Personal Data Protection Statement

1 July 2024

Personal data protection statement of ING Belgium NV/SA

Content

This is the Personal Data Protection Statement of ING Belgium NV/SA acting as data controller: ING Belgium NV/SA - Bank/Lender - Marnixlaan/Avenue Marnix 24, B-1000 Brussels - Brussels RPM/RPR – VAT BE 0403.200.393 - BIC: BBRUBEBB – IBAN: BE45 3109 1560 2789 – Insurance broker registered with the FSMA under the code number 0403.200.393 - www.ing.be - July, 2024.

ING Belgium NV/SA is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 (GDPR) and local personal data protection laws such as the Law on the Protection of natural persons with regard to the processing of personal data of 30/07/2018.

This is the Personal data protection Statement of ING Belgium NV/S.A. (“ING”, "ING Belgium", “we”, “us” and “our”), and it applies to us when we process Personal Data that belongs to individuals (“you”).

1. What are the purpose and the scope of this Statement?

At ING, we understand that your personal data is important to you. This Personal data protection 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 Personal data protection Statement applies to the following individuals (“you”):

- All past, present and prospective ING customers who are individuals. This includes one-person businesses.
- Anyone involved in any transaction with ING, whether it is in your personal capacity or as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, anyone that is a guarantor, ultimate beneficiary owner, etc.);
- Non-ING customers. These could include anyone that visits an ING website, branch or office, professional advisors, shareholders, family members (first degree), etc.

We obtain your personal data in the following ways:

- Directly, from you when you become a customer, register for our (online) services, complete an (online) form, sign a contract with ING, use our products and services, contact us through one of our channels or websites.
- Indirectly, from your organisation/employer (if it is an ING customer) when you may act as a representative or contact person of your organisation when it becomes a prospective customer or if it is an existing customer.
- From other available sources such as debtor registers (including the Central Individual Credit Register of the National Bank of Belgium (NBB)), land registers, 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, credit agencies, other financial institutions, commercial companies (e.g. LSEG that provides World-Check risk detection services), or public authorities.

Further information may be provided where necessary e.g. when you apply for a specific product or service.

We refer to our ING Cookie Policy as published on the ING website for more information about the use of cookies and similar technologies.

2. What types of personal data do we process?

A) Personal data

Personal data refers to any information that identifies or can be linked to a natural person. Personal data we process about you includes:

- **Identification data**: your name, date and place of birth, ID number, email address, telephone number, title, nationality and a specimen signature, fiscal code/social security number;
- **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, tax status, income and others revenues, 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 national or international sanctions (including US sanctions) and 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 or staff training purposes;
- **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.

B) Sensitive personal data

Sensitive personal data is personal data relating to your health, ethnicity, religious or political beliefs, genetic or biometric data or criminal data. We may process your sensitive personal data as set out below in Section 3 ("What do we do with your personal data?") if we have your explicit consent or when we are required or authorised to do so by applicable laws and regulations. For instance, we may process criminal data insofar as this is necessary for the management of our own disputes.

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. We may further process such data for example to verify the origin of the funds but only in the context of anti-money laundering and terrorism financing regulations.

C) Children´s personal data

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 applicable law.

In relation to the offer of information society services (for example, ING Banking) directly to a child under the age of 13, we would do so only if and to the extent that we have received authorization from the person holding parental responsibility.

Furthermore, we do not perform direct marketing aimed at children below the age of 12.

3. What do 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 process your personal data under one of the following legal grounds:

- To conclude and carry out our contract with you;
- To comply with our legal obligations;
- For our legitimate business interests. This data processing may be necessary to maintain good commercial relations with all our customers and other concerned parties. We may also process your data to prevent and combat fraud and to maintain the security of your transactions and of the operations made by ING;
- To protect your vital interests;
- When we have your consent. In this case, you may withdraw your consent at any time.

We may only process your personal data for the following purposes on basis of one of the following legal grounds:

A) 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 or manage some disputes that may arise 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 ING Banking/Home'Bank. We also use these account details to 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 and compatible purposes.

B) 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 a/an:

- **Integrity checks**: when entering into a customer relationship with you, we have a legal obligation (due to e.g. 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 to e.g. anti-money laundering and terrorism financing laws) to confirm your identity (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;
- **Credit checks**: Before entering into a customer relationship with you for the granting of a credit, 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 further detailed in Section 6 ("Do we make automated decisions and engage in profiling?"). Regarding overdraft facilities, we also have the legal obligation to assess your ability to reimburse the credit in the course of the contract;
- **Anti-money laundering and terrorism financing checks**: we have a legal obligation to check for potential money laundering and terrorism financing. This includes monitoring unusual transactions and sanctions lists as set out in Section 6 ("Do we make automated decisions and engage in profiling?");
- **Regulatory and statutory reports** to our regulators as set out in Section 4 ("Who do we share your personal data with and why?") and data requests from them;
- **Insider trading and market abuse control**: we monitor the transactions of ING Belgium staff members and other family members (within the first degree) within the framework of the applicable legislation.

