



Privacy Statement for ING Securities Capital Company customers - KSA

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.

For individuals residing in the Kingdom of Saudi Arabia ("KSA"), this Privacy Statement also reflects the Saudi Personal Data Protection Law ("PDPL"), its Implementing Regulations, and applicable Saudi banking-sector requirements. Where EU GDPR, ING's Global Personal Data Protection Policy ("GPDP"), EU transfer mechanisms or Binding Corporate Rules remain relevant, those protections continue to apply; however, for KSA customers and customer representatives we will also meet the additional and more specific requirements of Saudi law described in this Privacy Statement

For KSA individuals, this Privacy Statement is intended to satisfy your right to be informed under applicable Saudi law. It explains our identity and contact details, the legal basis and specific purposes for which we process personal data, the categories of personal data we process, the retention period or the criteria used to determine it, your rights and how to exercise them, and how you may withdraw consent where consent is the legal basis

This is the Privacy Statement of ING Securities Capital Company (ING SCC), a subsidiary of ING Bank N.V. and belonging to ING Group, all its entities, subsidiaries, branches, representative offices, affiliates ('WB', 'we', 'us' and 'our'), and it applies to us as long as we process personal data that belongs to individuals ('you').

1. Purpose and scope of this Privacy Statement

At ING Securities Capital Company, 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 ING Securities Capital Company (“WB”) customers. This may mean legal representatives of ING Securities Capital Company 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 ING websites, or visitors of our physical locations, professional advisors, auditors, or other individuals involved in transactions concerning an ING SCC customer.

We obtain your personal data in the following ways:

- Directly from you, when acting in the capacity of legal representative of an ING SCC 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.

Where we collect your personal data from a source other than you, we will inform you where required by applicable Saudi law, of the categories of personal data concerned and the source from which we obtained it, without undue delay and within the period required by law unless an exception applies

Where we collect personal data directly from you, we will tell you which data is mandatory and which is optional, the legal basis and purpose for collection, and the key consequences if mandatory data is not provided. We collect only the minimum personal data necessary for the relevant purpose, product, service, or legal / regulatory requirement.

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 ING website 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. For individuals in KSA, this also includes data relating to a deceased individual where it would lead to that person, or a member of their family, being identified. Personal data we can process about you may include (depending on your role while acting on behalf of or in relation to our ING SCC 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 ING SCC 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 an ING SCC customer, we may verify credit history, credit capacity, and other information relating to your credit worthiness and credit conditions. We also process electronic payment instrument data such as card number, expiry date or card verification code (CVV/CVC) for cards attached to banking products where you have been designated as user.
- **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 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 and your user behaviour when visiting on ING websites and apps.
- **Data about your interests and needs that you share with us,** for example when you contact our call centre or fill in an online survey or when you use our platforms or fill in surveys.
- **Know our customer data** 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:** where applicable and legally permissible, we process surveillance videos at ING premises, ING or affiliated ATMs or recordings of phone or video calls or chats with our offices. We can use these recordings or recordings of phone or video calls or chats with our offices. We can use these recordings to verify telephone orders, for example for fraud prevention and to respond to formal enquires initiated by competent authorities or staff training purposes.
- **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).

Sensitive personal data

For individuals in KSA, “Sensitive Data” includes personal data revealing racial or ethnic origin, religious, intellectual or political belief, data relating to security criminal convictions and offences, biometric or genetic data used for identification, health data, and data indicating that one or both of an individual’s parents are unknown. Where GDPR or another applicable data protection law also applies, ING will comply with the additional requirements of that law. These requirements may provide additional legal bases, safeguards or restrictions for specific types of personal data. We will process Sensitive Data only where permitted under applicable law and subject to appropriate safeguards. In particular:

- we will not rely on legitimate interest as a lawful basis for processing Sensitive Data under Saudi law;
- where consent is the applicable legal basis for processing Sensitive Data, we will obtain explicit consent;
- we will not use Sensitive Data for marketing purposes; and
- we will apply appropriate technical, organisational and administrative measures to protect Sensitive Data against unauthorised access, disclosure, alteration, loss or misuse.

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

We may process your sensitive data for the purposes set out below in [Section 3 \(What we do with your personal data\)](#).

For example, we process 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, or voice as recognition for authentication to access mobile apps and certain operations therein.

