Personal data protection statement of ING Belgium NV/SA

1 July 2022

Contents

This is the Personal data protection Statement of ING Belgium NV/SA ("ING", "we", "us" and "our"), and it applies to us as long as we process personal data that belongs to individuals ("you")

1. Purpose and scope of this Statement

At ING, we understand that your personal data is important for 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. Our approach can be summarised as: the right people use 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, legal representatives or contact persons acting on behalf of our corporate customers.
- 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, etc.

We obtain your personal data in the following ways:

- You share it with us 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 visit our websites.
- From your organisation when it becomes a prospective customer or if it is an existing customer, and your personal data is provided to help us contact your organisation.
- 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, publicly available sources or other companies within ING or third parties such as payment or transaction processors, credit agencies, other financial institutions, commercial companies (e.g. Thomson Reuters that provides World-Check risk detection services), or public authorities.

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:** the 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;
- **Financial data,** such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, credit capacity, financial products you have with ING, whether you are registered with a credit register, payment arrears and information on your income;
- **Socio-demographic data**, such as whether you are married and have children. Where local law considers this sensitive data, we respect the local law;
- **Online behaviour and preferences data,** IP address of your mobile device or computer you use 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;
- **Know our customer data as part of customer due diligence and** to prevent fraudulent conduct or behaviour that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud;
- **Audio-visual data**; where applicable and legally permissible, we process surveillance videos at ING branches, or recordings of phone or video calls or chats with our offices. 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 Facebook, Twitter, Instagram and YouTube. We follow public messages, posts, likes and responses to and about ING on the internet.

B) Sensitive data

Sensitive data is data relating to your health, ethnicity, religious or political beliefs, genetic or biometric data, or criminal data (information on fraud is criminal data and we process it). We may process your sensitive data if:

- We have your explicit consent such as when you instruct us to make a payment. For example, if you submit a payment to a political party or religious institution, we will only process this data according to your instructions.

- We are required or allowed to do so by applicable local law. For example, we process sensitive data in connection with money laundering or terrorism financing monitoring: we monitor your activity and may report it to the competent regulatory authorities.

C) Children´s data (only applies to our retail customers)

We only collect data about children if they have an ING product or if you provide us with information about your own children in relation to a product you buy.

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;
- When we have your consent. In this case, you may withdraw your consent at any time.

We may process the data of our customers for the following purposes:

- **Administration.** For example, when you open an ING account we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport) and to assess whether we can accept you as a customer. We also need to know your postal, e-mail address or phone number to contact you.

- **Performing agreements to which you are a party or taking steps prior to entering into agreements.** We use information about you when you enter into an agreement with us, or we have to contact you. We could analyse information about you, including your payment details, 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 behaviour 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. And we use your account details when you ask us to make a payment or carry out an investment order.

- **Relationship management and marketing.** We may ask you for feedback about our products and services, or record your conversations with us online, by telephone or in our branches. We may share this with certain members of our staff to improve our offering or to customise products and services for you. We may send you

newsletters informing you about these products and services. Of course, if you don't want to receive these offers you have the right to object or to withdraw your consent.

- **Personalised marketing based on profiling**
  With your consent, we may send you letters, e-mails, or text messages offering you a product or service based on your personal profile (payment data or other similar details) or show you such an offer when you log in to our website or mobile apps. You may at any time unsubscribe from such personalised offers.

    - **Providing you with the best-suited products, services and marketing.** We may use your data for commercial activities, including processing which is necessary for developing and improving our products and/or services, customer service, segmentation of customers and profiling and the performance of (targeted) marketing activities. We do this to establish a relationship with you and/or to maintain and extend a relationship with you and for performing statistical and scientific purposes. You have the right to withdraw your consent or object to personalised direct marketing or commercial activities, including related profiling activities. Moreover, you can always unsubscribe from receiving personalised offers.

  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 also carry out, without obtaining your prior consent, the following processing :

    - **The processing relating to improvement and development of our products and services**. 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: . 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;.
    - **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, ...) ;

- **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,...).

- **For credit risk and behaviour analysis.** We use and analyse data about your credit history and payment behaviour to assess your ability to repay a loan, at the time of conclusion of the credit contract, but also in the course thereof, and – as the case may be – to contact you on this topic.

- **Business process execution, internal management, statistics and management reporting.** We process your data for our banking operations and to help our management make better decisions about our operations and services.