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

C) 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 main purposes for which we process your personal data where we rely on legitimate interest:

1) Relationship management and marketing.

To the extent that the processing is necessary for the purposes of the legitimate interests pursued by us (unless your interests or fundamental rights and freedoms prevail), we may carry out, without obtaining your prior consent, the following processing:

o the processing relating to the promotion and offer of the best-suited products and services provided by us or other ING entities and/or of such products and services at a differentiated price or (credit or debit) interest rate.
We will process your personal data when informing or advising you (e.g. by e-mail, mail and phone)

about (similar) products and services from ING and when performing statistical purposes. Of course, if you do not want to receive these offers you have the right to object or to opt-out. We strive to understand you better and meet your changing needs by offering you services and/or price or interest rate that will suit your specific situation. To be able to provide you with tailor-made products and services and/or differentiated price or interest rate, we may:

- take into account your socio-demographic and financial situation (with the exclusion of your payment details);
- analyse your preferences in our various communications channels;
- analyse the products and services that you have already purchased from us.

We may also send you newsletters informing you about our activities. Of course, if you don't want to receive these newsletters you have the right to object.

o the processing relating to improvement and development of our products and services.
We may ask you for feedback about our 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.
Analysing how you use and interact with our products and services 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;
- Sometimes we analyse your personal data using automated processes, such as algorithms, to speed up credit decisions for loans and mortgages. On the basis of payment data or any other banking, financial or credit data, we may so predefine a maximum limit for the granting of credit in order to be able to respond rapidly to any request for credit from the data subject;
- 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 site.
- Unless this is not allowed according to applicable law, this can include recording your conversations with us, but we will always inform you about this beforehand.

o the processing relating to the communication of personalised information and offers ("personalised direct marketing") on the basis of payment data or other similar sensitive personal data (i.e. the use of such data for profiling purposes in the context of marketing), only to the extent that:

- such data is necessary to exclude individuals from marketing activities which are not considered appropriate for those individuals, based on semi-aggregated payment data (e.g. excluding customers from car insurance campaigns based on the absence of vehicle-related expenses, ...), or
- these data are necessary to prioritise marketing activities towards data subjects when the same person is the recipient of several marketing campaigns at the same time (except for the promotion of insurance services), based on a high level of categorisation of payment data (such as total amounts of incomes and expenses, total amounts of expenses on transport, at supermarkets, ...);

o the processing, carried out on the basis of payment data or any other banking, financial or credit data, to provide you with information on your past financial situation (incomes and/or expenses) (e.g. by providing an overview of the amounts spent per category: transport expenses, supermarkets, ...);

o the processing, carried out on the basis of payment data or any other banking, financial or credit data, to assess in advance whether you are eligible for certain products and services and, if so, to give you the opportunity to subscribe to them. For example, we may look at your payment behavior and credit history when you apply for a loan or a mortgage. We may also look at your payment data to show you which transactions are eligible for ING OneView services or ING Look Ahead services.

o the processing, carried out on the basis of payment data or any other banking, financial or credit data, 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 topic and/or take appropriate measures.

2) Business process execution, internal management, statistics and management reporting.

We process your data to ensure effective and efficient internal business process execution, 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. We will always choose aggregated data for this if we can, meaning that only information about groups of clients will be processed (so that you are not identifiable). This includes:

- analysing our market position in different segments;
- performing cost and loss analysis;
- training our staff for example by analysing recorded phone calls 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.

3) Safety and security.

We have a duty to protect your personal data and to prevent, detect and contain any breaches of your data. We not only want to protect you against fraud and cybercrime, we also have a duty to ensure the security and integrity of ING and the financial system as a whole.

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 respect, 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;
- As an entity of ING Group, we apply the American administrative sanctions lists, such as the OFAC list (Office of Foreign Assets Control of the US Treasury Department), both when entering into a relationship and when carrying out transactions;
- 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 an unusual location.

D) Protecting 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.

E) Respecting 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:

- promotional activities where we inform you about products and services from ING partners (such as these from our partners of ING +Deals).
- personalised marketing activities based on profiling performed on the basis of the analysis of your payments data.
  With your consent, we may send you letters, e-mails, or text messages 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.
- promotional activities on internet where we inform you about products and services based on your online behaviour. We may use your personal data when analysing your visit to our website with the aim of improving these. We use cookies and comparable technologies for this. For more information, we refer to our ING Cookie Policy as published on our website.

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

4. Who do 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.

A) Within ING Group

ING Belgium is part of ING Group which provides banking, financial, insurance or other services in over 40 countries. For more information about ING Group, please visit www.ing.com. ING Group is committed to your privacy.

Without prejudice to the legal provisions of public order, your personal data may be communicated to the other companies of ING group established in the European Union and carrying out banking, insurance, financial and/or other activities (list on request) for the purposes central customer management, marketing (except advertisements by e-mail and unless the person concerned un objects, upon request and free of charge, to direct marketing), global vision of the customer, provision of their services (the where applicable) and control of the regularity of transactions (including the prevention of irregularities).

