Privacy Statement for ING Wholesale Banking Customers

Dubai - November 2026

Contents

1. Purpose and scope of this Privacy Statement 3
2. The personal data we process 3
3. What we do with your personal data 6
4. Who we share your personal data with and why 9
5. Transfers of personal data outside the DIFC 13
6. Your rights and how we respect them 13
7. Retention 16
8. How we protect your personal data 16
9. Changes to this Privacy Statement 16
10. Contact and questions 16
Appendix A — Supplement to the Privacy Statement for ING Bank N.V., Dubai Branch on the testing of AI solutions or similar technologies by ING Bank N.V. 18

ING Bank N.V., Dubai Branch ("ING Dubai") is a financial institution established in the Dubai International Financial Centre (DIFC) and is subject to the data protection obligations set out in DIFC Data Protection Law No.5 of 2020 Overview | DIFC.

ING Bank N.V. has implemented data protection principles on a global scale through its Global Personal Data Protection Policy (GPDP) / Privacy Policy. The GPDP / Privacy Policy is binding on all ING entities, subsidiaries, branches, representative offices and affiliates worldwide. EU 2016/679 (GDPR).

In addition to applicable local privacy laws and regulations, ING Bank N.V. requires its entities, subsidiaries, branches, representative offices and affiliates worldwide to comply with the GPDP regardless of geographical location, market typology or target customer.

This is the Privacy Statement of ING Bank N.V., Dubai Branch, part of ING Wholesale Banking and ING Group ("ING Bank N.V., Dubai Branch", "ING", "WB", "we", "us" and "our"), and it applies when we process personal data relating to individuals ("you").

1. Purpose and scope of this Privacy Statement

At ING Wholesale Banking ("WB"), 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 and how. 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 past, present and prospective individuals ("you)" who are linked to WB customers. This may mean legal representatives of WB customers or contact persons acting on behalf of our corporate customers, beneficiaries or payees, guarantors, ultimate beneficial owners, directors and officers, members of supervisory board, shareholders, debtors or tenants of our customers, visitors of our WB websites, or visitors of our physical locations, professional advisors, auditors, or other individuals involved in transactions concerning an WB customer. This Privacy Statement also applies, where relevant, to individuals whose communications or meeting information may be captured in connection with WB Financial Markets services, including representatives of customers and prospective customers, counterparties, customer representatives, non-FM ING colleagues, professional advisers and other external parties who communicate with or interact with Financial Markets staff through approved business communication channels or in relevant business meetings.

We obtain personal data in the following ways:

▪ Directly from you, when you act in the capacity of legal representative of a WB customer, for example when you, as the companies' representative register yourself for our online services, complete a form, sign a contract with ING, use our products and services, contact us through one of our channels.

▪ 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) or when you are an employee in the context of salary payment conventions concluded between your employer and ING.

▪ From other available sources such as commercial registers, registers of association, the online or traditional media, cookies and similar technologies via our websites and apps, publicly available sources or other ING 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 where necessary, e.g. when you apply for a specific product or service.

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

2. The personal data we process

Personal data refers to any information that relates to an identified or identifiable living natural person, whether the person can be identified directly or indirectly. Personal data we can process about

you may include (depending on your role while 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 and National Identification Number, TIN, as well as other information included in the ID documentation (such as citizenship or date of issue or expiration), email address, address, telephone number, title, nationality and a specimen signature, fiscal code/social security number or identifier in systems of ING.

- **Transaction data,** such as any deposits, withdrawals and transfers made to or from the WB bank account, and when and where these took place, transaction identifiers and associated information.

- **Financial data:** when you undertake a guarantee with us for the benefit of a customer, we may verify credit history, credit capacity, and other information relating to your creditworthiness and credit conditions;

- **Socio-demographic data**, when a company applies for a corporate lending solution, 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 customer, for corporate credit risk assessment, monitoring, and review.

- **Online behaviour and preferences data:** IP address of your mobile device or computer and the pages visited on WB websites and apps;

- **Data about your interests and needs** that you share with us, for example when you contact our officers or call centre, use our platforms or complete an ING survey, including online surveys.

