Privacy Policy
for
ING customers

(version 2.1)

Table of contents

1. The purpose and scope of this Privacy Policy 3
2. Types of personal data that we process 3
3. What we do with your personal data 5
4. Who do we share your personal data with and why? 8
5. Your rights and how they are respected 10
6. Your obligation to provide data 13
7. How we protect your personal data 13
8. Amendments to this Privacy Policy 13
9. Contact and questions 13

ING Bank N.V. is a European financial institution that is subject to data protection obligations under EU Regulation 2016/679 – General Data Protection Regulation (GDPR). In order to comply with the requirements set out in the GDPR, ING Bank N.V. has implemented common data protection rules under the Global Data Protection Policy (GDPP). The Global Data Protection Policy is binding upon all ING entities, subsidiaries, branches, representative offices and affiliates worldwide, and has been approved by the data protection authorities of the European Union. In view of the foregoing, and in addition to the requirements imposed by local privacy laws and regulations, ING Bank N.V. has decided that all its entities, subsidiaries, branches, representative offices and affiliates worldwide must comply with the GDPP, regardless of the place of their operation, the typology of the market they operate in, and their target customers.

This document comprises the Privacy Policy of ING Bank N.V., all its entities, subsidiaries, branches, representative offices, affiliates and other ING group companies ("ING", "we", "us" and "our", etc.) and shall apply to us if we process Personal Data belonging to natural persons ("you").

1. The purpose and scope of this Privacy Policy

ING is aware that personal data are important to you. This Privacy Policy explains – in a simple and clear way – what personal data belonging to you we collect, record, retain, use and process, and how we do it. Our approach to this issue can be summed up as follows – the right people use the right data for the right purpose.

This Privacy Policy applies to:

- all former, current and potential ING customers who are natural persons (to "you"). This also applies to sole proprietorships, legal representatives or contact persons acting on behalf of our corporate customers;
- persons other than ING customers. This may include any person who makes a payment or receives a payment from an ING account, a person who visits an ING website, branch or office, a professional consultant, a shareholder, a person who is a guarantor, an ultimate beneficial owner, a member of management or representative of a company that uses our services, a debtor or tenant of our customer, or a person involved in other transaction conducted with us or our customers.

We obtain your personal data in the following way:

- you provide them to us when you become our customer, sign up to use our online services, fill out an online form, sign a contract with ING, use our products and services, contact us via one of our communication channels or visit our websites;
- from your organization when it becomes our potential customer or when it is already our customer, and your personal data are provided to us to facilitate contact with your organization;
- from other available sources, e.g. debtor registers, land registers, commercial registers, registers of associations, online or traditional media, publicly available sources, other companies within ING or third parties, e.g. entities processing payments or transactions, credit rating agencies, other financial institutions, commercial law companies or public authorities.

2. Types of personal data that we process

Personal data include any information that enables the identification of a natural person or may be associated with such a person. Your personal data that we process include the following:

For Retail Banking customers:

- **identification data:** full name, date and place of birth, ID number, e-mail address, telephone number, title, nationality and specimen signature, tax identification number/social security number;
- **transaction data**, such as your bank account number, any deposits, withdrawals and transfers made to or from your account, and information on when and where they were made;
- **financial data**, such as invoices, credit notes, payslips, payment behaviour, the value of your real property or other assets, your credit history, creditworthiness, financial products you hold with ING, whether you are listed in the debt register, any arrears in payment and information about your income;
- **socio-demographic data**, such as whether you are married, and whether you have children. If local law considers such data to be sensitive data, we comply with the requirements of local law;
- **data on online behaviour and preferences**, such as the IP address of the mobile device or computer you use and the pages you visit on ING websites and applications;
- **data on your interests and needs** that you share with us, for example by contacting our call centre or completing an online questionnaire;
- **data related to the Know Your Customer (KYC) process, collected as part of customer due diligence procedures** and to prevent fraudulent practices or behaviour contrary to international sanctions, and to comply with laws intended to prevent money laundering, terrorist financing and tax fraud;
- **data in audio-visual form** – if applicable and lawful, we process recordings from surveillance cameras at ING branches or recordings of telephone conversations, video conferences or chats with employees of our offices. We use these recordings, for example, to verify orders placed over the telephone to prevent fraud or for staff training purposes;
- **Your interactions with ING on social media** such as Facebook, Twitter, Instagram, Google+ and YouTube. We track online public messages, posts, likes and reactions to the content posted by ING and about ING.

