Privacy Statement for ING Wholesale Banking customers

US - April 2025

do your thing

Contents

ING Bank N.V. is an European financial institution and is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 (GDPR).

To comply with GDPR, ING Bank N.V. has implemented data protection principles on a global scale, through its Global Personal Data Protection Policy (GPDP). The GPDP is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide and approved by the EU Data Protection Authorities. Therefore, in addition to local privacy laws and regulations, ING Bank N.V. has resolved that all its entities, subsidiaries, branches, representative offices, and affiliates worldwide comply with GPDP regardless of geographical location, market typology or target customer unless the local laws or regulations to which any ING entities, subsidiaries, branches, representative offices, and affiliates may be subject conflict with the GDPR and are otherwise more stringent and favourable to the individuals (as defined below) whose data is intended to be protected.

This is the Privacy Statement of ING Financial Holdings Corporation and its wholesale banking directly and indirectly wholly owned subsidiaries and corporate affiliates, in each case operating in the United States, (hereafter, collectively "ING WB", "us" , or "we", as the context may require), in each case a directly or indirectly wholly owned subsidiary of ING Bank N.V. ("ING Bank"), itself a consolidated subsidiary of ING Group N.V. ("ING Group").

1. Purpose and scope of this Privacy Statement

We understand that your personal data is important to you. This Privacy Statement explains in a simple and transparent way what personal data we collect, record, store, use and process. When handling your data, we seek to ensure that the right people are using the right data for the right purpose.

This Privacy Statement applies to:

- All individuals ("you") who are linked to ING WB customers and provide personal data as described in paragraph 2 below in the course of acting for or on behalf of an ING WB customer, including such individuals that are legal representatives, employees or other contact persons acting on behalf of our corporate customers, their beneficiaries or payees, guarantors, ultimate beneficial owners (UBO's), directors and officers, managers, members of a supervisory board, shareholders, debtors or tenants of our customers, visitors of our ING WB websites, or visitors of our physical locations, professional advisors, auditors, or other individuals in each case involved in transactions concerning an ING WB customer.

We obtain your personal data in the following ways:

- Directly from you, when acting in the capacity as a duly authorized officer or other legal representative of an ING WB customer, for example when you, as the company's representative, complete a form, sign a contract with ING WB, use our products and services, contact us through one of our channels or otherwise communicate with ING WB.

- Indirectly from your employer, when you may act as a representative, contact person or when you exercise a mandate provided to you by your employer (i.e. corporate card users) when it becomes a prospective customer or if it is an existing customer.

- From other available sources such as commercial registers, registers of association, the online or other publicly available media platforms or media sources, cookies and similar technologies via our websites and apps, other generally publicly available sources or from other ING WB related companies or third parties such as payment or transaction processors, other financial institutions, commercial companies or public authorities.

Further information may be provided by you when necessary, e.g. when you apply for a specific product or service on behalf of an ING WB customer.

We refer to our cookie statement as published on the ING WB website, www.ingwb.com, for more information about the use of cookies and comparable technologies.

2. The 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 can process about you may include (depending on the role of the individual that is acting on behalf of or in relation to our ING WB customers):

- **Identification data and contact data**: your name, date and place of birth, ID number, Social Security Number / Tax Identification Number, and National Identification Number, as well as other information included in the ID (such as citizenship or date of issue or expiration), passport information, email address, address, telephone number, title, nationality and a specimen signature, or identifier in systems of ING WB.

- **Socio-demographic data**, such as when a company or other legal entity applies for a corporate lending solution or to establish a financial markets trading relationship, we may process the name, company mandate, education, and employment information of its shareholders, CEO, CFO or other individuals in similar roles acting on behalf of a corporate client, for corporate credit risk assessment, monitoring, and review.

- **Online behaviour and information about your devices,** such as your IP address and device ID of your mobile device or computer, and the pages you navigate and your user behaviour when visiting ING WB websites and apps.

- **Data about your interests and needs that you share with us**, for example when you fill in an online survey.

- **Know Your Customer data** such as the name, date and place of birth, address, nationality, TIN, and government issued ID of Ultimate Beneficial Owners, principals, directors and legal representatives of companies, which we may process as part of customer due diligence and to prevent fraudulent conduct or behavior that contravenes international sanctions, and comply with regulations against money laundering, terrorism financing and tax fraud

- **Audio-visual data**: where applicable and legally permissible, we process surveillance videos at ING WB premises, or recordings of phone or video calls or chats with our staff. We can use these recordings to verify telephone orders, for example, or for fraud prevention or staff training purposes.