ING Belgium may share your personal data with its parent company ING Bank N.V. (Bijlmerdreef 106, 1102 CT Amsterdam, The Netherlands) to ensure that ING Group is able to:

- 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 are specifically on an individual level 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 and that it can no longer be linked back to you;

- develop (also on behalf of ING Belgium) ING's internal credit models. Under EU banking rules, ING Group is obliged to develop these credit models to be able to calculate any counterparty risks and exposures. This allows 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 Belgium) ING's know your customer (KYC) models. To safeguard the ING Group against involvement in Financial Economic Crimes, KYC models are being developed on a group level for customer and transaction screening to detect potential or actual criminal activity. These KYC models incorporate mandatory requirements derived from the EU Directives and Regulations 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 Belgium also continues to strive to make its 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 Belgium will share your personal data with ING Group and other ING entities to centralize 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 fraud/KYC screening) or the processing of transactions have been centralised in processing centres, named ING Hubs located in countries such as Slovakia, Poland, Sri Lanka, Romania and the Philippines. These IBSS entities will process your data on behalf of ING Belgium;
- 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 Belgium 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 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.

B) With third parties

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

1) Government, supervisory and judicial authorities

We are obliged by law (to comply with our regulatory obligations) or we need (to defend ourselves) 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), National Bank of Belgium (NBB), the Financial Services and Markets Authority (FSMA)and the Federal Public Service Economy in Belgium;
- **Tax authorities** (including in the framework of the Foreign Account Tax Compliance Act (FACTA), the Common Reporting Standard (CRS) or the Law organising a Central Point of Contact for accounts and financial contracts) who 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 law;
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies (including at their express and legal request).

2) Other financial institutions and entities

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 superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

And we share information with business partners whose financial products we sell, such as insurance companies.

3) 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 (including customer satisfaction surveys);
- 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 advisors;
- 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).

4) Independent agents, brokers and business partners

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

5) 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.

A list of the main recipients and sources of your data (including an overview of the most important third-party service providers that will receive your personal data) is included under Section 13 of this Statement ("Supplement to the Personal data protection Statement of ING Belgium S.A.: Main recipients and sources of your data").

5. Under what conditions do we transfer 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 of 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, such as:

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

- **Binding Corporate Rules**; for personal data transfers within ING Group, we could 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 c as set out in Section 4 ("Who do we share your personal data with and why ?").

ING may also rely upon, amongst others:

- the respect of the EU-US Data Privacy Framework:
- 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;
- data transfer that are necessary 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 data importer is located.

6. Do we make automated decisions and engage in profiling?

Automated decision-making is when we make decisions by technological means without significant

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.

Since ING Belgium serves a wide group of customers, it makes the use of automated decision-making and profiling imperative. Examples are:

1) Credit risk rating
When you apply for a loan, a credit or a credit card, we create a profile to assess whether you can meet your financial obligations to us and to ensure that we do not offer loans, credits or credit cards 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 on automated decision-making. You have to achieve a pre-defined minimum score to ensure an acceptable risk for you and us.

The credit score is calculated mainly on your financial standing. Based on the personal data you provide in the credit-scoring process, we consult external credit (rating) registers (including the Central Individual Credit Register of the National Bank of Belgium) to acquire relevant financial information. 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. If you do not achieve the minimum score, the automated credit scoring will decline your application. In that case, we will not enter into an agreement with you since we consider the risks for you and us to be too high. You have the right to contest such automated decisions. We refer to section 7 on how to do this.

2) Prevention of fraud and money laundering and terrorism financing
We are obliged or we need to perform customer and transaction screening to detect potential an 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.

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. This ING's register is a list that includes persons and institutions who have committed fraud or otherwise pose a risk to the financial sector or 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 files on a need-to-know basis; Being listed on any public national or international sanctions lists.

7. What are your rights and how do we respect them?

If your personal data is processed, you have personal data protection rights. If you have questions about which rights apply to you, please get in touch with us, i.e. using the email address mentioned in Section 12 (“Contact and questions”).

You have the following rights:

A) Right of access

You have the right to ask us for an overview of your personal data that we process.

B) 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.

C) Right to object to processing

You can object to ING using your personal data for its own legitimate interests if you have a justifiable reason. We will consider your objection and whether processing your 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 conclude and fulfil a contract with you.

You can also object to receiving (personalised) commercial messages from us (e.g. by e-mail, mail and phone) or to have your personal data used for statistical purposes. When you become an ING customer, we may ask you whether you want to receive personalised commercial offers or information based on your payment data and other similar details. Should you later change your mind, you can choose to retrieve your consent of receiving these messages.

You can choose to opt out of receiving these (personalised) commercial messages by, amongst others:

- using the 'unsubscribe' link at the bottom of commercials e-mails;
- adapting your Personal data protection settings in your ING Home'Bank / Business'Bank or ING Banking;
- filling in our contact form on www.ing.be;
- calling ING +32.2.464.60.04;
- visiting www.robinsonlist.be/index.html and www.dncm.be (FR) subscribing to Robinson Mail and the "Do Not Call Me List".