Processing your sensitive personal data always takes place within the limitations of the following safeguards. Therefore, we process such data only when:

- You have provided your explicit consent;
- The processing is necessary to protect your or another individuals’ vital interests in cases where the individual (including yourself) is physically or legally incapable of providing consent;
- The sensitive data has been made manifestly public by you;
- The processing is necessary for the establishment, exercise or defense of legal claims;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;

- When the processing is carried out under the control of an official authority (applicable only for criminal data);
- When the processing is authorized by Union or Member State law (applicable only for criminal data).
- Where the processing involves Sensitive Data, Credit Data, or a decision based solely on automated processing, we will obtain explicit consent where applicable Saudi law requires it, unless another lawful exception applies.

Please note that if you (as a representative of an ING SCC customer) instruct us to make a payment to a political party, trade union, a religious institution or health care institution, this qualifies as sensitive personal data. Therefore, ING will not process this sensitive 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, adjusting, organising, using, disclosing, transferring or deleting it in accordance with applicable laws. We only use your personal data for:

For KSA customers and customer representatives, the lawful basis for processing under Saudi law may be: your consent; processing necessary to perform a contract with you or to take steps requested by you before entering into that contract; processing required by Saudi law; processing necessary to protect vital interests where reaching you is impossible or difficult; and, for non-sensitive personal data only, processing necessary for our legitimate interests where this does not prejudice your rights or interests, is within your reasonable expectations, and we have carried out the documented assessment required by applicable Saudi law.

Where we rely on consent under Saudi law, the consent request will be clear and specific, the relevant processing purpose(s) will be explained to you, separate consent will be sought for separate purposes where required, the consent will be documented so it can be evidenced later, and withdrawal will be as easy as, or easier than, giving consent

For the avoidance of doubt, where this Privacy Statement refers to our “legitimate interest” in relation to KSA data, that reference is limited to the narrower legitimate-interest basis permitted by Saudi law and does not apply to Sensitive Data.

- 1. 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 on behalf of the ING SCC customer, or when we have to execute our obligations under these agreements.

If you are acting on behalf of an ING SCC customer, we may use your personal data to enter into an agreement with the ING SCC customer, and to contact the ING SCC customer when needed. If you are an individual providing guarantee for the 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.

2. 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: 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. 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 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 SCC Customer** -we process the personal data of Legal 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 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 the extent permitted by applicable law, we may use your contact details to send you information about relevant ING products and services, or other marketing or promotional materials, only where we have obtained any prior consent required by applicable Saudi law and always with a clear and simple means for you to opt out of future marketing communications. We will not use Sensitive Data for marketing purposes

(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 SCC 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 contact you as the representative of the customer for relationship-management, service, transaction, regulatory, product-servicing or feedback purposes. Where a communication is marketing in nature and Saudi law requires consent, we will obtain that consent before sending it through your personal communication channels

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.

• **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 SCC customer.

Where we use automated processing or artificial intelligence tools in connection with your personal data, we will do so only for the purposes described in this Privacy Statement and subject to appropriate safeguards.

If a decision is made solely on the basis of automated processing of your personal data and Saudi law requires explicit consent or specific notice, we will provide the required information and obtain explicit consent where applicable before carrying out that processing.

Where automated processing or AI tools are used to support fraud prevention, financial crime detection, risk monitoring, customer servicing or operational efficiency, we will apply data minimisation, access controls, security measures and, where appropriate, pseudonymisation or anonymisation.

3. **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.

4. Based on your consent

Where we rely on consent under Saudi law, the consent request will be clear, specific and presented before or at the time we request your consent. We will explain the relevant processing purpose, document your consent in a way that allows it to be verified later, and request separate consent for separate processing purposes where required.

You may withdraw your consent at any time through the available communication channels. The withdrawal of consent will not affect the lawfulness of processing carried out based on consent before its withdrawal. Where consent is withdrawn, we will stop the relevant processing without undue delay, unless another lawful basis applies.

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 (our ING SCC customer) and to third parties.

Within ING

ING Securities Capital Company is part of ING Group which provides financial services in over 40 countries. For more information about ING Group, please visit <https://www.ing.com/About-us/Profile/ING-at-a-glance.htm>

ING is committed to your privacy, and it 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 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, client 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) 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.

Please note that ING SCC will remain responsible for ensuring that the processing of your personal data - including any processing carried out by other ING entities on our behalf as set out above - complies with the applicable data protection regulations. Within ING there are strict requirements included in internal policies and contractual arrangements in place 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 below.

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.
- **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 SCC 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:

- o account number of the beneficiary in the case this is an individual
- o payment details of such payment order to an individual
- o 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. 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).

