Privacy Statement

for

ING Luxembourg customers

v. 4.0 December 2025

Contents

1. Purpose and scope of this Privacy Statement 3
2. The types of personal data we process 4
3. What we do with your personal data 6
4. Who we share your personal data with and why 11
5. Transfer of personal data outside the EEA 16
6. Automated decision-making and profiling 17
7. Your rights and how we respect them 19
8. Are you obliged to provide us with your personal data? 23
9. How long we keep your personal data 23
10. How we protect your personal data 23
11. Changes to this Privacy Statement 24
12. Contact and questions 24

ING Bank N.V. is a European financial institution and is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 (GDPR). To comply with the GDPR, ING Bank N.V. has implemented data protection principles on a global scale, through its Global Data Protection Policy (GDPP). The GDPP is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide and approved by 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 GDPP regardless of geographical location, market typology or target customer.

This is the Privacy Statement of ING Luxembourg S.A. and its subsidiaries ING Lease Luxembourg S.A. and ING Solutions Investment Management S.A. (together, 'ING Luxembourg', 'we', 'us' and 'our'). It applies to us when we process Personal Data that belongs to the individuals mentioned in Section 1 below ('you').

1. Purpose and scope of this Privacy Statement

At ING, 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 ING customers who are individuals. This includes one-person businesses.

- Non-ING customers. These could include anyone who makes a payment to or receives a payment from an ING account; anyone who visits an ING website, branch or office; professional advisers, shareholders, anyone who is a guarantor of our customers; ultimate beneficial owners (including some individuals related to them, such as family members of politically exposed persons) as well as directors, representatives or contact persons of our corporate customers or other legal entities that uses our services; debtors, tenants or family members (first degree) of our customers; anyone involved in other transactions with us or with our customers(in their personal capacity or as a representative of a legal entity); final beneficiaries of sums deposited on a virtual bank account by customers. Depending on your relationship with us, especially if you are not an ING customer, we may

collect and use fewer personal data than described in this Privacy Statement. Feel free to reach out to us using the contact details indicated in Section 12 (Contact and questions) to exercise your right of access and receive an overview of your personal data that we process.

We obtain your personal data in the following ways:

- Directly from you when you become a customer, register 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 the organisation that you manage or that employs you when you act as a representative or contact person of this organisation and when the latter becomes a prospective ING customer or if it is an existing ING customer.

- From other available sources such as debtor registers, land registers, commercial registers, registers of association, the online or traditional media, cookies and comparable technologies via our websites and apps, publicly available sources or other ING Group companies or third parties such as payment or transaction processors, credit agencies, other financial institutions, commercial companies (e.g. Refinitiv which provides World-Check risk detection services), 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 Policy as published on our website (www.ing.lu) 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 an individual. Personal data we process about you includes:

- *Identification data,* such as your name, date and place of birth, ID number, email address, telephone number, title, nationality and a specimen signature, fiscal code/social security number, signature data (including electronic signature data).
- *Transaction data*, such as your bank account number, any deposits, withdrawals and transfers made to or from your account, and when and where these took place, transaction identifiers and associated information.

- *Financial data*, such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, credit capacity, credit worthiness and credit conditions, tax status, income and other revenues and/or financial products you have with ING, whether you are registered with a credit register, payment arrears and information on your income, electronic payment instrument data such as card number, expiry date or card verification code (CVV/CVC).
- *Socio-demographic data*, such as your gender, education, job position and marital status including whether you have children.
- *Online behaviour and information about your devices*, such as your IP address and device ID of your mobile device or computer and the pages you visit 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* as part of customer due diligence and to prevent fraudulent conduct or behaviour that contravenes international sanctions and for us to 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, or recordings of phone or video calls or chats with our offices. We can use these recordings to verify telephone orders, for example, or for fraud prevention and, more generally, to evidence commercial transactions and business communications you have with us.
- *Your interactions with ING on social media*, such as Meta (Facebook & 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 ATM.
- *Information related to your property* such as the property type (house, flat, etc.), its size, geo-location coordinates, specifications and its energy class.

