities.
Whenever we share your personal data with third parties located in countries outside the European Economic Area (EEA), we ensure that appropriate safeguards are in place to protect it. For this purpose, we rely amongst others on:

- Requirements set out in applicable regulations and local legislation.
- EU Standard Contractual Clauses (SCCs) to ensure that personal data transferred outside the EEA complies with the General Data Protection Regulation (GDPR). We also conduct a prior assessment of the transfer and the legislation of the recipient country to ensure that all necessary guarantees are in place. If an adequate level of protection is not guaranteed, we implement necessary organizational and/or technical mitigation measures (e.g., pseudonymization or encryption) to ensure an appropriate level of data protection.
- Adequacy decisions issued by the European Commission, which determine whether a country outside the EEA provides adequate protection for personal data.
- Binding Corporate Rules (BCRs) for transfers to ING Group companies located in countries without an adequate level of data protection.

ING Group 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 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 for ING BANK NV, and is binding on all ING Group entities worldwide with respect to:

- The processing of personal data within the scope of the GDPR.
- The transfer of personal data from ING Group companies established in the EU to other ING Group companies established outside the EU.

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

- Back-office activities, including IT services (IT security, hosting, remote administration, and application services), payment and transaction operations, fraud alerts, and customer information analysis derived from our Know Your Customer (KYC) obligations. These activities are centralized in ING Business Shared Services entities located, among others, in Slovakia, Poland, and the Philippines.
- Development of models related to process improvement, customer communication, and product/service quality. This processing is carried out by the Group's Analytics department, and your personal data will be pseudonymized when transferred for this purpose.
- Development of KYC-related models to protect ING Group against financial economic crimes. Group-wide models are being developed to screen clients and transactions to detect potential criminal activity. These models incorporate mandatory requirements derived from, among others, EU Directives and Regulations on anti-money laundering and terrorist financing, Basel Committee on Banking Supervision (BCBS) guidelines, and EU, US, and UN sanctions laws and regulations.

We generate 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). These reports are aggregated so that no individualized information is shared with these regulators.

Please note that ING remains responsible for ensuring that the processing

of your personal data, including any processing carried out by other ING entities on our behalf, complies with applicable data protection regulations. For example, we ensure that your data is only processed for a specific purpose based on an appropriate legal basis (considering any impact such processing may have on you), and that appropriate operational and technical measures are implemented to protect your rights.

Third Parties with Whom We Share Data

Government, Supervisory and Judicial authorities

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

- Public authorities, regulatory bodies, and supervisory entities, including central banks and other financial sector supervisors in the countries where we operate.
- Tax authorities, which may request information about your assets or other personal data such as your name and contact details.
- Judicial and investigative authorities, such as law enforcement agencies, public prosecutors, courts, and mediation/arbitration bodies, upon formal and legal requests. These authorities may be local or from countries where we operate, provided they are competent.

Financial Institutions

To provide certain payment and withdrawal services, we may need to share information about you or your representatives with other banks or specialized financial companies. We also share information with financial sector specialists who assist us with services such as:

- Secure financial transaction messaging;
- Global payments and financial transactions;
- Processing of electronic transactions worldwide;
- Settlement of domestic and cross-border payment and securities transactions.

Service Providers and Other Third Parties

We work with service providers who support us in activities such as:El diseño, desarrollo y mantenimiento de las herramientas y aplicaciones disponibles en internet;

- Designing, developing, and maintaining internet-based tools and applications;
- IT services (including cloud infrastructure and applications);
- Marketing events and customer communication management;
- Preparing reports and statistics, materials, and product design;
- Placing advertisements on apps, websites, and social media;
- Legal, auditing, or other specialized services provided by lawyers, notaries, administrators, company auditors, or other professional advisors;
- Fraud detection, investigation, and prevention services provided by specialized companies;
- Specialized services such as postal mail delivery by our agents, physical document archiving, contractors, and external service providers;
- Securitization arrangements (e.g., trustees, investors, and advisors).

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.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

ING will share with SWIFT personal identification data (e.g., name, address), transaction data (e.g., account number of the sender and recipient in the case of a payment order), intended use details, and transaction identifiers (e.g., transaction reference number) for the purpose of securely managing transactions. ING and SWIFT have a joint controllership agreement to regulate their respective responsibilities in processing your data for this purpose.