For Wholesale Banking customers:

- **identification data:** such as full name, date and place of birth, ID number, e-mail address, telephone number, title, nationality and specimen signature, tax identification number/social security number;
- **financial data** – if you provide us with a surety for a customer, we may verify your credit history, creditworthiness and other information related to your creditworthiness and credit conditions;
- **data on online behaviour and preferences**: such as the IP address of your mobile device or computer, and the pages you visit on ING websites and applications;
- **data on customer's interests and needs** that you share with us, by contacting our employees or completing an online ING questionnaire;
- **data related to the Know Your Customer (KYC) process, collected as part of customer due diligence procedures** and to prevent fraudulent practices or behaviour contrary to

international sanctions, and to comply with laws intended to prevent money laundering, terrorist financing and tax fraud;
- **data in audio-visual form** – if applicable and lawful, we process recordings from surveillance cameras at ING branches or recordings of telephone conversations, video conferences or chats with employees of our offices.

Sensitive data

Sensitive data include data concerning your health, ethnic origin, religious or political beliefs, genetic or biometric data or data related to crimes (data about crimes include information about fraud and we record such data). We may process your sensitive data if:

For Retail Banking customers:
- we obtain your express consent;
- we are required or authorized to do so by applicable local law. For example, we may be required to retain a copy of your passport or identity card if you become an ING customer;
- you instruct us to make a payment, e.g. to a political party or religious organization.
- If permitted under applicable local law and you choose this option, we may use your facial image, fingerprint or voice to verify your identity to enable you accessing mobile applications and making certain operations within such applications.

For Wholesale Banking customers:
- we obtain your express consent;
- we are required or authorized to do so by applicable local law; or
- you provide us with sensitive data as part of a contract or in connection with the product or service you want to obtain.

For example, we process sensitive data in connection with:
- obligations related to data covered by Know Your Customer (KYC) procedures – we may retain a copy of your passport or ID card if applicable under local law;
- the monitoring of activities related to money laundering or terrorist financing – we monitor your activities and may report them to the competent regulatory authorities; and
- if permitted under applicable local law and you choose this option, we may use your facial image, fingerprint or voice to verify your identity to enable you accessing mobile applications and making certain operations.

Data regarding children (only for Retail Banking customers)

We only collect data regarding children if they have an ING product or if you provide us with information about your children in connection with a product you buy. We obtain parental consent if required by local law.

3. What we do with your personal data

Processing means any action that may be taken in relation to personal data, such as collecting, recording, retaining, altering, organizing, using, disclosing, transferring or deleting such data in accordance with applicable law. We use your personal data only for business purposes, such as:

For Retail Banking customers:

- **performance of contracts to which you are a party or taking pre-contractual actions**: we use information about you, e.g. your name and contact details if you enter into a contract with us or we need to contact you. We analyse information about you to determine whether you qualify for certain products and services. For example, if you apply for a cash loan or mortgage loan, we may analyse your payment behaviour and credit history. We also use information about your account when you instruct us to make a payment or place an investment order with us;
- **relationship management and marketing**: we may ask you for your opinion about our products and services or record conversations we have with you online, over the telephone or at our branches. We may share them with some of our employees to improve our offer or tailor products and services to your needs. We may send you newsletters to inform you about such products and services. However, if you do not wish to receive such offers, you have the right to object or withdraw your consent;
    - **providing the best tailored products, services and marketing**: we may use your data for commercial activities, including processing that is necessary to develop and improve our products and/or services, customer service, customer segmentation and profiling, and to increase efficiency of the (target) marketing activities. We undertake these activities to establish and/or maintain and expand our relationship with you, and for statistical and scientific purposes. You have the right to withdraw your consent to receive personalized direct marketing or commercial activities, including profiling related to such activities, or to object to them. In addition, you can always choose not to receive personalized offers;
    - **improving and developing products and services**: analysing how you use our products and services and how you interact with our products and services helps us better understand you and find out where we could make improvements and how. For example:
        - if you open an account, we measure the time after which you are able to use it;
        - we analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns;
        - sometimes we analyse personal data using automated processes, e.g. we use algorithms to speed up credit decisions for cash loans and mortgage loans;
    - **credit risk and credit behaviour analysis**: we use and analyse data about your credit history and payment behaviour, e.g. to assess your ability to repay a loan;
- **business processes, internal management and management reporting**: we process your data in the area of our banking operations, and also to help our management team make better decisions related to our business and our services;
- **security**: it is our responsibility to protect your personal data, and to prevent, detect and contain data breaches. This applies to data that we are required to collect about you, e.g. to