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. Transfer of personal data outside the European Economic Area and outside the Kingdom of Saudi Arabia

Where personal data of individuals in KSA is transferred or disclosed outside the Kingdom, we will do so only where the transfer or disclosure is permitted under applicable Saudi law. This includes ensuring that the transfer is limited to the minimum personal data necessary for the relevant purpose, does not prejudice national security or the vital interests of the Kingdom, and does not undermine the protection required under Saudi law or your ability to exercise your rights.

Depending on the circumstances, the transfer may rely on an adequate level of protection, recognised by the competent Saudi authority appropriate safeguards recognized under Saudi law. Appropriate safeguards may include mechanisms such as Standard Contractual Clauses, Binding Common Rules or other safeguards recognised by the competent Saudi authority. Where required, we will carry out and document an assessment of the transfer and apply additional contractual, organisational or technical measures to protect your personal data.

Whenever we share your personal data (if EU data protection laws apply) with third parties or other ING entities 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. The EU transfer mechanisms referred to below continue to apply where EU GDPR is relevant. For transfers from KSA, those global mechanisms will be used only in a way that is also compliant with the Saudi 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 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).
- Saudi banking-sector localisation caveat - Where Saudi banking-sector rules applicable to a particular product or service require certain data or records to be stored in the Kingdom, or otherwise impose additional localisation controls, we will comply with those requirements

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, taking into account 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 in scope of Saudi PDPL, you may have the following rights, subject to the conditions and exceptions provided by the applicable law. 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 10 (How we protect your personal data)

You have the following rights:

Right to be informed

You have the right to be informed about how we collect and process your personal data, including the purpose, legal basis, categories of data, retention period or retention criteria, and how to exercise your rights.

Right of access and right to request a copy

You have the right to request access to your personal data and to request a copy of your personal data in a readable and clear format, subject to applicable legal limitations.

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 SCC 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. 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.

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

Should you as a customer or as a 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 Bank data protection officer. You can also lodge a complaint with the data protection authority located in the country where your personal data is processed by us. info@sdaia.gov.sa

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 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 where you hold your bank account. For generic questions related to this privacy statement, please send your request to **WB.DPE.OFFICE@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.

For requests made under the Saudi PDPL, we will act on your request without undue delay and, i, within 30 days of receipt. Where permitted by law, that period may be extended by up to a further 30 days and, if so, we will notify you in advance and explain the reason for the delay.

We may ask for additional information to verify your identity before actioning your request. We may refuse to act on a request where permitted by applicable law, for example where the request is repetitive, manifestly unfounded or requires disproportionate effort, and we will inform you of the reason where required.

7. Retention

We 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. For applicable retention periods we refer to the applicable local privacy statement. 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.

For KSA personal data, once the purpose of collection has ended, we will destroy, delete or anonymise the personal data without undue delay unless retention is required by Saudi law, other applicable legal or regulatory requirement, or because the data is closely related to a matter before a judicial authority. In such caases, we will retain the personal data only for the period required or permitted by 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, 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.

We take the organisational, administrative and technical measures required under applicable Saudi law to reduce the risk of personal data breaches and to preserve the security and privacy of your personal data. If a personal data breach occurs that may cause harm to your personal data or prejudice your rights or interests, we will notify the competent Saudi authority where the legal threshold is met, within 72 hours of

becoming aware of the incident. Where required by applicable law, we will also notify affected individuals without undue delay.

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 March 2025. Where required by applicable Saudi law, we will inform you before using your personal data for a purpose that is materially different from the purpose originally notified to you, and we will obtain consent where the law requires it.

10. Contact and questions

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 as indicated in the overview 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, using the dedicated email address as indicated in the overview below.

For generic questions related to this statement you can send an email to WB.DPE.OFFICE@ING.COM

For KSA-related privacy queries, rights requests or complaints, please keep WB.DPE.OFFICE@ING.COM and add an approved KSA external-facing branch contact route here: Lisa.Walker@ing.com. If you are not satisfied with how we handle your request or concern, you may contact us through the KSA 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 Saudi Data & AI Authority (“SDAIA”), where applicable.

Supplement to the Personal data protection Statement of ING Securities Capital Company on the testing of AI solutions or similar technologies by ING Bank N.V.

ING Bank NV, as Data Controller and parent company of ING Securities Capital Company KSA, 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 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. When relying on its legitimate interest, ING Bank NV

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 Securities Capital Company KSA's Personal data protection statement, above.