- **Your interactions with ING WB on social media**, such as Meta (Facebook and Instagram), Twitter, LinkedIn and YouTube. We follow public messages, posts, likes and responses to and about ING WB on the internet.

Sensitive personal data

Sensitive data may for include genetic, biometric or other health data, ethnicity, or your involvement in administrative or criminal proceedings or sanctions. For instance, we may process criminal data insofar as this is necessary for the management of our own disputes.

We may process your sensitive data for the purposes set out below in Section 3, "What we do with your personal data" if:

- We have obtained your explicit consent;
- We are required or allowed to do so by applicable local law; or when processing sensitive data in connection with:

- Know Your client (KYC) data obligations: we may keep a copy of your passport or ID card, as applicable based on local law;
- Money laundering or terrorism financing monitoring: we monitor your activity and may report it to the competent regulatory authorities; and
- If allowed under local law, and you choose to use it, we may use your face, fingerprint or voice as recognition for authentication to access mobile apps and certain operations therein.

3. What we do with your personal data

Processing means every activity that can be carried out in connection with personal data, such as collecting, recording, storing, adjusting, organising, using, disclosing, transferring or deleting it in accordance with applicable laws. We only use your personal data for:

Performing agreements to which you are a party or taking steps prior to entering into these agreements. We use your personal data when you enter into an agreement with us, or when we must execute our obligations under these agreements.

If you are acting on behalf of an ING WB customer, we may use your personal data to enter into an agreement with the ING WB customer, and to contact the ING WB customer when needed. If you are an individual providing a guarantee for the ING WB customer or a beneficiary of payment instruments, we may use your personal data to enter into an agreement or executing a payment order in connection to our arrangements with the customer. We may verify your capacity and powers using trade registers or incumbency certificates.

Compliance with our legal obligations. We use your personal data to comply with a range of legal obligations and statutory requirements, including banking and financial regulations such as: FinCEN's CDD Rule, OFAC's sanctions regulations and the Common Reporting Standard (hereinafter referred to as "CRS") or other regulations that oblige us to perform or provide:

- Integrity checks: when entering a customer relationship, we have a legal obligation to consult available incident registers and warning systems and national and international sanctions lists.

- Identity verification: when entering a customer relationship, we have a legal obligation to confirm identities (know your customer check) or check public exposure of such identities. We can do this by making a copy of an identity document, which we will only use for identification and verification purposes. Also, for identification purposes we may collect access/ logging data to our ING WB secure remote channels (via Home'Bank, via Business'Bank or via the ING Banking App, the chat room, or other apps). We may also rely on checks performed by other financial institutions to verify identities.

- In case of lending activities, information on address or geo-location details may be processed to ascertain the physical risk associated with assets in the event of natural disasters.

- Fraud prevention and anti-money laundering and terrorism financing checks: we have a legal obligation to check for potential fraud, money laundering and terrorism financing. This includes monitoring unusual transactions and sanctions lists).

- Regulatory and statutory reports to our regulators as set out in section 4, "Who we share your personal data with and why".

We rely on the lawful basis of 'necessary to comply with a legal obligation' when we use your data for these processing activities.

Our legitimate interest. We process your data for a range of purposes that are in our interests as described below.

When relying on legitimate interest, we ensure that processing remains proportionate and that your interests, fundamental rights and freedoms are respected. If you would like more information about the reasoning behind our assessment in a specific case, please contact us using the details provided in section 10, "Contact and questions".

Please find below an overview of the purposes for which we process your personal data where we rely on legitimate interest:

- **As our contact representing the ING WB Customer.** We process the personal data of authorized representatives and other employees or individuals acting on behalf of our corporate clients based on legitimate interest since we do not enter into an agreement with the individual but with the corporate client.

- **To develop and improve our products and services.** We may use your personal data when analysing your visit to our website or app with the aim of improving our website or app. We use cookies and comparable technologies for this purpose. For more information, please refer to our cookie statement as published on our site. We will also ask you for your feedback on our current products and services or ask for your opinion on new product ideas. This can include recording your conversations with us, but we will always inform you about this beforehand and obtain your consent via such notification, unless such recording is not allowed according to local law.

- **To maintain good commercial relations with all our ING WB customers and other concerned parties.** We may collect contact details of individuals acting on behalf of ING WB customers for commercial purposes (events, interesting deals, market research, etc.) and day to day contacts based on legitimate interest.

- **Relationship management and marketing.** We may ask you as the representative of the ING WB customer to give us feedback on the products and services offered to the ING WB customer. We may send newsletters regarding new and existing products and services offered by ING WB. You may opt out of any communication at any time.