- **Safety and security.** We have a duty to protect your personal data and to prevent, detect and contain any breaches of your data. This includes data we are obliged to collect about you, for example to verify your identity when you become a customer. Furthermore, we not only want to protect you against fraud and cybercrime, we have also a duty to ensure the security and integrity of ING and the financial system as a whole by combatting crimes like money laundering, terrorism financing and tax fraud.
  - 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.
  - 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.
- **Protecting your vital interests.** We process your 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. We will only process your data necessary for the vital interests of another natural person if we cannot base it on one of the other purposes mentioned.

- **Compliance with legal obligations to which we are subject.** We process your data to comply with a range of legal obligations and statutory requirements.

For **legal entities banking customers** (e.g. companies, financial institutions, etc.):

Performing agreements to which you are a party or taking steps prior to entering into agreements. We may process the personal data of legal representatives proxies, ultimate beneficiaries owners (UBOs), and other intervenients such as contact person, guarantors, etc. for the following purposes:

- **Administration.** For example, when a legal entity client opens an ING account we are legally obliged to collect personal data of its representatives, proxies, guarantors and ultimate beneficiary owners (UBO), to verify their identity (such as a copy of their ID card or passport) and to assess whether we can accept you as a customer. We also need to know their professional post address, phone number and e-mail information to reach out to these persons;

- **Performing agreements to which our legal entities banking customers** are a party or taking steps prior to entering into an agreement with the customer, and to contact the customer when needed. If you are an individual providing a guarantee for the customer, or a beneficiary of payment instruments, we may use your personal data to enter into an agreement or execute a payment order in connection to our arrangements with the customer. We may verify your capacity and powers using trade registers or incumbency certificates;

- **Relationship management and marketing.** We may ask you as the representative of the customer to give us feedback on the products and services offered to the business client. We may send newsletters regarding new and existing products and services offered by ING. You may opt out of any communication at any time.
    - **Providing the best-suited products and services.** When you as the representative of a customer, visit our website, call our customer service centre, talk to an ING employee or visit a branch, we may gather information about the customer;
    - **Improving and developing products and services**. Analysing how products and services are used helps us understand more about our performance and shows us where and how we can improve our products and services;

- **Business process execution, internal management, statistics and management reporting.** We process personal data for our financial services operations and to help our management make better decisions about our operations and services;

- **Safety and security.** We have a duty to protect all personal data and to prevent, detect and contain a data breach or fraud involving personal data collected to comply with regulations against money laundering, terrorism financing and tax fraud. To safeguard and ensure the security and integrity of ING, the financial sector, clients and employees, we may:
    - process your personal data to protect your organisation´s assets from fraudulent activities, for instance in case your identity (e.g. username and password) is compromised. In this respect, we process behavioural data (linked to your use of a mouse, a keyboard, etc.).
    - use certain personal data (e.g. name, account number, age, nationality, IP address, etc.) for profiling to detect fraudulent activities and the actors behind it.
    - use your personal data to alert you in case we detect suspicious activities involving your business´s assets, for example a transaction is taking place from an unusual location;

- **Compliance with legal obligations to which we are subject.** We process personal data to comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation etc.). For example, know your customer (KYC) rules and regulations require ING to verify the identity before accepting you as a customer. Upon request from authorities, ING may report the transactions carried out by customers.

When processing is not compatible with one of above purposes, we ask for your explicit consent which you may withhold or withdraw at any time.

4. With whom do we share your personal data and for which reasons ?

To offer you the best possible services and remain competitive in our business, we share certain data internally i.e., with other ING businesses and externally (i.e., outside of ING) with third parties.

Whenever we share your personal data externally (i.e., outside of ING) with third parties in countries outside of the European Economic Area (EEA) we ensure the necessary safeguards are in place to protect it. In case of transfer to a country outside the European Economic Area whose local regime is considered as inadequate by the European Commission, ING relies 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.
- EU Model clauses, when applicable, we use standardised contractual clauses in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with GDPR.
- data transfer that are necessary for reasons of public interests;
- your explicit consent;
- the respect of international treaties.

A) ING entities

We transfer data across ING businesses and branches for various purposes (see section 'What we do with your personal data' for the full list). We may

also transfer data to centralised storage systems or to process it at a central point within ING for efficiency purposes.