Sensitive personal data

Sensitive personal data is personal data relating, for instance, to your health, ethnicity, religious or political beliefs or biometric data as well as data relating to criminal convictions and offences (e.g. information on fraud). We may process some of your sensitive personal data as set out below in Section 3 (What we do with your personal data) if we have your explicit consent, when we are required to do so by applicable

laws and regulations, or when otherwise permitted by applicable laws and regulations, for instance, where the processing is necessary for reasons of substantial public interest or for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Please note that if you 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. However, it is possible that as a result of our obligation to comply with anti-money laundering and terrorism financing regulations, our interest in preventing fraud and in exercising or defending legal claims, we may further process such data, for example to verify the origin of the funds in the context of anti-money laundering and terrorism financing regulations.

Children data (only applies to our retail customers)

We only collect personal data about children if they have an ING product or if you provide us with personal data about your own children in relation to a product you obtain from us. We will seek parental consent when it is required by law.

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. Processing may be performed on multiple hardware and software environments, including generative AI-powered applications. We only use your personal data for:

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

For instance, we use your account details when you ask us to make a payment or carry out an investment order or to provide you with statements of your accounts or your annual overview in My ING. We also use these account details to, when necessary, block payments, investigate and remediate product dysfunctionalities and solve claims, petitions and complaints regarding the requested services, when necessary. We also use your personal data to contact you in order to notify you of issues such as contractual term changes, the expiry of a deadline/contractual

condition, registering a debt or to provide you with information related to your services/relationship.
We rely on the lawful basis of 'necessary for performing agreements' when we use your personal data for these purposes and for other compatible purposes.

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, that oblige us to perform or provide:

- *Integrity checks*: when entering into a customer relationship with you, we have a legal obligation (due mainly to anti-money laundering and terrorism financing laws) 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 (due mainly to anti-money laundering and terrorism financing laws) to confirm your identity (also referred to as Know-Your-Customer check). We can do this by making a copy of your identity document, which we will only use for identification and verification purposes. We may also rely on checks performed by other financial institutions to verify your identity. We also need to know your postal, e-mail address or phone number to contact you.
- *Credit checks*: before entering into a customer relationship with you, we have a legal obligation to check whether you qualify as an eligible customer. We assess your credentials from a risk perspective and predict if you can meet your financial obligations towards us as set out in Section 6 (Automated decision-making and profiling). 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. This includes monitoring unusual transactions and sanctions lists as set out in Section 6 (Automated decision making and profiling).
- *Regulatory and statutory reports to our regulators* as set out in Section 4 (Who we share your personal data with and why).
- *IT security checks and related measures:* we have a duty to protect your data and to ensure the security and integrity of ING systems.
- *Checks on our communications with you:* we have a duty to record electronic communications and telephone conversations concerning transactions on financial instruments with investors or potential investors.

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

Our legitimate interest. We process your data for a range of purposes that are in our interests as described below. When relying on legitimate interest, we ensure that processing remains proportionate and that your interests, fundamental rights and freedoms are respected. If you would like more information about our reasoning behind our assessment in a specific case, please contact us using the details provided in Section 12 (Contact and questions). Please find below an overview of the purposes for which we process your personal data where we rely on legitimate interest:

- **To develop and improve our products and services.** We will for example ask you for your feedback on our current products and services or ask for your opinion on new product ideas. We may share this with certain members of our staff to improve our offering.

  Also, we analyse how you use and interact with our products and services. This helps us understand more about you and shows us where and how we can improve. For instance:

  - when you open an account, we measure how long it takes until you are able to use your account;
  - we analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns.

  We also use your payment data or any other banking, financial or credit data, to:

  - provide you with information on your past financial situation (incomes and/or expenses). This can take the form of an overview of the amounts spent per category: transport expenses, supermarkets, ...
  - assess in advance whether you are eligible for certain products and services and, if so, give you the opportunity to subscribe to them. For example, we may look at your payment behaviour and credit history when you apply for a loan or a mortgage;
  - for credit monitoring. We use and analyse data about your credit history and payment behaviour to assess your ability to repay a loan in the course of the credit contract and, as the case may be, to contact you on this matter.