- **Know our customer data as part of customer due diligence** and to prevent fraudulent conduct or behaviour that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud; such as the name, date and place of birth, address, nationality, TIN, and government issued ID of UBOs, 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 and communications monitoring data:** where applicable and legally permissible, we process surveillance videos at ING branches, or recordings of phone or video calls or chats with our offices. In the context of Financial Markets services, this may include communication conducted through approved business communication channels used for regulated market activities. The data processed may include the content of the communication, date and time, participants, contact details, channel identifiers, recordings, transcripts where applicable, and related audit information. We use this information, among other things, to verify instructions and transactions, meet legal and regulatory obligations, support market conduct monitoring, investigate incidents, respond to requests from competent authorities, handle disputes and complaints, and where permitted, support staff training and quality assurance.

- **Your interactions with ING 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.

- **Information related to your location when making a payment or when accessing certain products/services**, for example when you withdraw cash from an automated teller machine (ATM). Or geo-coordinates linked to assets movable or immovable (in the case of physical risk processes for loans).

Special Categories of Personal Data

Special Categories of Personal Data include personal data revealing or concerning, directly or indirectly, racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership, health or sex life, genetic data, and biometric data where it is used for the purpose of uniquely identifying a natural person. We will process Special Categories of Personal Data only where permitted by applicable law and subject to appropriate safeguards.

We may process your Special Categories of Personal Data where:

- You have provided your explicit consent, where consent is required by applicable law;
- The processing is necessary to comply with legal or regulatory obligations;
- The processing is necessary to protect your vital interests or those of another individual where permitted by law;
- The processing is necessary for the establishment, exercise or defence of legal claims; or
- The processing is otherwise permitted or required under applicable law.

We apply appropriate technical, organisational and administrative measures to protect Special Categories of Personal Data against unauthorised access, disclosure, alteration, loss or misuse. We do not use Special Categories of Personal Data for marketing purposes.

We may process Special Categories of Personal Data in connection with:

- Compliance with know your customer (KYC), sanctions screening, anti-money laundering and counter-terrorist financing obligations;
- Fraud prevention, detection and investigation activities and reporting to competent authorities where required by law;
- The establishment, exercise or defence of legal rights or claims; and
- Biometric authentication services, where available and permitted by law, such as the use of facial recognition, fingerprints or voice recognition technologies, where you choose to use such functionality and any required consent has been obtained.

Where another applicable law, including GDPR, ING's GPDP or Privacy Policy provides additional protections for special categories of personal data, we will also apply those protections where relevant.

Please note that if you (as a representative of an WB customer) instruct us to make a payment to a political party, trade union, a religious institution or health care institution, this qualifies as Special Categories of Personal Data. Therefore, ING will not process those Special Categories of Personal Data for purposes other than executing the transaction or with your explicit consent. It is possible that as a result of our obligation to comply with anti-money laundering regulations and our interest in preventing fraud, we may further process such data, for example to verify the origin of the funds, but only in the context of anti money laundering regulations.

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, organising, adapting, using, analysing, disclosing, transferring, restricting, anonymising or deleting it in accordance with applicable laws and regulations.

We process your personal data for the following purposes:

1. Performing agreements and providing financial services

We use your personal data when entering into, administering or performing agreements with our customers and when taking steps prior to entering into such agreements.

If you act on behalf of a corporate customer, we may process your personal data to establish and manage the customer relationship, verify your authority to act on behalf of the organisation, communicate with you, and provide products and services requested by the customer.

If you are a guarantor, beneficiary, authorised signatory, director, ultimate beneficial owner, legal representative or other individual connected with a customer relationship, we may process your personal data in connection with our arrangements with the customer, including verifying your authority, identity or capacity through trade registers, corporate records, incumbency certificates or other reliable sources.

2. Compliance with legal and regulatory obligations

We use your personal data to comply with a range of legal obligations and statutory requirements, including banking and financial regulations such as the Common Reporting Standard (hereinafter referred to as "CRS") or reporting obligations related to FATCA or to the Deposit Guarantee schemes in the Banking System, MiFID, EMIR, MMSR – or other regulations that oblige us to perform or provide:

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

▪ Identity verification: when entering into a customer relationship with you, we have a legal obligation to confirm your identity (know your customer check) or check your public exposure. We can do this by making a copy of your identity document, which we will only use for identification and verification purposes. Also, for identification purposes we may collect your access/ logging data to our ING SCC 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 your identity.

▪ In case of lending activities, information on address or geo-location details may be processed in order to ascertain the physical risk associated with your 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.