B) Government, Supervisory and Judicial authorities and regulated professions

To comply with our regulatory obligations we may disclose data to the relevant government, supervisory and judicial authorities and regulated professions such as:

- **Public authorities, regulators** and **supervisory bodies** such as the central banks and other financial sector supervisors in the countries where we operate.
- **Tax authorities** may require us to report customer assets or other personal data such as your name and contact details and other information about your organisation. For this purpose, we may process your identification data such as social security number, tax identification number or any other national identifier in accordance with applicable local law.
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.
- **Lawyers,** for example, in case of bankruptcy, **notaries,** for example, when granting a mortgage, **trustees** who take care of other parties' interests, and **company auditors.**

C) Financial institutions

To process certain payment and withdrawal services, we may have to share information about the customer or its representative with another bank or a specialised financial company. We also share information with financial sector specialists who assist us with financial services, for instance, in the following cases:

- exchanging secure financial transaction messages;
- payments and credit transactions worldwide;
- processing electronic transactions worldwide;
- settling domestic and cross-border security transactions and payment transactions; or
- 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.

D) 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. 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 (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 like postal mail by our agents, archiving of physical records, contractors and external service providers; or
- carrying out securitisation arrangements (such as trustees, investors and the advisers).

E) Account information and payment initiation services within the EU

The revised EU Payment Service Directive (PSD2) allows you to instruct a third-party payment service provider (TPP) to retrieve account information or initiate payments on your behalf with respect to your accounts with ING. The TPP may do so only if you have given your explicit consent to those services.

When we receive a request from a TPP on your behalf, we are obliged to carry out the request for payment or account information, as requested.

Additionally you can also use the PSD2 services to manage your accounts with other banks through your ING channels or apps. You may use the ING app or channel to

- view account information of your current payment accounts with other banks;
- make online payments from your current payment account with other banks.

In this case, we will be the TPP and we may only offer these services if we receive your explicit consent. If you decide that you no longer want to use these PSD2 services, you can simply turn off the feature in the ING online environment.

F) Intermediaries and business partners

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

G) 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's 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. The personal data is shared on an aggregated level and the results of the research are anonymous.

A list of the main recipients and sources of your data is included under point 11 of this Statement ("Supplement to the Personal data protection Statement of ING Belgium S.A.: Main recipients and sources of your data").

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

We respect your individual rights to determine how your personal information is used. These rights include :

A) Right to access information

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 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 information has any undue impact on you that would require us to stop processing your personal data.

You may not however 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 commercial messages from us (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 offers (based on your payment data and other similar details).

Should you later change your mind, you can choose to opt out of receiving these messages by, amongst others:
▪using the 'unsubscribe' button at the bottom of each commercial e-mail;
▪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 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 (applicable to retail customers only)

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 information. 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 perform or fulfil a contract with you. In both cases, you may ask for human intervention and contest the resulting decision (e.g. automatic refusal of an online credit application).

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 the usage of your personal data if :

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

G) Right to erasure (also known as right to be forgotten)

You may ask us to erase your personal data. However, at times ING is 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 data for our own legitimate interests or for personalised commercial messages;
- ING unlawfully processes your personal data; or
- A local law requires ING to erase your personal data.

H) Right to complain

Should you as a customer or its 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 contact the Belgian Data Protection Authority: Rue de la presse, Drukpersstraat 35, 1000 Brussels. (website: www.autoriteprotectiondonnees.be).

I) Exercising your rights

If you want to exercise your rights or submit a complaint, please use the below details for ING Belgium. For other countries contact information there is a list 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:

- Connecting to your ING Home'Bank, Business'Bank or ING Banking and sending us a message with a reference to "Privacy",
- Visiting your local branch, contacting your relationship manager, your personal or private banker,
- Calling us +32.2.464.60.04, or
- Completing the online form on www.ing.be/contact with the reference "Privacy".

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 send us a request with "Privacy" as a reference via:

- E-mail: plaintes@ing.be / klachten@ing.be
- Letter: ING Complaint Management, Cours Saint Michel 60/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, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 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.autoriteprotectiondonnees.be).

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

We want to address your request as quickly as possible. 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.

6. 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.

7. How do we protect your personal data ?

We take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it's processed. We apply an internal framework of policies and minimum standards across all our business to keep your personal data safe. These policies and standards are periodically updated 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.

8. How long do we keep your personal data ?

We are only allowed to keep your personal data for as long as it's still necessary for the purpose we initially required 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 in this context can serve as evidence in litigation, but we will not use such personal data actively.
For instance, your data may be archived for up to 10 years after your bank account has been closed or even up to 30 years for your mortgage loan data. Other data, collected by surveillance cameras or call recordings are kept for shorter periods as required by law.

When your personal data is no longer necessary for a process or activity for which it was originally collected, we delete it, or bundle data at a certain abstraction level (aggregate), render it anonymous and dispose of it in accordance with the applicable laws and regulations.

9. 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 2022 and enters into force on 1st July 2022. The most recent version is available at ING.be.