SWIFT may also act as an independent data controller for statistical analysis and the development of SWIFT products and services. You can find more information in SWIFT's Privacy Policy. If you wish to exercise your individual rights regarding this processing, you can contact SWIFT at opt.out@swift.com or privacidad.officer@swift.com

Transfers Outside the European Economic Area (EEA)

Whenever we share your personal data externally with third parties located in countries outside the EEA, we ensure that appropriate safeguards are in place to protect it. This includes:

- Compliance with applicable regulatory requirements and local legislation;
- EU Standard Contractual Clauses (SCCs): where applicable, we use SCCs in agreements with service providers to ensure that personal data transferred outside the EEA complies with the GDPR. Before making such transfers, we assess the transfer and the legislation of the recipient country to ensure that all necessary guarantees are in place. If an adequate level of protection is not ensured, we implement necessary organizational and/or technical mitigation measures (e.g., pseudonymization or encryption) to ensure an appropriate level of data protection;
- International treaties that protect personal data transferred to certain service providers in countries outside the EU;
- Adequacy decisions issued by the European Commission, which determine whether a country outside the EEA provides adequate protection for personal data;
- Binding Corporate Rules (BCRs) for transfers to ING Group companies located in countries without an adequate level of personal data protection.

Additionally, we assess on a case-by-case basis whether it is necessary to implement organizational, technical (such as encryption), and/or contractual measures to ensure that personal data is adequately protected, considering the legal framework of the country where the data importer is located.

7. Your rights and how we respect them

This section outlines your rights regarding the personal data we process and how you can exercise them.

Right of Access

You have the right to request a list of the personal data we process about you.

Right to Rectification

If your personal data is incorrect, you have the right to request that we correct it. If we have shared your data with third parties and it is subsequently corrected, we will also notify those parties of the correction.

Right to Object to Processing

You may object to our processing of your personal data when the legal basis is our legitimate interest. We will review your objection and, if appropriate, stop processing your personal data.

You may also object to receiving our commercial communications:

You may also object to receiving our commercial communications by:

- Using the “unsubscribe” link located at the bottom of commercial emails.
- Sending your objection request to proteccion.datos@ing.es.

In any case, even if you opt out of receiving these communications, to ensure your rights, we will continue to send you communications that are directly related to the products and services you have contracted with us, 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, you should be aware of because it affects the products and services you have contracted with ING.

Right to object to automated decisions

This right allows you to request that decisions based solely on automated processing of your data (i.e., by technological means without human involvement), including profiling, not be made if they may negatively affect you.

You have the right to object to automated decision-making and request that the decision be reviewed by a person, to express your point of view, and to challenge the decision, where appropriate.

Right to restrict processing

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

- You believe your personal data is inaccurate.
- You believe we are processing the data unlawfully.
- We no longer need to process your data, but you want us to retain it for use in a legal claim.
- You have objected to our processing of your personal data based on our legitimate interests.

Right to data portability

You have the right to request that we transfer your personal data directly to you or to another company. This right applies to personal data we process by automated means. Where technically feasible, we will transfer your personal data directly to the company you specify.

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 through your “Personal Area”.

Exercising your Rights

You may exercise your rights through any of the following channels:

- By sending your request to proteccion.datos@ing.es or to the postal address of : ING España: c/ Vía de los Poblados, 1F, 28033 Madrid.
- By calling the phone number 0034 91 206 66 66.

When submitting a request, please be as specific as possible so we can assist you effectively. If we deny your request, we will explain the reason for the denial. Please note that, in some cases, we may charge a reasonable fee for processing your request (e.g., when requests are repetitive, excessive, or unfounded).
We aim to respond to your request as quickly as possible and always within the legally established timeframes. However, in some cases, response times may vary. If we need more time than normally permitted by law to complete your request, we will notify you immediately and explain the reason for the delay.

- If you are not satisfied with their response, you may also file a complaint with the Comissão Nacional de Protecção de Dados (https://www.cnpd.pt)
- If you are not satisfied with how we handle your personal data, you have the right to file a complaint with ING's Data Protection Officer by sending an email to: dpo@ing.es

8. How we protect your personal data

We are committed to ensuring the integrity and confidentiality of your personal data. To this end, we have implemented technical and organizational measures (policies and procedures, IT security, etc.). We apply an internal framework of policies and minimum standards to maintain the security of your personal data, which we update periodically to align with regulatory requirements and market developments.
ING employees are subject to confidentiality obligations and may not unlawfully or unnecessarily disclose your personal data.
We will never ask you to provide your passwords or access credentials via email or other unofficial channels.
If you suspect that your personal data may have been compromised, please contact us immediately.

9. Changes to this Privacy Statement

We may amend this Privacy Statement to remain compliant with legislative changes and/or to reflect changes in how we process personal data. The date of the latest version of this document is September 15, 2025.

10. Contact and Questions

- If you would like more information about how we process your personal data, you can contact us at: proteccion.datos@ing.es
- If you wish to contact ING's Data Protection Officer, you can do so at: dpo@ing.es

ING BANK NV, Sucursal en España, C/ Vía de los Poblados, 1F, 28033 Madrid, CIF W0037986G, inscrita en el Registro Mercantil de Madrid, Tomo 31798, Folio 1, Sección 8ª, Hoja M-572225.

ing.es

GDPR WB PORT ENG OL 09/25