- **We may also analyse your interactions with ING WB on social media**, such as Meta (Facebook and Instagram), Twitter, LinkedIn and YouTube. We follow public messages, posts, likes and responses to and about ING on the internet.

- **To ensure effective and efficient internal business process execution and management reporting.** We process your data for our internal processes and operations and to help our management to make better data-driven decisions about our operations and services. Data used for this purpose will be aggregated for this purpose where possible and required so that you are not identifiable.

  This includes:

  - analysing our market position in different segments;
  - performing a cost and loss analysis;

- training our staff, for example by analysing recorded phone calls (if recording is permitted by local law) in our call centres to improve our calling scenarios;
- automating our processes such as application testing, automatic filling of complaints handling, etc.;
- conducting litigation and complaint management.
- Meeting our environmental, social and governance commitments including external reporting.

- **To introduce and deploy Artificial Intelligence systems in order to increase the efficiency and effectiveness of our workflows.** We may process customers' personal data collected and stored for the financial crime and fraud prevention purposes, to ascertain the efficiency and effectiveness of deploying Artificial Intelligence solutions to improve ING WB's financial crime and fraud prevention processes. ING WB and ING Bank performs such testing activities based on its legitimate interest using state of the art technology in order to ensure prevention, detection and containment of financial crime and fraudulent activities and to contribute to the security and stability of the financial system.

- **ING WB may also use generative AI systems** (i.e. AI systems which are able to create original content such as new texts or images) for the following processing activities and purposes:
  - enhancement of our chatbot functionality if you use the chat, available from an ING WB Channel. If you use such Chatbot, you will be informed that you are interacting with an AI system;
  - engaging marketing content creation;
  - in the context of investigational initiatives directed at accurately detecting any suspicious activity that can be red flagged as fraud (early warning indicators)

- **To protect your vital interests.** We process your personal data when necessary to protect your interests which are essential for your life or that of another natural person. For example, for urgent medical reasons pertaining to you. We will only process your personal data necessary for the vital interests of another natural person if we cannot base it on one of the other purposes mentioned.

- **To respect your choice if we request your consent for specific personal data processing**.

- **To promote and offer the ING WB customer the best-suited products and services.** We will process your personal data when informing or advising you about similar products and services from ING WB. If you don't want to receive these offers you have the right to object or to opt out (please check the methods in section 6, "Your rights and how we respect them". We strive to understand you better and meet your changing needs by offering you services that will suit your specific situation. To achieve such personalisation, we may:
  - analyse your habits and preferences in our various communications channels, visits to our website or other online environments, etc.);
  - analyse the products and services that you have already purchased from us.

- For certain types of personal data processing, we will provide you with

specific information about the process and request your prior consent before processing your personal data. This may include:

- the use of biometric data such as face or fingerprints as authentication and/or verification purposes such as for access to mobile apps;
- recording your conversations with us online, by telephone or in our offices;

You may withdraw your consent at any time as set out in section 6, "Your rights and how we respect them."

4. Who we share your personal data with and why

There are situations in which we need to provide your personal data to other parties involved in the provision of our services. This could include data transfers across ING Group entities, to your employer (our ING WB customer) and to third parties.

Within ING

ING WB and the entities organized as a part thereof are subsidiaries of ING Group which provides financial services in over 40 countries. For more information about ING Group (with ING Bank, ING WB and related corporate affiliates and subsidiaries within the group, collectively "ING"), please visit https://www.ing.com/About-us/Profile/ING-at-a-glance.htm

ING Group is committed to your privacy and has adopted strong privacy principles through its Global Personal Data Protection Policy ('GPDP'). The GPDP is approved by the Dutch Data Protection Authority, which is the lead supervisory authority for ING, and is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide (also known as 'Binding Corporate Rules'.)

We may share your personal data within ING and its affiliates in other countries to ensure that we're able to comply with our legal obligations such as:

- To comply with any regulatory and statutory reporting obligations and data requests as required by ING Group's European regulators, including the European Banking Authority (EBA), European Central Bank (ECB) and the Financial Stability Board (FSB). Unless data on an individual level is specifically requested by a regulator, we will make sure that personal data is aggregated, meaning that only information about groups of customers will be shared with the Group's regulators to ensure that it can no longer be linked back to you.

- For the development of ING Group's internal credit models. Under EU banking rules, ING is obliged to develop these credit models to be able to calculate any counterparty risks and exposures. This allows ING WB to determine our risks as well as the extent of the financial buffer we are required to hold when providing financial services to your company.