- **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. We may also send you newsletters informing you about our activities.
  Of course, if you do not want to receive these offers and newsletters, you have the right to object and to opt out. Moreover, 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:

  - take into account your sociodemographic and financial situation;
  - take into account your property and its energy efficiency;
  - analyse your habits and preferences in our various communications channels;
  - analyse the products and services that you have already purchased from us.

- **To ensure effective and efficient internal business process execution, everyday procedures, statistics 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. This includes:

  - analysing our market position in different segments;
  - performing cost and loss analysis;
  - training our staff;
  - automating our processes such as application testing, automatic filling of complaints handling, etc.;
  - managing litigation and complaints;
  - examining whether new rules have been properly implemented, to determine whether processes are being done properly, or to identify risks associated with a process;I
  - allowing some customers to sign documents electronically;
  - sharing your data with other entities within the ING Group to centralise or optimise certain operations to achieve economies of scale, as well as with external service providers (IT service providers, for instance) that carry out certain activities in the normal course of business on our behalf. You can find more specific information regarding these operations and activities undertaken by the aforementioned ING Group entities and external service providers in the “Summary Table of the Third-party and/or ING Group common infrastructure” which is accessible in the General Terms and Conditions section of our website (www.ing.lu);

- meeting our environmental, social and governance (so-called ESG) commitments including external reporting.

- **To ensure safety and security.** In certain cases, even in the absence of a specific legal obligation to do so, we put in place measures that ensure the safety and security of your personal data when we deem that those measures are necessary and proportionate. Many of these measures relate to network and information security and preventing and combatting cybercrime, fraud and any other actions that compromise the availability, authenticity, integrity or confidentiality of your personal data. For instance:

  - we may process your data to protect your assets from fraudulent activities online, for example, if you are hacked and your username and password are comprised. In this context, we process behavioural data (linked to your use of a mouse, a keyboard, etc.);
  - we may use certain information about you (e.g. name, account number, age, nationality, IP address, etc.) for profiling purposes to detect fraudulent activities and the perpetrators;
  - we may use your personal data to alert you if we detect suspicious activity on your account, for example when your debit or credit card is used in a non-typical location.

- **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 individual (for example, for urgent medical reasons pertaining to you). We will only process your personal data as needed for the vital interests of another natural person if there is no other lawful basis to base this processing activity.

- **To respect your choice if we request your consent for specific personal data processing.** For certain types of personal data processing, we will provide you with specific information about the process and request your prior consent before processing your personal data. This may include:

- Using your personal data when analysing your visit to our website or app with the aim of improving these and to promote and offer you the best-suited products and services. We use cookies and comparable technologies for this. For more information, we refer to our Cookie Policy published on our site.
- Promotional activities where we inform you about products and services from ING partners.
- Personalised marketing activities based on profiling performed on the basis of the analysis of your payments data or similar details. With your consent, we may send you communications offering you a product or service based on your personal profile (based on payment data) or show you such an offer when you log in to our website or mobile apps.

You may withdraw your consent at any time as set out below.

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 and to third parties.

Within ING Group
ING Luxembourg is part of the ING Group which provides financial services in over 40 countries. For more information about ING Group, please visit www.ing.com. ING Group is committed to your privacy.

ING Luxembourg may share your personal data with its parent company ING Bank N.V. (located in the Netherlands) to ensure that the ING Group will be able 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), the 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 ING Group's regulators to ensure that it can no longer be linked back to you.

- Meet its commitments in terms of sustainability and issues related to environment, social and governance (so-called ESG). Unless data on an individual level is required

to attain these commitments, we will make sure that the personal data shared with our parent company ING Bank N.V. for this purpose cannot be linked back to you.

- Develop (also on behalf of ING Luxembourg) global and local ING internal credit models. Under EU banking rules, the ING Group is obliged to develop these credit models to be able to calculate any counterparty risks and exposures. This allows the ING Group to determine our risks as well as the extent of the financial buffer we are required to hold when providing financial services to you.

