Privacy Statement for ING Belgium nv/sa

Contents

1. About this Privacy Statement

This Privacy Statement of ING Belgium nv/sa (hereafter referred to as ING) aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following people:

- All past, present and prospective ING customers;
- Anyone involved in any transaction with ING, whether it's in your personal capacity or as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, etc.);
- Non-ING customers such as payees or the contact persons of corporate clients.

Personal data refers to any information that tells us something about you or that we can link to you. This includes your name, address, date of birth, account number, IP address or information about payments you've made from your bank account.

By **processing** we mean everything we can do with this data such as collection, recording, organisation, storage, adaptation, use, disclosure, transfer or erasure.

You share personal data with us when you:

- Become a customer;
- Register with our (online) services;
- Complete an (online) form;
- Sign a contract;
- Use our products and services; or
- Contact us through one of our channels.

We also use data that is legally available from public sources such as the Central Individual Credit Register of the National Bank of Belgium (NBB), commercial registers, media, or is legitimately provided by other companies within the ING Group or third parties such as Thomson Reuters that provides World-Check risk detection services.

2. The types of data we process about you

The personal data we process includes:

- **Identification data**, such as your name, surname, date and place of birth, ID number, e-mail address and the IP address of your computer or mobile device.
- **Transaction data**, such as your bank account number, deposits, withdrawals and transfers related to your account.
- **Financial data**, such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, your credit capacity, financial products you have with ING, whether you are registered with a credit register of the BNB, payment arrears and information on your income.
- **Socio-demographic data**, such as whether you are married and have children.
- **Your online behaviour and preferences data**, such as the IP address 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 ING branches, call centre or fill in an online survey.
- **Audio-visual data**, such as surveillance videos at ING branches or recordings of

phone calls to our customer service centres.

Sensitive data

We do not record sensitive data relating to your health, ethnicity, philosophical, political opinion, religion or beliefs, trade union membership unless it is strictly necessary. When we do it is limited to specific circumstances, for example if you instruct us to pay a membership fee to a political party.

Children´s data

We know how important it is for our customers that we protect their children´s data. We only collect data about children if they have an ING product or if you provide us with information about children in relation to a product you buy.

In relation to the offer of information society services (for example, ING Smart 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 do direct marketing to children that are below the age of 12.

3. What we do with your personal data

We only use 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 your data 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.
- **Product and service delivery**. We use information about you to assess whether you are eligible for certain products and services such as a current or savings account, mortgage, loan or investment.
- **Managing customer relationships**. We may ask you for feedback about our products and services and share this with certain members of our staff to improve our offering. We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you.
- **Credit risk and behaviour analysis**. For example, to assess your ability to repay a loan we apply specific statistical risk models based on your personal data.
- **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 and services**. When you visit our website, call our customer service centre or visit a branch we gather information about you. We analyse this information to identify your potential needs and assess the suitability of products or services. For example, we may suggest investment opportunities suited to your profile. We analyse your payment behaviour, such as large amounts entering or leaving your account. We assess your needs in relation to key moments when a specific financial product or service may be relevant for you, such as starting your first job or buying a home. We assess your interests based on simulations you participate in on our website.
- **Improving and developing products and services**: Analysing how you use our products and services helps us understand more about you and shows us where we can improve. For instance,
  - We use transactional data to gain understanding on how you use our services to improve them. When you open an account, we measure the time it takes until your first transaction to understand how quickly you are able to use your account.
  - We analyse data on transactions between you and our corporate customers to offer information services to our corporate customers or provide them advice on how they can make better use of ING's products and services. When ING processes personal data for this purpose, aggregated data may be made available to the corporate customer. A corporate customer cannot identify you from these aggregated data.
  - We analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns.
  - Sometimes we may use automated processes to analyse your personal data, for example we use an algorithm to speed up credit decisions for loans and mortgages.
- **Preventing and detecting fraud and data security**: We have a duty to protect your personal data and to prevent, detect and contain data breaches. We are also obliged to screen your transactions, for example to comply with regulations against money laundering, terrorism financing and tax fraud.
  - We may process your personal information to **protect you and your assets** from fraudulent activities, for example if you are the victim of identity theft, if your personal data was disclosed or if you are hacked.
  - We may use certain information about you for profiling (e.g. name, account number, age, nationality, IP address, etc.) to quickly and efficiently detect a particular crime and the person behind it.
  - We use contact and security data (such as card readers or passwords) to secure transactions and communications made via remote channels. We could use this data to alert you, for example when your debit or credit card is used in a non-typical location.
- **Internal and external reporting**: We process your data for our banking, credit and financial operations and to help our management make better decisions about our operations and services. We as well process your data to comply with a range of legal obligations and statutory requirements (for example credit, anti-money laundering and tax legislations).