- For the development of ING Group's know your customer (KYC) models. To safeguard ING Group against involvement in financial economic crimes, KYC models are being developed on a group level for customer and transaction screening to detect potential or actual criminal activity. These KYC models incorporate mandatory requirements derived from the EU Directives and Regulations around the prevention of money laundering and terrorist financing, the Basel Committee on Banking Supervision Guidelines (BCBS)

and EU, US and UN sanctions laws and regulations.

ING Group also continues to strive to make our everyday procedures more efficient and effective since it is in our legitimate interest to offer you the best possible services at competitive rates. As such, ING WB will share your personal data across certain affiliates of ING Group to centralise certain operations to achieve economies of scale, such as:

- For efficiency reasons, certain operational and administrative tasks in relation to the agreements we have with our customers, client management (including screening) or the processing of transactions have been centralised in processing centres, known internally as "ING HUBS", located in countries such as Slovakia, Poland, Romania, Turkey and the Philippines. These entities will process your data on behalf of ING and are fully subject to ING's Global Personal Data Protection Policy (GPDP) to ensure an adequate level of data protection.
- The development of models mainly related to improving customer processes such as optimisation of account management and product management. For efficiency reasons, these models are mainly developed by our analytics department on a group level. Your personal data will be pseudonymised when transferred for this purpose.
- We may use centralised storage systems to process data at a central point within ING for efficiency purposes. For instance, to create different types of credit risk models as mentioned above. These centralised storage systems are operated by ING Group or third parties such as Microsoft and might be located outside the EU. In any case, ING WB will always ensure that adequate measures are in place to safeguard your personal data.

Please note that ING WB will remain responsible for ensuring that the processing of your personal data - including any processing carried out by other ING Group entities on our behalf as set out above - complies with the applicable data protection regulations.

Across ING Group and its affiliates, including ING WB, there are strict requirements included in internal policies and contractual arrangements to ensure that your personal data will only be processed for a specific purpose on the basis of an appropriate legal basis if so required by local law (taking into account any effect such processing may have on you) and that adequate organisational and technical measures have been implemented to protect your rights.

We will also remain responsible for handling any request you may have in relation to your personal data protection rights as described in section 6, "Your rights and how we respect them".

With third parties

We also may share your personal data with the following third parties:

Government, supervisory and judicial authorities

To comply with our regulatory obligations, we're obliged by law to disclose certain personal data to the relevant government, supervisory and judicial authorities, including:

- **Public authorities, regulators** and **supervisory bodies** such as the European Central Bank (ECB) and De Nederlandsche Bank (the Dutch central bank, DNB) in the Netherlands.

- **Local 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. For this purpose, we may process your identification data such as social security number, tax identification number or any other national identifier in accordance with applicable local law.
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies at their express and legal request.

Other financial institutions
To process certain payment and withdrawal services, we may have to share information about the ING WB customer or its representative with another bank or a specialised financial company based in other countries. We may also share information with financial sector specialists who assist us with financial services like:

- Payments and credit card transactions worldwide, including Mastercard and VISA where applicable. Processing electronic transactions worldwide.
- Settling domestic and cross-border security transactions and payment transactions.
- Other services offered by other financial services organisations, including banks, broker-dealers, custodians, fund managers and portfolio service providers.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Joint controller
ING WB is working together with SWIFT as joint controllers to fulfill a common purpose: processing securely and reliable transaction services in line with our contractual commitment. In order to fulfill this purpose, personal data such an account number of the beneficiary should this be an individual or the payment details of such an individual, a payment order to an individual and other transaction identifiers (e.g. transaction reference number) are being shared with SWIFT.

As joint controllers, ING WB and SWIFT agreed to address requests concerning data subject rights and/or other relevant data protection questions concerning the processing activities performed jointly (processing of payments) in a centralized manner; as such, ING WB will be the main point of contact for any such requests as stated under section 6, “Your rights and how we respect them”.

Service providers and other third parties
When we use other service providers or other third parties to carry out certain activities in the normal course of business, we may have to share personal data required for a particular task. We carefully select these companies and enter into clear agreements with them on how they are to handle your personal data. We remain responsible for your personal data. These service providers support us with activities such as:

- Designing, developing and maintaining internet-based tools and applications.
- IT service providers who may provide application or infrastructure services (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.
- Legal, auditing or other special services provided by lawyers, notaries, trustees, company auditors or other professional advisers.
- Identifying, investigating or preventing fraud or other misconduct by specialised companies.

- Performing specialised services such as postal mail by our agents, archiving of physical records, contractors and external service providers.
- Carrying out securitisation arrangements (such as trustees, investors and the 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, such as insurance, with us. They are registered in line with local legislation and operate with due permission of regulatory bodies.