- Develop (also on behalf of ING Luxembourg) global and local ING Know Your Customer (KYC) models. To safeguard the ING Group against involvement in Financial Economic Crimes, KYC models are being developed on ING Group level for customer and transaction screening to detect potential or actual criminal activity. These KYC models incorporate mandatory requirements derived from, among others, EU Directives and Regulations in the area of prevention of money laundering and terrorism financing, the Basel Committee on Banking Supervision Guidelines (BCBS) and EU, US and UN sanctions laws and regulations.

- Carry out the overall management of legal and reputational risks related to money laundering and terrorism financing.

We also continue 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 Luxembourg will share your personal data with other entities of the ING Group to centralise certain operations to achieve economies of scale. These operations include:

- For efficiency reasons, certain operational and administrative tasks in relation to agreements we have with our customers, client management (including screening) or the processing of transactions have been centralised in processing centres named ING Business Shared Services (also called ING Hubs) and located in countries such as Slovakia, Poland, Romania and the Philippines. Our ING Hubs will process your data on behalf of ING Luxembourg and are fully subject to ING's Global Data Protection Policy (GDPP) to ensure an adequate level of data protection. More specifically, the tasks performed by ING Hubs notably relate to:
    - enabling third-party payment service providers to carry out operations on your account(s) that you instruct them to carry out;
    - Know Your Customer (KYC) services;

- Swift and payment services platforms;
- our tech infrastructure, including in relation to IT security service;
- our portal used to facilitate the management of our products and services;
- the printing and management of client documents;
- credit risk management;
- market risk management;
- our Web-Banking platform My ING;
- our secure digital communication channels (e.g. audio calling, chat messaging and messaging);
- central services for Over-the-Counter (OTC) financial instrument transactions;
- central services linked to positions acquired in financial instruments on European markets (in relation to our retail and private banking customers only);
- credit and debit card production and management as well as transaction authentication via the Internet;
- marketing event management;
- client relationship management;
- an automated translation system;
- the technical infrastructure supporting our internal emails, SharePoint data and archiving;
- our contact centre;
- regulatory reporting;
- trading and contract management services for International Swaps and Derivatives Association (ISDA) and related collateral (in relation to corporate customers only);
- cash management;
- global client support (in relation to corporate customers only);
- lending administration services (in relation to corporate customers only).

You can find more specific information regarding the tasks listed above and the location of the ING Hubs that carry out these tasks in the Summary Table of the Third-party and/or ING Group common infrastructure which is accessible in the General Terms and Conditions section of our website (www.ing.lu).

- The development of models mainly relates 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 the

analytics department at the ING 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 Luxembourg 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 the ING Group, 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 (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 categories of third parties:

Government, supervisory and judicial authorities

To comply with our regulatory obligations, we are obliged by law to disclose personal data to the relevant government, supervisory and judicial authorities, such as:

- **Public authorities, regulators** and **supervisory bodies** such as the European Central Bank (ECB) and Luxembourg Financial Sector Regulator (*Commission de Surveillance du Secteur Financier*) and, in case of requests for mortgage-related interest subsidies, the Luxembourg Ministry of Housing (*Ministère du Logement*).
- **Local tax authorities**, for instance to comply with the Foreign Account Tax Compliance Act (so-called FATCA), with the Common Reporting Standard (so-called CRS) and with the rules on the Central Electronic System of Payment information (so-called CESOP). This may require us to report customer assets or other personal data such as your name and contact details and, as the case may be, 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 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 share your personal data with another bank or a specialised financial company. We also share your personal data with financial sector specialists who assist us with financial services such as:

- Exchanging secure financial transaction messages such as Worldwide Interbank Financial Telecommunication (SWIFT).
- Payments and credit transactions worldwide, including Mastercard and VISA where applicable.
- Processing electronic transactions worldwide.
- Settling domestic and cross-border security transactions and payment transactions.
- Account information services: if you have specifically instructed an account information service provider to retrieve account information from your ING accounts on your behalf, we are obliged to share the necessary transaction data with such a provider as long as you have consented to this.
- Payment initiation services: if you have specifically instructed a payment initiation service provider to initiate payments from your ING accounts on your behalf, we are obliged to share access to your accounts with such a provider as long as you have consented to this.
- Other financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

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.
- Providing IT 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.
- Mortgage mandates services.
- Identifying, investigating or preventing fraud or other misconduct by specialised companies.
- Performing specialised services such as postal mail by our agents, archiving of physical records, contractors and external service providers.
- Carrying out securitisation arrangements (such as trustees, investors and the advisers).