In addition, even if you opt out of receiving commercial (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.

D) Right to object to automated decisions

You have the right not to be subject to decisions which may legally or significantly affect you and that were based solely on automated processing using your personal data. In such cases you may ask to have a person to make the decision instead.

Some of our decisions are however the result of automated processes for which you gave us explicit consent or these decisions are necessary to conclude or fulfil a contract with you (e.g. in relation to credit scoring as explained above). In both cases, after the automated decision being made, you may ask for human intervention and contest the resulting decision (e.g. automatic refusal of an online credit application, based on credit scoring).

Your right to object and to contest may be impeded if automated decisions are made for legal reasons.

E) 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.

F) 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 with 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 local law, we will transfer your personal data.

G) Right to erasure ('right to be forgotten')

You may ask us to erase your personal data. However, ING is sometimes legally obliged to keep your personal data. Your right to be forgotten is only applicable if:

- 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.

H) 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 response to your complaint, you can escalate it to the Data Protection Officer (DPO) of ING Belgium. You can also lodge a complaint with the Belgian Data Protection Authority: Rue de la presse/Drukpersstraat 35, 1000 Brussels. (website: www.dataprotectionauthority.be).

I) 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 do 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.

J) Exercising your rights

If you want to exercise your rights or submit a complaint, please use the below details for ING Belgium. For other ING Entities in other countries there is a list of contact information at the end of this Personal data protection Statement.

If you want to exercise your rights you can already access and amend some of your personal data when you log in on ING Home'Bank / Business'Bank or ING Banking.
If you have questions, want to know more about ING's data protection policies and how we use your personal data, you can primarily contact us through our usual channels by:

- logging on to our ING secure remote channels (via Home'Bank, via Business'Bank or via the ING Banking App, the chat room is available to you), and sending us a message with a reference to "Privacy",
- contacting your relationship manager, your personal or private banker,
- making an appointment at your nearest branch via the following contact form; or
- contacting us by phone: +32 464 60 02 (FR), +32 464 60 01 (NL), +32 464 60 04 (EN).

In case of requests to exercise your Personal data protection rights or in the event of complaints relating to the processing of your personal, you can also send us a request with a copy of your identity document and with "Privacy" as a reference via:

- E-mail: plaintes@ing.be / klachten@ing.be
- Letter: ING Customer Care Center, Cours Saint Michel /Sint-Michielswarande 60, B-1040 Brussels.

If you did not obtain a satisfactory resolution of your case or if you would like to receive further information about this Personal data protection Statement, you can submit a written request to the ING Data Protection Officer (DPO) via:

- E-mail: ing-be-PrivacyOffice@ing.com
- Letter: ING Privacy Office, Avenue Marnix / Marnixlaan 24, B-1000 Brussels.

If you would like more information or if you are not yet satisfied with our reaction, you have the possibility to obtain information and the right to lodge a complaint with the Data Protection Authority (e.g. via the website: www.dataprotectionauthority.be).

When exercising your right, the more specific you are with your request, the better we can assist. We may ask you for a copy of your ID, additional information to verify your identity, or for example, we may ask you to go to an ING branch to identify you correctly. In some cases, we may deny your request and, if permitted by law, we will also 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. In any case treating your request should not take longer than 1 month after receipt of your request. Should we require more time to complete your request, we will notify you immediately and provide reasons for the delay.

In certain legal cases, we may deny your request. If it's legally permitted, we will let you know in due course why we denied it.

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 do we keep your personal data?

We do not store your personal data longer than we need to for the purposes (as set out in Section 3 ("What do 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 (e.g. anti-money laundering law). Personal data collected in the context of conclusion or performance of an agreement can also be kept as evidence in litigation.

In most cases, the retention period will be 10 years after the end of our agreement (regarding your bank account) or business relationship with you or even up

to 30 years for your mortgage loan data. 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.

In addition, for the purposes of establishing credit risk models, your personal data relating to credit agreements are kept for a period of at least 20 years and (in particular for data relating to mortgages) for a maximum of 30 years after the end of these contracts. As far as possible, however, your data are pseudonymised or anonymised.

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 do 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 Statement

We may amend this Personal data protection Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created and published at the end of April 2024 and enters into force on 1st July 2024. The most recent version is available at ING.be.

12. Contact and questions

To learn more about how we protect and use your personal data or for other additional information, you may also consult Article 5 (Professional discretion) and Article 6 (Protection of personal data) of the General Regulations of ING Belgium or the specific provisions regarding the protection of personal data in your agreements with ING Belgium or in specific terms and conditions of ING Belgium, available at ING branches and on www.ing.be.

For any other question, feel free to contact the Data Protection Officer of ING Belgium (ing-be-PrivacyOffice@ing.com or ING Privacy Office, Avenue Marnix / Marnixlaan 24, B-1000 Brussels).

13. Supplement to the Personal data protection Statement of ING Belgium NV/SA: Main recipients and sources of your data

A) MAIN RECIPIENTS

Your data are processed by ING Belgium in confidential manner.