5. Transfer of personal data outside the European Economic Area

Whenever we share your personal data (if EU data protection laws apply) with third parties or ING WB affiliates located in countries outside the European Economic Area (EEA) that do not offer an adequate level of data protection, we will make sure there are adequate measures in place to ensure that your personal data is sufficiently protected.

For this purpose, we rely on so-called transfer tools, including:

- **EU Model clauses** or Standard Contractual Clauses - these are contractual clauses we agree with any external service providers located in a non-adequate country to ensure that such a provider is contractually obliged to provide an adequate level of data protection.

- **Binding Corporate Rules -** for personal data transfers within ING Group, we also rely on binding internal Group policies (i.e. the Binding Corporate Rules) to ensure that ING WB-related entities located in a non-adequate country adhere to an adequate level of data protection when processing personal data as set out in section 4, "Who we share your personal data with and why".

Furthermore, we will assess, where applicable, whether any organisational, technical (such as encryption) and/or contractual safeguards need to be implemented to ensure your personal data is adequately protected, considering the legal framework of the country where the data importer is located.

6. Your rights and how we respect them

If your personal data is processed, you have rights. Based on applicable laws, your personal data protection rights may vary from jurisdiction to jurisdiction. If you have questions about which rights apply to you, please get in touch with us using the email address mentioned in section 8, "How we protect your personal data."

You have the following rights:

Right of access
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 share 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 WB using your personal data for its own legitimate interests if you have a justifiable reason. We will

consider your objection and whether processing your personal data has any undue impact on you that would require us to stop processing your personal data.

You may not object to us processing your personal data if:

- we are legally required to do so; or
- it is necessary to fulfil a contract with you.

You can also object to receiving personalised commercial messages from us should you receive such messages.

Should you change your mind in the future, you can **choose to opt out of receiving these messages** by filling in our contact form on www.ing.com or contacting us at the email addresses in Section 10, "Contact and questions".

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

- you believe the personal data is inaccurate;
- we are processing the personal data unlawfully;
- we no longer need the personal data, but you want us to keep it for use in a legal claim;
- you have objected to us 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 you have provided us with directly and that we process by automated means with your consent or on the basis of a contract. Where technically feasible, and based on applicable local law, we will transfer your personal data.

Right to erasure ('right to be forgotten')
ING is sometimes legally obliged to keep your personal data. However, if you exercise your right to be forgotten, we will erase your personal data when:

- we no longer need it for its original purpose;
- you withdraw your consent for processing it;
- you object to us processing your personal data for our own legitimate interests;
- ING unlawfully processes your personal data; or
- local law requires ING to erase your personal data.

Right to complain
Should you as an ING WB customer's representative be unsatisfied 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 WB Data Protection Officer in the United States. If local law allows, you can also lodge a complaint with the data protection authority located in the country where your personal data is processed by us.

Right to withdraw consent
If you have given your consent to us for specific processing of your personal data as set out in section 3, "What we do with your personal data", you can withdraw your consent at any time. From that moment, we are no longer allowed to process your personal data. Please be aware that such withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Exercising your rights
To exercise any of the rights as set out above, please send your request to the local Data Protection Executive at WB-Americas.DPE@ing.com.

When exercising your right, the more specific you are with your request, the better we can assist you. We may ask you for 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 of your request. If permitted by law, we may charge a reasonable fee for processing your request.

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

7. Retention

ING WB do not store your personal data longer than we need to for the purposes (as set out in section 3, "What we do with your personal data", for which we have processed it. Sometimes we use different storage periods. For example, if the supervisory authority or government regulator requires us to store certain personal data longer, or if you have filed a complaint that makes it necessary to keep the underlying personal data for a longer period.

If we no longer need your personal data as described above, we delete or anonymise the personal data, in accordance with applicable laws and regulations.

8. How we protect your personal data

We take appropriate technical and organisational measures to ensure the availability, confidentiality and integrity of your personal data and the way it is processed. This includes state-of-the-art IT security, system and access controls, security monitoring, and segregation of duties for employees. 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 reviewed to keep them up to date with 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.

9. Changes to this Privacy Statement

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 in April 2025.

10.Contact and questions

For generic questions about this Privacy Statement, to learn more about how we protect and use your personal data, or if you wish to exercise your rights as a data subject, please send an email to the local Data Protection Executive office ("**local DPE**") at the dedicated email address indicated below.
While we encourage you to always contact the local Data Protection Executive office first, you can also directly contact the local Data Protection Officer ("**local DPO**"), using the DPO's email address below.

Location	Local DPE	Local DPO
United States	WB-Americas.DPE@ing.com	DPO.US@ing.com