Independent agents, brokers and business partners

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

Researchers

We are always looking for new insights to help you get 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 EEA

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:

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

- **Binding Corporate Rules**: for personal data transfers within ING Group, we also rely on binding internal Group policies (i.e. the Binding Corporate Rules) to ensure that ING entities located in non-adequate countries 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).

We may also rely upon, amongst others:
- the conclusion or the execution of an agreement, a transaction or a third-party transaction in your favour;
- requirements based on applicable local laws and regulations;
- the need to transfer the personal data for reasons of public interests;
- your explicit consent;
- the respect of international treaties.

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 third party or other ING entity to which we transfer data is located.

You may obtain a copy of the Standard Contractual Clauses and Binding Corporate Rules by contacting us using the contact details found in Section 12 below.

6. Automated decision-making and profiling

Automated decision-making is when we make decisions relying heavily on technological means (i.e. with minimal human involvement). Profiling involves the automated processing of personal data with a view to evaluating or predicting personal aspects such as the economic situation, reliability or likely behaviour of a person.

We currently do not take decisions which would affect you significantly without any human intervention in the process. However, since ING Luxembourg serves a wide

group of customers, it makes the use of automated decision-making and profiling imperative. Examples are:

Credit risk rating
When you apply for a loan or credit, we create a profile to assess whether you can meet your financial obligations to us and to ensure that we do not offer loans that are not suitable for you. We assess the risk connected to a contract with you via a method called credit scoring.
Your credit score is calculated based partly on automated decision-making. You have to achieve a pre-defined minimum score to ensure an acceptable risk for us.

The credit score is calculated mainly on your financial standing. If you already have or had a relationship with us in the past (taking into account applicable retention periods), we combine the external financial information with your internal payment history. This credit risk rating process relies on profiling as this concept is defined above.

Prevention of fraud and money laundering and terrorism financing
We are obliged to perform customer and transaction screening to detect potential and actual criminal activity. As a result, we pay particular attention to unusual transactions and to transactions that, by their nature, result in a relatively high risk of fraud, money laundering or terrorism financing. To do this we create and maintain a risk profile for you. If we suspect that a transaction is connected with money laundering or terrorist financing, we are obliged to report this to the authorities. This overall process involves some form of automated decision-making as this concept is defined above.

Examples of factors that we take into account that may indicate an increased risk of fraud or money laundering and terrorist financing are:

- Changes in a person's normal spending and payment behaviour, such as unexpectedly large amounts being transferred or debited.
- Payments to or from suspicious countries, stores or addresses.
- Two PIN payments by a single person in two vastly different locations at the same time.
- Being listed on an internal referral register. ING's internal referral register is a list of persons and institutions with whom we no longer want a relationship. They are a risk to ING, its staff and/or its customers. Only some employees of specific ING departments may have access to the details of the register, on a need-to-know basis.
- Being listed on any public national or international sanctions lists.

7. Your rights and how we respect them

If your personal data is processed, you have rights. If you have questions about which rights apply to you, please get in touch with us using the contact details mentioned in Section 12.

You have the following rights:

Right to access information: an overview of your personal data

You have the right to ask us for an overview and for a copy of your personal data that we process. That is called the 'Right to access'. The purpose of this right is that you can check whether your data is accurate and complete. Then you can adjust the data if necessary.

You can see many of these data when you log in on our website and online applications (like myING for retail customers). It is also possible to make the request using the contact details mentioned in Section 12. You will receive a standard overview of your personal data. If you are looking for particular personal data, please indicate this in your request. Otherwise you will receive the standard overview of your personal data.