4. Who we share your data with and why

To be able to offer you the best possible services and remain competitive in our business, we share certain data internally and outside of ING. This includes:

ING entities

We transfer data across entities of ING Group for operational, regulatory or reporting purposes, for example to screen new customers, comply with certain laws, secure IT systems or provide certain services. (See section 'What we do with your personal data' for more details). We may also transfer data to centralised storage systems or to process it globally for more efficiency.

Self-employed agents and brokers

We share information with self-employed agents and brokers who act on our behalf. These agents and brokers are registered in line with local legislation and operate with due permission of regulatory bodies.

Government authorities and regulated professions

To comply with our regulatory obligations we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering or to prevent excessive indebtedness.

In some cases, we are **obliged by law** to share your data with external parties, including:

- **Public authorities, regulators** and **supervisory bodies** such as the central banks of the countries where we operate.
- **Tax authorities** may require us to report your assets (e.g. balances of deposits, payment or savings accounts or holdings on an investment account). We may process your social security number or Tax Identification Number for this.
- **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.**

Financial institutions

When you withdraw cash, pay with your debit card or make a payment to an account at another bank, the transaction always involves another bank or a specialised financial company. To process payments we have to share information about you with the other bank or specialised financial company, such as your name and account number. We also share information with financial sector specialists who assist us with financial services like:

- Exchanging secure financial transaction messages;
- Payments and credit transactions worldwide;
- Processing electronic transactions worldwide;
- Settling domestic and cross-border security transactions and payment transactions.

Sometimes we share information with banks or financial institutions in other countries, for example when you make or receive a foreign payment. And we share information with business partners whose financial products we sell, such as insurance companies.

Service providers

When we use other service providers we only share personal data that is required for a particular assignment for the benefit of ING. Service providers support us with activities like:

- Designing and maintenance of internet-based tools and applications;
- Marketing activities or events and managing customer communications;
- Preparing reports and statistics, printing materials and designing products;
- Placing advertisements on apps, websites and social media.

Partnerships for innovation

We are always looking for new insights to help you get ahead in life and in business. For this, we may exchange personal data with partners like universities, who use it in their research, and innovators. The researchers we engage must satisfy the same strict requirements as ING employees. This personal data is shared at an aggregated level and the results of the research are anonymous.

In all of these cases, we ensure the third parties can only access personal data that is necessary for their specific tasks.

Communication of personal data in other countries

Whenever we share your personal data internally or with third parties in other countries, 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 amongst others on:

- The conclusion or the execution of an agreement, one of your transactions or a third-party transaction in your favour;
- EU Model clauses, which are standardised contractual clauses used in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with EU data protection law. We may provide you with a copy of these clauses upon request;
- Data transfer that are necessary for reasons of public interests;
- Your explicit consent;
- Privacy Shield framework that protects personal data transferred to the United States.

5. Your rights and how we respect them

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

Right to access information

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

Right to rectification

If your personal data is incorrect, you have the right to ask us to rectify it. If we shared data about you with a third party and those data are later corrected, we will also notify that party.

Right to object to processing

You can object to ING using your personal data for its own legitimate interests (for example, marketing). We will consider your objection and stop processing your data unless we assess that we have legitimate and imperious reasons that justify processing your data.

You can also object to receiving commercial messages from us (by e-mail, mail and phone) or 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 privacy settings in your ING Home'Bank / Business'Bank / Smart Banking;
- Filling in our contact form on www.ing.be ;
- Calling ING +32.2.464.60.04;
- Visiting http://www.robinsonlist.be/index.html and https://www.dncm.be/fr/ subscribing to Robinson Mail and the "Do Not Call Me List».

Even if you have opted out of receiving commercial messages, you cannot object to us processing your personal data:

- If we are legally required to do so;
- If it is necessary to fulfil a contract with you;
- If there are security issues with your account, such as when your card is blocked.