verify your identity when you become our customer. In addition, we not only want to protect you from fraud and cybercrime, but we are also committed to maintaining the security and integrity of ING and the entire financial system by fighting crimes such as money laundering, terrorist financing and tax fraud.
    - This is aimed at protecting your assets from fraudulent activity on the Internet, for example if your device is hacked and your username and password are compromised.
    - We may use certain information about you (e.g. full name, account number, age, nationality, IP address, etc.) for profiling to detect fraudulent activities and their perpetrators.
    - We may use your personal data to alert you if we detect suspicious activity on your account, for example if your debit or credit card is used in an unusual location;
- **protection of your vital interests**: we process your data if it is necessary to protect your vital interests that are of key importance to your life or the life of another natural person. Examples include emergencies requiring medical attention. We will process your data that are necessary to pursue the vital interests of another natural person only if such processing cannot be carried out on the basis of other listed purposes;
- **compliance with our legal obligations**: we process your data to comply with a number of legal obligations and statutory requirements.

For Wholesale Banking customers:

- **performing contracts to which you are a party or taking pre-contractual actions**: if you are a representative of a corporate customer, we may use your personal data to conclude a contract with such a customer and contact them, if necessary. If you are a natural person providing a surety for a customer or beneficiary of payment instruments, we may use your personal data to conclude a contract or execute a payment order in connection with our arrangements with the customer. We may verify your rights on the basis of commercial registers or certificates containing a list of current shareholders;
- **relationship management and marketing**: we may ask you, as the customer's representative, to express your opinion on the products and services offered to that corporate customer. We may send newsletters about new and existing products and services offered by ING. You may opt out of any such communications at any time;
    - **providing the best tailored products and services**: we may collect information about the customer when you, as a customer representative, visit our website, call our customer service centre, talk to an ING employee or visit our branch;
    - **improving and developing products and services**: analysing how customers use our products and services helps us better understand the results we achieve and see where we could make improvements and how;
- **business processes, internal management and management reporting**: we process your personal data in the area of our financial operations, and also to help our management team make better decisions related to our business and our services;
- **security:** we have a duty to protect all personal data and to prevent, detect and counteract breaches of personal data protection or fraud related to collected personal data in order to comply

with anti-money laundering, terrorist financing and tax fraud regulations. In order to protect and ensure the security and integrity of ING, the financial sector, customers and employees, we may:

  - process your personal data to protect your organization's assets from fraudulent activities, e.g. where your identity is disclosed (e.g. username and password);
  - use certain personal data (e.g. full name, account number, age, nationality, IP address, etc.) for profiling to detect fraudulent activities and their perpetrators;
  - use your personal data to alert you if we detect suspicious activity involving your company's assets, for example a transaction taking place in an unusual location;
- **compliance with our legal obligations:** we process personal data to comply with a number of legal obligations and statutory requirements (arising from statutory tax or anti-money laundering regulations, etc.). Examples include the KYC rules and regulations which require ING to verify your identity before accepting you as our customer. ING may report customer transactions upon request received from competent authorities.

If the processing is not based on one of the above purposes, we ask for your express consent which you may withhold or withdraw at any time.

Applicable law requires us to retain personal data for a certain period of time. The period of personal data retention may vary from several months to several years depending on applicable local law. If your personal data are no longer needed for the process or activity for which they have been originally collected, we delete you data or combine them with other data on some abstract (aggregated) level, anonymize and dispose of them in accordance with applicable laws and regulations. We specified the periods of personal data retention in the Information on processing of personal data by ING Bank Śląski S.A.

4. Who do we share your personal data with and why?

In order to be able to offer the best services and remain competitive in our sector, we share certain data both internally (with other ING entities) and externally (outside ING) with third parties.

Whenever we share your personal data externally (outside ING) with third parties in countries outside the European Economic Area (EEA), we apply the necessary safeguards to protect your data. For that, we rely, among other things, on:

- requirements based on applicable local laws and regulations;
- EU model clauses (if applicable) which are standardized contractual clauses used in contracts with service providers, with which we are sure that personal data transferred outside the European Economic Area are compliant with the GDPR;

For Retail Banking and Wholesale Banking customers:

ING entities

We transfer data between ING entities and branches for various purposes (the full list of which can be found in the section "What we do with your personal data"). We may also transfer data to centralized storage systems or process data centrally at ING to achieve a better efficiency. For data transferred internally, we rely on our binding corporate rules, as required by Regulation (EU) 2016/679, our Global Data Protection Policy (GDPP), and applicable local laws and regulations.

