Privacy Statement for ING customers

EU version - May 2018

Contents

1. About this Privacy Statement

This Privacy Statement 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. We are legally obliged to retain personal data about you, also for a certain period once the relationship has ended, in compliance with 'know your customer' regulations.
- Anyone involved in any transaction with our bank, 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 collecting it, recording, storing, adjusting, organising, using, disclosing, transferring or deleting.

You share personal information 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 debtor registers, land registers, commercial registers, registers of association and the media, or is legitimately provided by other companies within the ING Group or third parties such as credit agencies.

2. The types of data we collect about you

The personal data we collect includes:

- **Identification data**, such as your name, surname, date and place of birth, ID number, email address and the IP address of your PC 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, 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
- **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 to your interests and needs** that you share with us, for example when you contact our 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, religious or political beliefs 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. We are legally obliged to keep a copy of your passport.

Children´s data

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.

3. What we do with your personal data

We only use your personal data for legitimate business reasons. This includes:

- **Administration**. 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 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**. To assess your ability to repay a loan we apply specific statistical risk models based on your personal data.
- **Personalised marketing**. We may send you letters, emails, or text messages offering you a product or service based on your personal circumstances, or show you such an offer when you log in to our website or mobile apps. . You may unsubscribe from such personalised offers. You have the right, not to consent or to object to personalised direct marketing or commercial activities, including profiling related to these activities.
- **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,
  - 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.
  - we may use your data to send you personalised offers by post, email or on our website or mobile apps. You have the right to object at any time to personalised direct marketing or commercial activities, including profiling related to these activities.
- Preventing and detecting fraud and data security: We have a duty to protect your personal data and to prevent, detect and contain data breaches. This includes information we are obliged to collect about you, 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 operations and to help our management make better decisions about our operations and services. To comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation, for example).

Data that we process for any other reason is anonymised or we remove as much of the personal information as possible.

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 ING businesses and branches 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 the full list). We may also transfer data to centralised storage systems or to process it globally for more efficiency. All internal data transfers are in line with our Global Data Protection Policy.

Independent agents

We share information with independent agents who act on our behalf. These agents are registered in line with local legislation and operate with due permission of regulatory bodies. You can read more about how we work with these agents at https://www.ing.com/en.htm and in the relevant terms and conditions for your banking product.

Government authorities

To comply with our regulatory obligations we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering. 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 on deposit, payment or savings accounts or holdings on an investment account). We may process your social security 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, 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. Service providers support us with activities like:
- performing certain services and operations
- 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.

Researchers
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.

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. For this, ING relies on:
- Binding Corporate Rules as defined in EC Regulation (EU) 2016/679. These are known as the ING Global Data Protection Policy (GDPP) and have been approved by the data protection authorities in all EU member states.
- 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.
- Privacy Shield framework that protects personal data transferred to the United States.

5. Your rights and how we respect them

We respect your rights as a customer 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 ask us to rectify it. If we shared data about you with a third party that is 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. You can do this online, at a branch or by telephone. We will consider your objection and whether processing your information has any undue impact on you that requires us to stop doing so.

You can also object to receiving personalised commercial messages from us. When you become an ING customer, we may ask you whether you want to receive personalised offers. Should you later change your mind, you can choose to opt out of receiving these messages by using the **'unsubscribe' link** located at the bottom of each commercial email.

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; even if you have opted out of receiving personalised commercial messages.

Right to object to automated decisions
We sometimes use systems to make automated decisions based on your personal information if this is necessary to fulfil a contract with you, or if you gave us consent to do so. You have the right to object to such automated decisions (for example the price we charge for a product or service) and ask for an actual person to make the decision instead.

Right to restrict processing
You have the right to ask us to restrict using your personal data if:
- you believe the information is inaccurate
- we are processing the data unlawfully
- ING no longer needs 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.

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.

Right to erasure
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 or for personalised 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 ING Bank Data Protection Officer. You can also contact the data protection authority in your country.

Exercising your rights
If you want to exercise your rights or submit a complaint, please contact us. There is a list of contact details for the ING office in your country at the end of this Privacy Statement. How you exercise your rights depends on your ING product and the availability of services in your country. It could be through our website, by visiting a branch or by telephone. We aim to respond to your request as quickly as possible. In some instances this could take up to one month (if legally allowed). 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 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 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 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 to protect your data, but there are certain things you can do too:
- 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 emails 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.

10. Contact us

If you want to know more about ING's data policies and how we use your personal, you can send us an email, call us or visit your local branch. There is a list of contact information at the end of 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 Bank N.V. and its group companies (hereafter referred to as 'ING'). It applies to all entities and branches of ING to the extent that they process personal data.

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 on 1 May 2018. The most recent version is available on ING.com, as well as on the local ING websites in each country where we operate.

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	klachten@ing.be	Belgian Privacy Commission 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

ING