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 Luxembourg using your personal data for its own legitimate interests if you have a justifiable reason. Please give a short explanation why you want to make use of this right. 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 for instance object to receiving commercial messages from us (by e-mail, mail and phone) or to have your personal data used for statistical purposes. Should you later change your mind, 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 or calling ING at 44.99.1.

Please note that, even if you opt out of receiving 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 object to significant solely automated decisions

You have the right to object to automated decisions taken without human intervention and which affect you significantly. If ING Luxembourg decides to take such automated decisions in the future, you may ask for an actual person to make the final decision.

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 to us 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 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 commercial messages;
- ING unlawfully processes your personal data; or
- applicable 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 Data Protection Officer of ING. You can also lodge a complaint with the Luxembourg Data Protection Authority (the *Commission Nationale pour la Protection des Données* or *CNPD*), located at L-4370 Belvaux, 15, Boulevard du Jazz (http://cnpd.public.lu)

Right to withdraw consent

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

Your rights and SWIFT

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 identification data (e.g. name, address), order data (e.g. account number of the ordering party and the beneficiary in the case of a payment order), details of the intended use 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 this section "Your Rights and how we respect them".

Separate controller

In certain cases, SWIFT can also act a separate controller (independent controller), when it comes to processing of your personal data for Statistical Analysis and Product development of SWIFT services and products. For these processes, SWIFT directly will handle all requests concerning the rights granted to data subjects. In this situation SWIFT can be contacted via opt.out@swift.com or privacy.officer@swift.com. However, ING will assist SWIFT in authenticating the ING client who has filed such a request by relying on the client identification information available to us; no further details would be shared with SWIFT in this scenario. You can find details about these processing activities and their purpose as well as contact details applicable for requests or complaints concerning them in the SWIFT Privacy Protection policy.

Exercising your rights

To exercise any of the rights as set out above, please contact us using the information indicated in Section 12 below.

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, the response times may vary. Should we require more time to complete your request, we will notify you immediately and provide reasons for the delay.

8. Are you obliged to provide us with your personal data?

In some cases, we are legally required to collect personal data or your personal data may be needed before we may perform certain services and provide certain products. We undertake to request only the personal data that is strictly necessary for the relevant purpose. Failure to provide the necessary personal data may cause delays or lead to refusal of certain products and services for instance loans or investments.

9. How long we keep your personal data

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 which we have processed it. Consequently, retention periods may depend on circumstances. When assessing how long to keep personal data, retention requirements might be stipulated by other applicable laws (for instance, anti-money laundering law). Personal data collected in the context of the conclusion or performance of an agreement can also be kept as evidence in litigation.

In many cases, this will be up to ten years after the end of our agreement or business relationship with you. 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. Other data collected by surveillance cameras are kept for shorter periods as required by law. 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.

10. 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.

11. 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 December 2025. The most recent version is available at www.ing.lu

12. Contact and questions

To learn more about ING's data privacy policies and how we use your personal data, you can primarily contact us through our usual channels by:

- Connecting to your My ING and send us a message with a reference to "Data Protection"
- Visiting your local branch, contacting your relationship manager, your personal or private banker

If you are a client of ING Luxembourg S.A.: contact ING via dpo.lu@ing.com referring to "Data Protection"

If you are a client of ING Lease Luxembourg S.A.: contact ING Lease via contact@lease.ing.lu referring to "Data Protection"

If you are a client of ING Solutions Investment Management S.A. (ISIM): contact ISIM via data.protection@ing-isim.lu referring to "Data Protection"

In case of disagreement or complaints related to the processing of your personal data, you can send us a request with "Data Protection" as reference via:

- Letter: Complaints Service, 26, Place de la Gare, L-2965 Luxembourg
- E-mail : complaints@ing.lu

If you did not obtain a satisfactory resolution of your case, you can submit a written request to the Data Protection Officer of ING via :
- E-mail: dpo.lu@ing.com
- Letter: Data Protection Office, 26, Place de la Gare, L-2965 Luxembourg.

You may also lodge your complaint with the Luxembourg Data Protection Authority (the *Commission Nationale pour la Protection des Données* or *CNPD)* which is located at L-4370 Belvaux, 15, Boulevard du Jazz (http://cnpd.public.lu).