They shall not be shared with third parties for other reasons than those mentioned in point 4 of this Statement ("Who do we share your personal data with and why?").

A list of the main recipients can be found hereunder:

Persons designated by you

These persons can be:

- The beneficiaries of your payments;
- Your family members
- Organisations intervening upon your request, such as Ombudsfin, an insurance company, ...

Independent intermediaries and commercial partners

This concerns primarily independent agents and brokers offering ING Belgium's products and services.

Competent authorities

The main competent authorities receiving your personal data are the following:

- Communications to **judicial or administrative authorities** (including the Data protection authority, the tax authorities, ...), or an extrajudicial mediation service (in particular, Ombudsfin) or an association defending people's interests or a specific cause;
- Legal communications at the **Central Point of Contact** of the National Bank of Belgium (NBB);
- Legal communications to the **Central Individual and Corporate Credit Register** of the NBB;
- Communications to the **Basic Banking Service Chamber** within the FPS Economy, responsible for appointing a basic banking service provider within the framework of the basic banking service for businesses;
- Communications to public authorities or bodies in connection with combating fraud, with ING limiting itself to confirming whether or not a person is the holder of an account number, with the person's details and associated account numbers being communicated by the public authority or body concerned, notably:
  - Federal Pensions Service
  - National Social Security Office
  - FPS Finance
  - Federal Agency for Occupational Risks (FEDRIS)
  - National Office for Annual Vacations (ONVA)
  - Horeca Social and Guarantee Fund
  - Famiris, Fons and Famiwal
  - Ministry of the German-speaking Community, Ministry of Family and Social Affairs
  - Kind & Gezin
  - Walloon Agency for Health, Social Protection, Disability and Families (Aviq)
  - Iriscare (THAB)

Financial sector specialists and other service providers

We also call on various companies whose involvement is necessary or useful to achieve one of the purposes pursued by us. In doing so, these companies act in principle as subcontractors of ING Belgium (and/or in some cases also as (joint) controllers of the processing of your personal data).

They are:

- Financial sector specialists, or
- Other service providers.

a) Financial sector specialists

Financial sector specialists who also have a legal obligation to treat personal data with all due care are:

- **SWIFT SC/CV** (established in Belgium) for secure financial transaction message exchange whose data are stored in the United States and are subject to US law;
- **MasterCard Europe SA/NV** (established in Belgium) and **VISA Europe Limited** (established in the United Kingdom) for payments and credit transactions worldwide;
- **Card Stop** (service of equensWorldline) to block your debit or credit card (including the ING Card);
- **equensWorldline SE** (established in The Netherlands) for global credit transactions and equensWorldline Group companies in Morocco and India, which operate as subcontractors;
- **Euroclear NV/SA** (established in Belgium) for settlement / delivery of securities worldwide, for

domestic and international bond and equity transactions;
- **Gemalto** (established in France) for the personalisation of debit or credit cards (including the ING Card);
- **Payconiq** (established in Luxembourg) to facilitate payments with smartphone;
- **Isabel NV** (established in Belgium) for services via the Internet and the Zoomit service of Isabel:
- **Axepta BNP Paribas BENELUX NV/SA** (established in Belgium) for the provision of payment terminals to professionals;
- **Correspondent banking/financial institutions in foreign countries**;
- Clearing and settlement institutions for payments (**Centre d'Echange et de Compensation ASBL** ("CEC", established in Belgium), **Systèmes technologiques d'échange et de traitement SA** ("STET", established in France), EBA Clearing SA (established in France), etc.) and for financial instruments (NBB-SSS, Euroclear Belgium and Euroclear Bank, etc.);
- **Companies involved in the mobilisation of bank claims**;
- **Credit institutions, financial institutions and equivalent institutions** in connection with the disclosure of information or intelligence relating to money laundering or terrorist financing, including the (possible) transmission of information to the Financial Intelligence Processing Unit (FIPU);
- **Batopin SA/NV** (established in Belgium), the consortium created by the major Belgian banks to manage the ATM network and services;
- **Belgian Mobile Wallet NV/SA** (established in Belgium) for the provision of identification, authentication and digital signature services;
- The **other members affiliated to the Kube platform of Isabel SA/NV** (established in Belgium), a list of which is available on www.kube-kyc.be.
  Via this Kube platform, ING Belgium communicates the personal data of the legal representatives and ultimate beneficiaries owners (UBOs) of companies/corporations which are Clients of ING Belgium as well as those of self-employed persons who are Clients of ING Belgium, with the other above-mentioned members with whom these companies and self-employed persons are also Clients or wish to become Clients and which must also comply with the obligations of the anti-money laundering legislation or the legal obligations relating to the automatic exchange in connection with cross-border tax arrangements as mentioned in article 5.7 of the General Banking Regulations. The data thus communicated are those obtained during the customer acquisition process with ING Belgium as well as those subsequently updated with the latter;
- **Insurance companies authorised in Belgium** (for which ING is not acting as an intermediary) in connection with combating fraud, with ING limiting itself to confirming whether or not a person is the holder of an account number, with the person's details and associated account numbers being communicated by the insurance company concerned.