▪ 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.

3. Legitimate business interests

We may process personal data where necessary for our legitimate business interests, provided that those interests are not overridden by your rights and freedoms.

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 our 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 Dubai Customer** -we process the personal data of Legal Representatives and other employees or individuals acting on behalf of our corporate customers based **on legitimate interest** since we do not enter into an agreement with the individual but with the corporate customer.

▪ **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 these. We use cookies and comparable technologies for this. For more information, we refer to our cookie statement as published on our sit. We will also ask 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 unless this is not allowed according to local law.

▪ **To promote and offer you the best-suited products and services provided by us or other ING entities.** We will process your personal data when informing or advising you about similar products and services from ING. Of course, if you don't want to receive these offers you have the right to object or to opt out (please check the methods to our "Right to object to processing" section. 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.

▪ **To maintain good commercial relations with all our customers and other concerned parties. We** may collect contact details of individuals acting on behalf of ING Dubai 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 customer to give us feedback on the products and services offered to the business customer. We may send newsletters regarding new and existing products and services offered by ING. You may opt out of any communication at any time.

▪ **We may also analyse your interactions with ING 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. We will always choose aggregated data for this if we can, 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.

▪ **Safety and security**. We have a duty to protect all personal data and to prevent, detect and contain a data breach or fraud involving personal data collected to comply with regulations against money laundering, terrorism financing and tax fraud. To safeguard and ensure the security and integrity of ING, the financial sector, customers and employees, we may

- Process your personal data to protect your organisation´s assets from fraudulent activities, for instance in case your identity (e.g. username and password) is compromised.

- Use certain personal data (e.g. name, account number, age, nationality, IP address, etc.) for profiling to detect fraudulent activities and the actors behind it.

- Use your personal data to alert you in case we detect suspicious activities involving your business´s assets, for example a transaction is taking place from a non-typical location.

To test 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 financial crime and fraud prevention purposes, in order to ascertain the efficiency and effectiveness of deploying Artificial Intelligence solutions in order to improve ING's financial crime and fraud prevention processes. ING Bank NV performs such testing activities based on its legitimate interest of 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. The testing activities lead to the selection and deployment of technologies which meet our standards of efficiency and correctness.

ING 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 Channel. If you use such Chatbot, you will be informed when you are interacting with an AI system;

▪ engaging in 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).

▪ in the context of loan origination and monitoring processes, in order to identify potential indicators of financial distress or other issues which may affect the reimbursement capacity, we monitor financial market information, news articles and external ratings by relying on generative AI solutions. As part of this process your name, role or facts associated with your activities may be processed, as a representative/individual connected with the ING Dubai customer.

Where personal data is used in connection with autonomous or semi-autonomous systems, including artificial intelligence, generative AI and machine-learning solutions, we will implement appropriate technical and organisational safeguards, including access controls, security measures, data minimisation and governance processes designed to ensure responsible processing. These safeguards may include testing for accuracy, reliability and bias, controls on the use and retention of prompts and outputs, appropriate human oversight, and procedures for reviewing and correcting inaccurate or unsupported outputs.

In accordance with DIFC Regulation 10, we assess the role performed by each relevant ING entity and service provider in relation to a system, including whether it acts as a Deployer, Operator, Provider, Controller or Processor. Where a system may involve High Risk Processing, we will carry out the required risk and data protection impact assessments and determine whether Regulation 10 certification or other enhanced governance measures apply before the system is used commercially.

Where automated processing is used, we will provide meaningful information where required about the nature and purpose of the processing, the types of outputs produced and the significance and reasonably foreseeable consequences for individuals. We will not make a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects you unless the decision is permitted by applicable law and appropriate safeguards are in place. Where those safeguards apply, you may request human intervention, express your point of view and contest the decision.

Further information about the testing of artificial intelligence solutions or similar technologies by ING Bank N.V. is set out in Appendix A.

4. 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.

5. Processing based on consent

Where we rely on consent as the legal basis for processing, we will clearly explain the relevant purpose and, where required, request separate consent for separate processing activities.

You may withdraw your consent at any time through the available communication channels. Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

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 within ING Group, to your employer (the organisation or corporate customer that you represent) and to third parties.

Within ING

ING Dubai is part of ING Group which provides financial services in over 40 countries. For more information about ING Group, please visit ING at a glance | ING.