10. Contact and questions

To learn more about ING's Personal data protection policies and how we use your personal data, you can send us an email, call us or visit your local branch or office.

11. Supplement to the Personal data protection Statement of ING Belgium S.A. 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 ("With whom do we share your personal data and for which reasons?").

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**, 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 **File of non-regulated registrations** of the NBB.
- 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
  - National Office for Annual Vacations (ONVA)
  - Horeca Social and Guarantee Fund
  - Famiris
  - Fons
  - Famiwal
  - Ministry of the German-speaking Community, Ministry of Family and Social Affairs
  - Kind & Gezin

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 and other service providers

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

- **SWIFT SCRL/CVBA** (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 SP/BV** (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** (established in Belgium) for global credit transactions and equensWorldline Group companies in Morocco and India, which operate as subcontractors,
- **Euroclear** (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** (established in Belgium) for services via the Internet and the Zoomit service of Isabel,

- **Axepta BNP Paribas 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), 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),
- 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, including:

- 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),
- The service of **ING Business Shared Service Colombo** in Colombo, Sri Lanka for the management of credits,
- The services of **Accuity Inc**. en **Fircosoft SAS** (established in the United States) for the screening and monitoring of clients and transactions.
- The service of **Finance Active SAS** (established in France) for the management of the active debt management platform for Institutional Clients,
- IT services (including security) of suppliers such as **Unisys Belgium SA/NV** (established in Belgium), **IBM Belgium SRL/BV** (established in Belgium), **Adobe** (established in Ireland), **Contraste Europe VBR** (established in Belgium), **Salesforce Inc.** (established in the US), **Ricoh Nederland BV** (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, Bisnode Belgium SA/NV** and **Social Seeder SRL/BV** (all 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** 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 **G4S 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** and **Speos NV/SA** (both located in Belgium),
- 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: **Cannock Outsourcing BV** (in the Netherlands), **Opportunity SAS** (in France) and **Flowcast Inc** (in the United States),
- 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).
- The services for the management of cookies on ING's electronic communication channels in Belgium ("third-party cookies"): **Adobe** (in the United States), **Relay42 BV** (in the Netherlands), **Webtrekk GmbH** (in Germany), **ADMO, Doubleclick Inc, Google Ireland Ltd** (in Ireland), **Facebook Ireland** Ltd (in Ireland), **Medallia Inc** (in the United States).

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 S.A./N.V.,**
- **NN Insurance Belgium S.A./N.V.,**
- **Aon Belgium S.R.L./B.V.,**
- **Inter Partner Assurance S.A./N.V.,**
- **AXA Belgium S.A./N.V.,**
- **Cardif Assurance Vie S.A./N.V.** and **Cardif Assurances Risques Divers S.A./N.V.,**
- And to their potential representatives in Belgium (in particular **NN Insurance Services Belgium SA/NV** for **NN Non-Life Insurance sa/nv**) (list on request).

Other partners

Personal data may be transmitted to other partner companies of ING (e.g. **Payconiq International S.A.** established in Luxembourg or **Payvision B.V.** established in the Netherlands; 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 **Moniteur Belge**, 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 Moniteur Belge, the data of the representatives of all companies, whether clients or not, which are published in the annexes of the Moniteur Belge. 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;
- the **File of non-regulated registrations** ("ENR") 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 **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;
- **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 (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 **Thomson Reuters Ltd.** (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 SCRL** (in Belgium), the services of **Deloitte Belgium** (in Belgium), the services of **Graydon Belgium SA** (in Belgium), **Dun & Bradstreet SA** (in Belgium), **Swift SCRL** (in Belgium), Internet search engines, press and other reliable sources in connection with combating terrorism and money laundering;
- the financial information services **of Graydon Belgium SA**, Bel-first of **Bureau van Dijk Electronic Publishing SA** (information about companies and their representatives), the postal address identification services of **Bisnode Belgium SA** (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), **Roularta Media Group SA** (in Belgium) **Coface SA** (in France), **Fitch Ratings Ltd** and **Creditsights Ltd** (in the United Kingdom), **Bloomberg Ltd** (in the United States) and **Inoopa NV** (in Belgium) in connection with identifying company representatives, granting and managing loans, marketing and asset management;
- the services "BehavioSec" of **Behaviometrics AB** (established in Sweden) in the context of combating fraud in the use of ING Belgium's electronic services.

For further details, please refer to the General Regulations on the ING Belgium S.A./N.V.
https://www.ing.be/static/legacy/SiteCollectionDocuments/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, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 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, Cours Saint-Michel 60, B-1040 Brussels – 07/2022.