Please read the specific data protection policies/personal data protection statements of these specialists on their respective websites.

b) Service providers

Some specific personal data may be shared with service providers, such as:

Intragroup services
- The service of **ING Business Shared Services Bratislava** in Bratislava, Slovakia for payment and account-related transactions,
- The service of **ING Business Shared Services Manila** in Manila, Philippines for payment, credit and financial transactions (including the release of funds),
- The service of **ING Business Shared Services Bratislava** in Bratislava, Slovakia, **ING Business Shared Services Manila** in Manila, Philippines and **ING Business Shared Services Warschau** in Warsaw, Poland for the identification of clients and other persons concerned, as well as the control and surveillance of their activities (in the context of the fight against terrorism and money laundering),

Generic service providers
- The services of **Fircosoft SAS** (established in the United States) for the screening and monitoring of clients and transactions.
- IT services (including security) of suppliers such as **Unisys Belgium SA/NV** (established in Belgium), **Adobe** (established in Ireland), **Contraste Europe VBR** (established in Belgium), **Salesforce Inc.** (established in the US), **Ricoh Nederland B.V.** (established in the Netherlands), **Tata Consultancy Services Belgium SA/NV** (established in Belgium and India), **HCL Belgium SA/NV** (established in Belgium and India), **Cognizant Technology Solutions Belgium SA/NV** (established in Belgium and India), **ING Business**

Shared Services Warschau (established in Poland),
- The service of **Selligent SA/NV** and **Social Seeder SRL/BV** (established in Belgium) and, where applicable, **external call centres** (in particular, as part of surveys) for marketing activities,
- The services delivered by **B-Connected SA/NV**, **CXL SA/NV** and **N-Allo SA/NV** (both located in Belgium) in the context of the helpdesk calls (Digital Channel Private Individuals), concerning the support of the digital channels used by our Private customers,
- The security service of funds and securities of **Securitas SA/NV / Loomis Belgium SA/NV** (established in Belgium),
- The archiving service of your banking, financial or insurance data in paper or electronic form from **OASIS Group** in Turnhout in Belgium,
- The postal and correspondence management services of **BPost NV/SA**, **Exela NV/SA**, **Group Joos NV/SA**, **Mastermail SRL/BV**, **Omnilevel NV/SA** and **Speos NV/SA** (both located in Belgium),
- The services for the management of cookies on ING's electronic communication channels in Belgium ("third-party cookies"): **Adobe** (in the United States), **ADMO, Doubleclick Inc, Google Ireland Ltd** (in Ireland), **Facebook Ireland** Ltd (in Ireland), **Medallia Inc** (in the United States) and **Tiktok Information Technologies UK Ltd**. (established in the United Kingdom).

<u>Product of segment specific service providers</u>
- The service of **ING Business Shared Service Colombo** in Colombo, Sri Lanka for the management of wholesale banking credits,
- The service of **Finance Active SAS** (established in France) for the management of the active debt management platform for Institutional Clients,
- The service of management of the consumer credit and mortgage credit agreements of **Stater Belgium SA/NV** (established in Belgium),
- The services for managing payment and credit incidents by those who carry out an amicable consumer debt recovery activity and who, for this purpose, in accordance with Article 4, § 1 of the Law of 20 December 2002 on amicable consumer debt recovery, are registered with the Federal Public Service Economy, SMEs, Self-employed and Energy (list available on demand), such as the company **Fiducre SA**,
- The services for managing credits: **Opportunity SAS** (in France),
- The custody service of foreign financial instruments and the management of their "corporate actions":
  - for foreign securities:
    BNP Paribas securities services (Italy, Netherlands, France, Germany), ING Luxembourg (third party funds), Bank of New York Mellon (Central/Eastern Europe and Asia) , Brown Brothers Harriman (US markets and NN Funds issued in Luxembourg), UBS (Switzerland, Austria, Portugal, Denmark, Sweden, Norway, Finland, UK, Ireland, South Africa, Spain, Canada), CitiBank Luxembourg (South Africa), Clearstream banking Luxembourg (as international securities depositary for bonds).
  - o for domestic securities:
    National Bank of Belgium (securities depository for government bonds), Euroclear Belgium (Belgian shares, warrants), KBC (Belgian Linear bonds), RBC Dexia Investor Services (NN Funds issued in Belgium) and Delen Private Bank, Belfius, Deutsche Bank, Fortis Bank, Beo Bank, Credit Agricole, Argenta, Axa Bank, VDK Bank, Delta Lloyd (as top of the pyramid for cash certificates).

Insurances

Personal data may be transmitted as part of the conclusion or execution of an insurance contract to entities outside the ING Group which are established in a Member State of the European Union and in particular:
- **NN Non-Life Insurance N.V.,**
- **NN Insurance Belgium SA/NV,**
- **Aon Belgium S.R.L./B.V.,**
- **Inter Partner Assurance S.A./NV,**
- **AXA Belgium SA/NV,**
- **Cardif Assurance Vie S.A.** and **Cardif Assurances Risques Divers S.A.**,
- **Qover SA/NV,**
- And to their potential representatives in Belgium (in particular **NN Insurance Services Belgium SA/NV** for **NN Non-Life Insurance N.V.**) (list on request).