Public, supervisory and judicial authorities

In order to comply with our regulatory obligations, we may disclose data to competent public, supervisory and judicial authorities, e.g.

- **public authorities, regulatory authorities and supervisory authorities**, such as central banks and other authorities supervising financial sectors of countries in which we operate;
- **tax authorities**, which may require us to provide information about customer's assets or other personal data, such as your full name and contact details and other information about your organization. For this purpose, we may process your identification data, e.g. social security number, tax identification number or any other national identification number in accordance with applicable local law;
- **judicial/law enforcement authorities**, such as the police, prosecutor's office, courts and arbitration/mediation bodies at their express and lawful request.

Financial institutions

The processing of certain payment and withdrawal services may require us to share information about our customer or their agent with another bank or specialized financial firm. We also share information with professionals in the financial sector who help us provide financial services such as:

- secure exchange of financial transaction messages;
- making payments and deposits worldwide;
- processing electronic transactions worldwide;
- clearing domestic and cross-border collateral and payment transactions; or
- other organizations providing financial services, including banks, pension funds, brokers, trustees, fund managers and portfolio management service providers.

Service providers and other third parties

If we use other service providers or other third parties to perform certain activities in the ordinary course of business, we may be required to share personal data necessary to complete a specific task. Service providers support us in activities such as:

- design, development and maintenance of web tools and applications;
- IT service providers who may provide application or infrastructure services (e.g. cloud services);
- marketing activities or events and managing customer communications;
- preparing reports and statistics, printing materials and designing products;
- placing advertisements in applications, websites and social media;

- legal, auditing or other specialized services provided by lawyers, notaries, trustees, internal auditors or other professional consultants;
- detecting, analysing or preventing fraud or other misappropriation by specialized companies;
- providing specialized services, e.g. mail delivery by our agents, archiving of physical records, activities of contractors and third party service providers; or
- making securitization arrangements (e.g. trustees, investors and consultants).

EU account information and payment initiation services

The amended EU Payment Services Directive (PSD2) allows you to instruct a Third Party Payment Service Provider (TPP) to download account information or initiate a payment on your behalf in relation to your accounts with ING. TPP may do this only if you give your express consent to such services.

When we receive a request from a TPP, submitted on your behalf, we are required to comply with this request for payment or account information in accordance with its content.

In addition, you may also use PSD2 services to manage your accounts with other banks through ING channels or applications. You may use ING channel or application to:

- view information about your account pertaining to current payment accounts with other banks,
- make online payments from the current payment account with other banks.

In this case, we will act as a TPP, but we can only offer these services if we receive your express consent. If you decide that you no longer wish to use such PSD2 services, you may simply disable this feature in the ING online environment.

Only for Retail Banking customers:

Independent agents, brokers and business partners

We may share your personal data with independent agents, brokers or business partners who act on our behalf or who offer together with us products and services, e.g. insurance. They are registered in accordance with local law and operate on the basis of permits issued by regulatory authorities.

Researchers

We are always happy to accept new insights to help you stay one step ahead in life and in business. For this reason, we share personal data (where permitted by law) with partners such as universities and other independent research institutions that use such data in their research and innovation. The researchers we work with must meet the same stringent requirements as ING employees. Such personal data are shared in the form of aggregated data, and the research results are anonymous.

5. Your rights and how they are respected

If your personal data are processed, you have the right to privacy protection. Based on applicable laws, privacy rights may vary by jurisdiction. If you have questions regarding which rights that apply to you, you may contact us by sending a message to the e-mail address provided in clause 9.

We grant you the following rights:

The right to access information

You have the right to contact us to obtain a list of your personal data that we process.

The right to rectify data

If your personal data are incorrect, you have the right to request that we rectify such data. If we share your data with a third party and such data are later rectified, we will also notify that third party.

The right to object to processing

You may object to the use of your personal data by ING for purposes involving legitimate interests of ING, if you have a good reason to do so. We will review your objection and whether the processing of your information has any adverse effect on you that requires us to stop processing your personal data.

You are not permitted to object to our processing of your personal data if:

- we are obliged to do so by law; or
- it is necessary to perform the contract we have concluded with you.

Only for Retail Banking customers:
You may also object to receiving personalized commercial messages from us. When you become an ING customer, we may ask you if you wish to receive personalized offers. If you later change your mind, you may opt out from receiving these messages, for example by clicking on the "**unsubscribe**" link at the bottom of any commercial e-mail, or by managing your preferences on our website or in the mobile banking application.