ING is committed to your privacy, and it has adopted strong privacy principles through its Global Personal Data Protection Policy ('GPDP') / Privacy Policy. The GPDP / Global Privacy Policy is approved by the Dutch Data Protection Authority, which is the lead supervisory authority for ING Bank N.V., 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 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 always 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'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 to determine our risks as well as the extent of the financial buffer we are required to hold when providing financial services to you.

▪ For the development of ING's know your customer (KYC) models. To safeguard ING 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 in the area of 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 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 will share your personal data within ING 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, customer management (including screening) or the processing of transactions have been centralised in processing centres, named 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) / Privacy Policy 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 in customer channels. 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 or third parties such as Microsoft and might be located outside the EU. In any case, ING will always ensure that adequate measures are in place to safeguard your personal data.

ING Dubai remains responsible for ensuring that personal data processed on its behalf by other ING entities complies with applicable data protection requirements. Internal policies and contractual arrangements require personal data to be used for specified purposes, on an appropriate lawful basis, and protected by suitable technical and organisational measures. ING Dubai also remains responsible for responding to requests concerning processing for which it is the controller.

With third parties

We also 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. Also, including the Central Bank of the UAE (CBUAE), Dubai Financial Services Authority and the DIFC Commissioner of Data Protection.

▪ 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 Dubai 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 financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Joint controller

ING 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 as:

- account number of the beneficiary in the case this is an individual
- payment details of such payment order to an individual
- and transaction identifiers (e.g. transaction reference number) are being shared with SWIFT.

As joint controllers, ING 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 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. Where a party processes personal data on our behalf, we remain responsible for meeting our obligations as Controller. Some recipients may instead act as independent or joint Controllers and will be responsible for their own processing under applicable law. 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).

Where we appoint service providers or processors to process personal data on our behalf, we will select parties that provide sufficient guarantees to protect personal data in accordance with applicable law. Our agreements with such parties will include appropriate terms on the purpose of processing, categories of personal data, duration of processing, confidentiality, security, breach notification and any relevant cross border transfer or foreign-law considerations.

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.

Researchers

We are always looking for new insights to empower you to stay a step ahead in life and in business. For this reason, we exchange personal data (when it is legally allowed) with partners such as universities and other independent research institutions, who use it in their research and innovation. The researchers we engage must satisfy the same strict requirements as ING employees. When

possible, the personal data will be shared at an aggregated level to ensure the results of the research are anonymous.

5. Transfers of personal data outside the DIFC

Whenever we share your personal data with third parties or other ING entities located outside the DIFC, for the jurisdictions that have been recognized by the DIFC Commissioner of Data Protection as providing an adequate level of protection, we may rely on that recognition, for the jurisdictions that do not offer an adequate level of data protection, we will use a transfer mechanism permitted by the applicable data protection law that ensures appropriate safeguards are in place.

Appropriate safeguards may include mechanisms such as Standard Contractual Clauses, Binding Corporate Rules or other safeguards recognised by the DIFC Commissioner of Data Protection. Where required, we will carry out and document an assessment of the transfer and apply additional contractual, organisational or technical measures 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. The EU transfer mechanisms referred to below continue to apply where EU GDPR is relevant. For transfers from Dubai, those global mechanisms will be used only in a way that is also compliant with the DIFC data- transfer regime described above.

▪ 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 entities located in a non-adequate jurisdiction 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).

▪ Other safeguards or legal grounds including the DIFC Standard Contractual Clauses permitted by the DIFC Data Protection Law (Data Export & Sharing: Transferring Personal Data | DIFC).

Furthermore, we will assess on a case-by-case basis 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 privacy rights. Based on applicable laws, your privacy rights may vary from jurisdiction to jurisdiction. If you have questions about which rights apply to you, please get in touch with us through the email address mentioned in section 10.

You have the following 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 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. When you become an ING customer, we may ask you whether you want to receive personalised offers.

Should you change your mind later on, you **can choose to opt out of receiving these messages**. For example, you can use the **'unsubscribe' link** at the bottom of commercial emails or manage your preferences on our website or mobile banking app.

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.

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 with you. Where technically feasible, and based on applicable local law, we will transfer your personal data.