Other partners

Personal data may be transmitted to other partner companies of ING (e.g. **Bancontact Payconiq Company SA/NV** established in Belgium; list available on demand), which are established in a Member State of the European Union, for and on behalf of which ING offers products or services, in the event of the people concerned subscribing to these or showing an interest in them,

B) MAIN SOURCES

A list of the public and private bodies which are the main sources for your data can be found hereunder:

Public bodies

- the **Belgian National Register** and the **Belgian Social Security Crossroads Bank** (via the non-profit association Identifin) for identifying the Client and other people concerned in the event of distance contracts (in connection with combating terrorism and money laundering) or dormant accounts or safe-deposit boxes;
- **Checkdoc**(.be) for verifying Belgian identity documents;
- the **Belgian Official Gazette** (Moniteur Belge/Belgisch Staatsblad), for identifying legally incapacitated people and their representatives or even representatives of companies in connection with combating terrorism and money laundering. In order to identify the representatives of the companies for this purpose, ING systematically consults the Graydon Insights service of **Graydon Belgium SA/NV** (established in Belgium), and records in its database which centralises the data of the Belgian Official Gazette, the data of the representatives of all companies, whether clients or not, which are published in the annexes of the Belgian Official Gazette. In this database, only the data of companies which are ING customers or which have taken steps to open a relationship with ING Belgium are accessible to any ING collaborator;
- the **Belgian register of beneficial owners** ("UBO register") for identifying the beneficial owners of companies, non-profit associations, foundations, trusts and other legal entities similar to trusts in connection with combating terrorism and money laundering;
- the **Crossroads Bank for Enterprises** in connection with identifying the representatives of companies in connection with combating terrorism and money laundering;
- the **Central Individual and Enterprise Credit Register** of the National Bank of Belgium in connection with combating excessive debt,
- notably in connection with assessing the creditworthiness of the Client credited; the **Central Balance Sheet Office** held by the National Bank of Belgium, notably in connection with assessing the creditworthiness of the Client credited and in connection with combating terrorism and money laundering;
- the **Basic Banking Service Chamber**, within the FPS Economy, responsible for appointing a basic banking service provider within the framework of the basic banking service for businesses.
- **CADGIS**, notably to consult the Belgian land registry plan in connection with assessing the real estate offered as security by the person credited;
- the **Register of pledges** held by the FPS Finances;
- the mortgage registry held by the FPS Finances.
- the **Notary Deeds Database** (NABAN), under the responsibility of the Manager of the Notariële Aktebank (helf by the Royal Federation of Belgian Notaries);
- the **Database of statutes and powers of representation** (held by the Royal Federation of Belgian Notaries);
- the database of the **Flemish Agency for Energy and Climate** (VEKA) on energy performance certificates for the analysis of the application for a mortgage or for a credit for energy-efficient renovations;
- a database of the **Federal Public Service Finance** to retrieve certain data from the tax return of a self-employed credit applicant and his/her partner for the purpose of analysing his/her credit application;
- the **judicial or criminal authorities**, in connection with law enforcement (including in the event of seizures) or an **extrajudicial mediation service** (in particular, Ombudsfin) or an association defending people's interests or a specific cause.

Private bodies

- the World-Check risk detection service of **London Stock Exchange Group plc** (in the United Kingdom, collecting data both within and outside of the European Union) or of **Regulatory DataCorp Ltd**. (in the United Kingdom, collecting data both within and outside of the European Union), the services of **PricewaterhouseCoopers Belgium SC/CV** (in Belgium), **Deloitte Belgium** SRL (in Belgium), **Graydon Belgium SA** (in Belgium), **Swift SC/CV** (in Belgium), **Isabel NV** (in Belgium), **Morningstar Holland B.V.** (in the Netherlands), Internet search engines, press and other reliable sources in connection with combating terrorism and money laundering;
- The **other members affiliated to the Kube platform of Isabel SA/NV** (established in Belgium), a list of which is available on www.kube-kyc.be.
  Via this Kube platform, ING Belgium may receive the personal data of the legal representatives and ultimate beneficiaries owners (UBOs) of companies/corporations which are Clients of these other members as well as those of self-

employed persons who are Clients of these other members, from the other above-mentioned members provided that these companies and self-employed persons are also Clients of ING Belgium or wish to become Clients of ING Belgium, and this in order to also comply with the obligations of the anti-money laundering legislation or the legal obligations relating to the automatic exchange in connection with cross-border tax arrangements as mentioned in article 5.7 of the General Banking Regulations. The data thus communicated are those obtained during the customer acquisition process with these other members as well as those subsequently updated with these members;