In addition, even if you opt out from receiving personalized offers, we will provide you with alerts about suspicious activity on your account, for example:

- if your debit or credit card is blocked,
- if we receive a transaction request from an unusual location.

Right to object to automated decisions (Retail Banking customers only)

We sometimes use systems to make automated decisions based on your personal data if it is necessary to perform a contract with you or if you have granted your consent. You have the right to object to such automated decisions (for example, the price we charge for a product or service) and request that a real person make the decision.

The right to limit processing

You have the right to request that we limit the use of your personal data if:

- you believe that these personal data are incorrect;
- we process these data unlawfully,
- we no longer need these data, but you want us to keep them in case of claims;
- you have objected to our processing of your data due to the legitimate interests of ING.

The right to transfer data

You have the right to request that we transfer your personal data directly to you or to another organization. This applies to personal data that we process in an automated manner and with your consent or on the basis of a contract concluded with you. Where technically feasible and in accordance with applicable local laws, we will transfer your personal data.

The right to erase

ING has a legal obligation to retain your personal data. You may request that we delete your personal data available online, and the right to be forgotten will apply if:

- we no longer need these data for the original purpose;
- you withdraw your consent to their processing;
- you object to us processing your data for purposes related to our legitimate interests or for the purpose of sending personalized commercial messages;
- ING processes your personal data unlawfully; or
- local law requires ING to delete your personal data.

Right to lodge a complaint

If, as a customer or their representative, you are not satisfied with the way we have reacted to your concerns, you have the right to lodge a complaint with ING. If you are still not satisfied with the measures we have taken in response to such a complaint, you may forward it to the ING Data Protection Officer. You may also contact the data protection authority in your country, if applicable.

Exercising your rights

The way you exercise your rights depends on the ING product you have and the availability of services in your country. If you want to exercise your rights or lodge a complaint, please contact us.

When exercising your right, the more specific your request is, the better we can respond to your question. We may ask you for a copy of your ID card or additional information to verify your identity. In some cases, we may deny your request and, where permitted by law, we will notify you of the reason for the denial. Where permitted by law, we may charge a reasonable fee to process your request.

We are committed to respond to your requests as soon as possible, but the response time may vary depending on your location and applicable law. If we need more time (than stipulated by law) to respond to your request, we will notify you immediately and explain the reasons for the delay.

6. Your obligation to provide data

In some cases, we are legally required to collect your personal data or may need such data before we are able provide certain services and products. We agree to request only personal data that are strictly necessary for the purpose. Failure to provide the necessary personal data may result in delayed availability of certain products and services.

7. How we protect your personal data

We use appropriate technical and organizational measures (policies and procedures, IT security measures, etc.) to guarantee the confidentiality and integrity of your personal data and their processing. In order to protect your personal data, we have a number of internal policies and minimum standards across our organization. Such policies and standards are updated periodically to ensure that they comply with the law and changes in the market at all times.

In addition, ING employees are subject to confidentiality obligations and must not unlawfully or unnecessarily disclose your personal data. To help us ensure that your personal data are protected at all times, you should always contact ING if you suspect that your personal data may have been disclosed.

8. Amendments to this Privacy Policy

We may amend this Privacy Policy to keep it compliant with any changes in the law and/or to reflect how we process personal information within our organization. This version was drafted on 1 February 2021.

9. Contact and questions

For further information on ING data protection policies and the use of your personal data, you may contact us via email, telephone or by visiting your local ING branch or office.

Country	ING contact details	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	Belgian Privacy Commission http://www.privacycommission.be

Country	ING contact details	Data protection authority
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	Privacy Commissioner for Personal Data (PCPD), 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 www.dataprotection.org
Japan	dpotokyo@asia.ing.com	Personal Information Protection Commission Japan (PPC) 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	Jabatan Perlindungan Data Peribadi (PDP) http://www.pdp.gov.my/index.php/en/
the Netherlands	privacyloket@ing.nl	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/
Philippines	dpomanila@asia.ing.com	National Privacy Commission https://privacy.gov.ph/
Poland	abi@ing.pl	Office for Personal Data Protection https://uodo.gov.pl/
Portugal	dpo@ing.es	Comissão Nacional de Protecção de Dados (CNPD) https://www.cnpd.pt

Country	ING contact details	Data protection authority
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	Personal Data Protection Commission Singapore (PDPC) 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	
ES	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