Rights relating to automated decision-making

Where a decision is based solely on automated processing, including profiling, and produces legal effects or similarly significantly affects you, you may have the right not to be subject to that decision and to request human intervention, express your point of view and contest the decision, subject to the conditions and exceptions in applicable law.

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 or for personalised commercial messages;
- ING unlawfully processes your personal data; or
- local law requires ING to erase your personal data.

Right to complain

If you are dissatisfied with how we have handled your personal data or responded to your request, you may complain to ING Dubai using the contact details in section 10. You may also lodge a complaint with the DIFC Commissioner of Data Protection. A person who suffers damage as a result of a contravention of the DIFC Data Protection Law or Regulations may have the right to apply to the DIFC Courts for compensation; damage may include financial loss and non-financial damage such as distress.

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. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal. Depending on your circumstances and the other laws applicable to the processing, you may also have additional rights under GDPR, ING's GPDP / Privacy Policy or other applicable data protection laws.

Exercising your rights

To exercise any of the rights as set out above, please send your request to your ING branch location. For generic questions related to this privacy statement, please send your request to DPE_UAE@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 and provide reasons for the delay. To exercise a right, contact ING Dubai through your usual relationship contact or use the privacy contact details in section 10. Please describe your request clearly. We may ask for additional information to verify your identity or authority to make the request.

We will respond within the period required by applicable law. Where permitted, we may extend that period, refuse a request or charge a reasonable fee, for example where a request is manifestly unfounded, excessive or repetitive. We will explain our decision where required.

7. Retention

We do not store your personal data longer than we need to for the purposes set out in section 3 (What we do with your personal data). For applicable retention periods we refer to the applicable local privacy statement. We determine retention periods by reference to the duration of the customer relationship, applicable legal and regulatory retention requirements, limitation periods, financial-crime and sanctions obligations, disputes, investigations and litigation holds. Sometimes we use different storage periods. For example, if the supervisory authority 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 regulatory provisions and applicable law.

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. 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.

If a personal data breach occurs, we will assess its nature, scope and likely consequences; take reasonable steps to contain and remedy it; document the incident; and notify the DIFC Commissioner of Data Protection as soon as practicable, where required. Where the breach is likely to result in a high risk to your security or rights, we will also notify you as soon as practicable, unless an applicable exception applies.

9. Changes to this Privacy Statement

We may update this Statement to reflect changes in law, regulation, guidance, our business, technology or processing activities. We will make the current version available through the appropriate ING channel and provide additional notice where required. This version is dated November 2026.

10. Contact and questions

To learn more about how we protect and use your personal data, or if you wish to exercise your rights, please contact the people responsible for data protection compliance for ING Bank N.V., Dubai Branch. You may also raise a complaint with the DIFC Commissioner of Data Protection using the details in the overview below.

For generic questions related to this statement you can send an email to DPE_UAE@ing.com

For Dubai-related privacy queries, rights requests or complaints, please contact DPE_UAE@ing.com and Elena-raluca.barzu@ing.com. If you are not satisfied with how we handle your request or concern, you may contact us through the Dubai privacy contact details set out in this Privacy Statement. You may also consult or lodge a complaint through the public channels made available by the DIFC Commissioner of Data Protection.

Contacts for ING Dubai	Details
ING Data Protection Contact Email	DPE_UAE@ing.com
Data Protection Executive	Zsolt Katona Zsolt.katona@ing.com
Data Protection Officer	Raluca Elena Barzu Elena-raluca.barzu@ing.com
DIFC Commissioner of Data Protection	Commissioner@dp.difc.ae

Appendix A — Supplement to the Privacy Statement for ING Bank N.V., Dubai Branch on the testing of AI solutions or similar technologies by ING Bank N.V.

ING Bank N.V., as Data Controller and parent company of ING Dubai, 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 or similar technologies in order to improve ING Group's financial crime and fraud prevention processes. ING Bank N.V. performs such testing activities based on its legitimate interest of 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. When relying on its legitimate interest, ING Bank N.V. ensures that the processing remains proportionate, in respect of data protection by design principles and that the data subject's interests, fundamental rights and freedoms are safeguarded. All other relevant information on the underlying processing activities related to financial crime and fraud prevention workflows, including information on the exercise of the data subjects rights, the technical and organisational measures taken by ING Group to protect your personal data, data retention as well as ING's contact details can be found in the relevant sections of ING Dubai Personal data protection statement, above.