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 information. In such cases you may ask to have a person to make the decision instead.

Some of our decisions are 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.

Right to restrict processing

You have the right to ask us to restrict using your personal data for the period necessary to ING for its verifications if:

- You believe the information is inaccurate or we are processing the data unlawfully;
- You have objected to us processing your data for our own legitimate interests.

You have the same right if ING no longer needs the data, but you want us to keep it for use in a legal claim.

Right to data portability

You have the right to ask us to transfer some of your personal data directly to you or to another company. This applies to personal data we process by electronic means and with your consent or on the basis of a contract with you. Where technically feasible, we will transfer your personal data.

Right to erasure

Unless required by law, you may ask us to erase your personal data 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 (except for legitimate and compelling interests) or for commercial messages;
- ING unlawfully processes your personal data; or
- A law of the European Union or a member state of the European Union requires ING to erase your personal data.

Right to complain

Should you not be satisfied with the way we have responded to your concerns you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the Data Protection Officer (DPO) of ING Belgium. You can also contact the Belgian data protection authority.

Exercising your rights

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 / Smart Banking.

You can also exercise your rights by contacting us (see section 10).

We aim to respond to your request as quickly as possible. In some instances this could take up to one month. Should we require more time to complete your request, we will let you know how much longer we need 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. Your duty to provide data

There is certain information that we must know about you so that we can commence and execute our duties as a Bank, Lender or Insurance Intermediary and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this data we may not be able to open an account for you or perform certain banking, credit, financial and insurance activities.

7. How we protect your personal data

We apply an internal framework of policies and minimum standards across all our business to keep your data safe. These policies and standards are periodically updated to keep them up to date with regulations and market developments. More specifically and in accordance with the law, 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.

In addition, ING employees are subject to confidentiality and may not disclose your personal data unlawfully or unnecessarily.

8. What you can do to help us keep your data safe

We do our utmost best to protect your data, but there are certain things you can do as well:

- Install anti-virus software, anti-spyware software and a firewall. Keep them updated.
- Do not leave equipment and tokens (e.g. bank card) unattended.
- Report the loss of a bank card to ING and cancel the lost card immediately.
- Log off from online banking when you are not using it.
- Keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures.
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing e-mails requesting personal information.

9. How long 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. After this we look for feasible solutions, like archiving it.

When assessing how long to keep personal data, retention requirements might be stipulated by other applicable laws (e.g. anti-money laundering law). Kept personal data can serve as legal evidence in litigation, but we will not use such personal data actively.

Retention periods may depend on circumstances. For example, 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.

10. Contact us

If you have questions, want to know more about ING's data 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 Smart Banking (app) 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
- Sending us an e-mail to info@ing.be referencing "Privacy".

In case of disagreement or complaints related to the processing of your personal data, you can send us a request with "Privacy" as 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 Privacy Statement, you can submit a written request to the ING Data Protection Officer via:

- E-mail: ing-be-PrivacyOffice@ing.com
- Letter: ING Privacy Office, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 Brussels.

When you contact us we will have to identify you before carrying out your request. We may for example ask you to an ING branch to identify you correctly. You may be asked to provide us with a valid ID or passport.

You will find below a list of contact information for this Privacy Statement, as well as a list of data protection authorities in each country where ING operates.

11. Scope of this Privacy Statement

This is the Privacy Statement of ING Belgium n.v./s.a. acting as data controller, ING Belgium n.v/s.a. - Bank/Lender - 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 12381A. - www.ing.be - Publisher: Marie-Noëlle De Greef - Cours Saint-Michel 60, B-1040 Brussels. 05/18.

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created in May 2018 and enters into force on May 25th 2018. The most recent version is available at ING.be.