- the financial information services of **Graydon Belgium SA**, Bel-first of **Bureau van Dijk Electronic Publishing SA**, **Dun & Bradstreet BV** (information about companies and their representatives, all in Belgium), the research services of **Foundation OpenStreetMap Ltd**. (in the United Kingdom) and other search engines in connection with marketing;
- the financial and commercial information services of **Moody's Investors Service Ltd** (in the United Kingdom), **Coface SA** (in France), **Creditsights Ltd** (in the United Kingdom) and **Bloomberg Ltd** (in the United States) in connection with identifying company representatives, granting and managing loans, marketing and asset management;
- the services of **Mitek Systems B.V.** (in the Netherlands) for the identification of the clients based on their picture, in the framework of our purpose of monitoring the regularity of transactions (including the prevention of irregularities);
- the simulation services of **Corporate Facility Partners B.V.** (in the Netherlands) and **Rocketestate SRL** (in Belgium) for the assessment of the energetic efficiency of buildings and the works required to improve it or the risks associated with the climatic impact (e.g. flood zones) when granting a related credit with ING Belgium.

For further details, please refer to the General Regulations (in particular, articles 5 and 6) on the website of ING Belgium S/NV:

https://assets.ing.com/m/6a745e7b85191fe4/GeneralRegulationsNewEN.pdf

Country	Contact details for Data Protection Officer within ING Entities	Data Protection Authority
Australia	customer.service@ing.com.au	OAIC- Office of the Australian Information Commissioner https://oaic.gov.au/
Belgium	ing-be-privacyoffice@ing.com or ING Privacy Office, Avenue Marnix / Marnixlaan 24, B-1000 Brussels	Data Protection Authority https://www.dataprotectionauthority.be/ Rue de la Presse 35 / Drukpersstraat 35, B-1000 Brussels
Bulgaria	Emil.Varbanov@ing.com	Commission for Personal Data Protection https://www.cpdp.bg/
China	dpochina@asia.ing.com	
Czech Republic	Dpo-cz@ing.com	Úřad pro ochranu osobních údajů https://www.uoou.cz
France	Dpo.privacy.france@ing.com	Commission Nationale Informatique et Libertés https://www.cnil.fr/fr
Germany	datenschutz@ing.de	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de/
Hong Kong	dpohongkong@asia.ing.com	PCPD- Privacy Commissioner for Personal Data, Hong Kong https://www.pcpd.org.hk/
Hungary	communications.hu@ingbank.com	Hungarian National Authority for Data Protection and Freedom of Information http://www.naih.hu/
Italy	privacy@ingdirect.it	Garante per la protezione dei dati personali www.gpdp.it www.garanteprivacy.it
Japan	dpotokyo@asia.ing.com	PPC – Personal Information protection Commission Japan https://www.ppc.go.jp/en/
Luxembourg	dpo@ing.lu	CNPD - Commission Nationale pour la Protection des Données https://cnpd.public.lu
Malaysia	dpomalaysia@asia.ing.com	PDP - Jabatan Perlindungan Data Peribadi http://www.pdp.gov.my/index.php/en/
Netherlands	privacyloket@ing.nl	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/
Philippines	dpomanila@asia.ing.com	National Privacy Commission https://privacy.gov.ph/
Poland	abi@ingbank.pl	Generalny Inspektor Ochrony Danych Osobowych http://www.giodo.gov.pl/
Portugal	dpo@ing.es	CNPD- Comissão Nacional de Protecção de Dados https://www.cnpd.pt
Romania	protectiadatelor@ing.ro	National Supervisory Authority for Personal Data Processing (ANSPDCP) http://www.dataprotection.ro/
Russia	Mail.russia@ingbank.com	The Federal Service for Supervision of Communications, Information Technology, and

		Mass Media (Roskomnadzor) https://rkn.gov.ru/
Singapore	dposingapore@asia.ing.com	PDPC- Personal Data Protection Commission Singapore https://www.pdpc.gov.sg/
Slovakia	dpo@ing.sk	Úrad na ochranu osobných údajov Slovenskej republiky https://dataprotection.gov.sk/uoou/
South Korea	dposouthkorea@asia.ing.com	
Spain	dpo@ing.es	Agencia Española de Protección de Datos https://www.agpd.es
Taiwan	70th floor, Taipei 101 Tower 7 XinYi Road, Sec. 5 11049 Taipei Taiwan	
Ukraine	dpe.offfice@ing.com	Personal Data Protection department of Ombudsman http://www.ombudsman.gov.ua
United Kingdom	ukdpo@ing.com	Information Commissioner's Office (ICO) https://ico.org.uk

ING Belgium SA/NV - Bank/Lender - Avenue Marnix 24, B-1000 Brussels - VAT BE 0403 200 393 – Brussels RPM/RPR –
BIC: BBRUBEBB – IBAN: BE45 3109 1560 2789 – www.ing.be - Contact us via ing.be/contact.
Insurance broker registered with the FSMA under the code number 0403200393.
Publisher: Sali Salieski, Avenue Marnix / Marnixlaan 24, B-1000 Brussels – 07/2024.