Country	Contact details for Data Protection Officer	Data Protection Authority
Australia	customer.service@ing.com.au	**Office of the Australian Information Commissioner (OAIC)** https://oaic.gov.au/
Belgium	ing-be-PrivacyOffice@ing.com or **ING Privacy Office, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 Brussels**	**Belgian Privacy Authority** Rue de la Presse 35/ Drukpersstraat 35, 1000 Brussels http://www.privacycommission.be
Germany		**Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** http://www.bfdi.bund.de
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 www.dataprotection.org
Luxembourg		**CNPD – Commission Nationale pour la Protection des Données** https://cnpd.public.lu
Netherlands	privacyloket@ing.nl	**Autoriteit Persoonsgegevens** https://autoriteitpersoonsgegevens.nl/
Philippines		**National Privacy Commission** https://privacy.gov.ph/
Poland	abi@ingbank.pl	**Generalny Inspektor Ochrony Danych Osobowych** http://www.giodo.gov.pl/
Romania	dpo@ing.ro	**National Supervisory Authority for Personal Data Processing (ANSPDCP)** http://www.dataprotection.ro/
Slovakia	dpo@ing.sk	**Úrad na ochranu osobných údajov Slovenskej republiky** https://dataprotection.gov.sk/uoou/
Spain	dpo@ing.es	**Agencia Española de Protección de Datos** https://www.agpd.es

12. Supplement to the Privacy Statement of ING Belgium S.A.

Competent authorities

The following competent authorities receive personal data :

- Legal communications to **judicial or administrative authorities**,
- 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.

Financial sector specialists

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 SPRL/BVBA** (established in Belgium) and **VISA Europe Limited** (established in the United Kingdom) for payments and credit transactions worldwide,
- **Card Stop** (service of Worldline) to block your bank card,
- **Atos Worldline / EquensWorldline** (established in Belgium) for global credit transactions and Atos 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 bank cards,
- The **Payconiq** (Luxembourg) to facilitate payments with smartphone,
- **Isabel** (Belgium) for services via the Internet and the Zoomit service of Isabel,
- **INGenico** (Belgium) for the provision of payment terminals to professionals,
- **SIA** (established in Italy) for the authorization of transactions and the provision of credit card statement information,
- Correspondent banking/financial institutions in foreign countries

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

Service providers

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

- The risk detection service World-Check of **Thomson Reuters Ltd.** (established in the United Kingdom that collects data in and outside the European Union) or **Regulatory DataCorp Ltd.** (established in the United Kingdom collecting data in and outside the European Union);
- The services of **Graydon Belgium SA/NV, Dun & Bradstreet, Swift SCRL/CVBA**, Internet search engines, press and other reliable sources on counter-terrorism and anti-money laundering,

- The financial information services of **Graydon Belgium SA/NV**, Bel-first of **Bureau van Dijk Electronic Publishing SA/NV** (Belgium) (information on companies and their representatives) and **OpenStreetMap** in the context of marketing,
- The financial and commercial information service of **Coface SA/NV** (France), **Roularta Media Group SA/NV** (Belgium) and the service of **Bloomberg Ltd** (established in the United States) and **Fitch Ratings Ltd** (established in the United Kingdom) for the identification of company representatives,
- The service of **ING Business Shared Services Bratislava** in Slovakia for payment and account-related transactions,
- The service of **ING Business Shared Services Manila** in Manila, Philippines for payment, credit and financial transactions,
- IT services of suppliers such as **Unisys Belgium SA/NV**, **IBM Belgium SPRL/BVBA**, **Adobe** (established in Ireland), **Contraste Europe VBR** (established in Belgium), **Salesforce Inc.** (established in the US), **Ricoh Nederland BV** (established in the Netherlands), **Fujitsu BV** (established in the Netherlands), **Tata Consultancy Services Belgium SA/NV** (established in Belgium and India), **HCL Belgium SA/NV**, **Cognizant Technology Solutions Belgium SA/NV**, **Getronics BV** (established in the Netherlands), **ING Tech Poland** (established in Poland),
- The service of **Selligent SA/NV**, **Bisnode Belgium SA/NV** et **Social Seeder SPRL/BVBA** (all established in Belgium) and, where applicable, external call centers (in particular, as part of surveys) for marketing activities,
- The security service of funds and securities of **G4S SA/NV** / **Loomis Belgium SA/NV** (in Belgium),
- The archiving service of your banking, financial or insurance data in paper or electronic form from **OASIS Group** in Thurnhout in Belgium,
- The service of management of the consumer credit and mortgage credit agreements of **Stater Belgium SA/NV** (in Belgium),
- The custody service of foreign financial instruments and the management of their «corporate actions»: custodians, in particular **Clearstream** (in Luxembourg), the National Bank of Belgium, **Euroclear** (in Belgium), **BNP Paribas SA/NV** (in France), **ING Luxembourg SA/NV** (in Luxembourg).

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.P.R.L./B.V.B.A.,**
- **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).

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