ING Bank Śląski S.A. information
concerning ING Bank N.V. Privacy Policy
(Privacy Statement ING Bank N.V.)

The Privacy statement of ING Bank N.V. (Privacy Statement of ING Bank N.V). is attached to this information. ING Bank N.V. is a bank which has its registered office in Amsterdam at Bijlmerplein 888, 1102 MG Amsterdam, the Netherlands, is governed by the law of the Kingdom of the Netherlands and is the parent company of ING Bank Śląski S.A.

The ING Bank N.V. Privacy Policy contains the information required by law, including the GDPR[1] Regulation, regarding the processing of personal data by ING Bank N.V. This policy is in force, other than ING Bank Śląski S.A., subsidiaries or affiliates within the ING Capital Group.
The Privacy Policy of ING Bank N.V. is applied in case when ING Bank N.V. is the controller of your personal data. This shall also include situation when ING Bank Śląski S.A. has transferred your personal data to ING Bank NV for you have given your consent or authorization underlying such transfer.

Please read the attached Privacy Policy of ING Bank N.V.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Privacy Statement ING Bank N.V.

Contents

ING Bank N.V. is a European financial institution and is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 (GDPR) REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation).

To comply with GDPR, ING Bank N.V. has implemented data protection principles on a global scale, through its Global Data Protection Policy (GDPP). The GDPP is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide and approved by the EU Data Protection Authorities. Therefore, in addition to local privacy laws and regulations, ING Bank N.V. has resolved that all its entities, subsidiaries, branches, representative offices, and affiliates worldwide comply with GDPP regardless of geographical location, market typology or target customer.

This is the Privacy Statement of ING Bank N.V., all its entities, subsidiaries, branches, representative offices, affiliates and other ING group companies ('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 Privacy Statement

At ING, we understand that your personal data is important to you. This Privacy Statement explains in a simple and transparent way what personal data we collect, record, store, use and process and how. When handling your data, we seek to ensure that the right people are using the right data for the right purpose.

This Privacy Statement applies to:

- 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.

- Non-ING customers. These could include anyone who makes a payment to or receives a payment from an ING account; anyone that visits an ING website, branch or office; professional advisers; shareholders; anyone who is a guarantor; ultimate beneficial owner, director or representatives of a company that uses our services; debtors or tenants of our customers; anyone involved in other transactions with us or our customers.

We obtain your personal data in the following ways:

- Directly from you when you become a customer, register for our online services, complete a form, sign a contract with ING, use our products and services, contact us through one of our channels.

- Indirectly, from your employer (if it is an ING customer) when you may act as a representative or contact person of your employer when it becomes a prospective customer or if it is an existing customer.

- From other available sources such as debtor registers, land registers, commercial registers, registers of association, the online or traditional media, cookies and comparable technologies via our websites and apps, publicly available sources or other ING companies or third parties such as payment or transaction processors, credit agencies, other financial institutions, commercial companies, or public authorities.

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

We refer to our cookie statement as published on the ING website for more information about the use of cookies and comparable technologies.

2. The types of personal data we process

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 and contact data: your name, date and place of birth, ID number, email address, address, geo-coordinates (in the case of physical risk processes for loans), telephone number, title, nationality and a specimen signature, fiscal code/social security number.
- Transaction data, such as your bank account number, any deposits, withdrawals and transfers made to or from your account, and when and where these took place, transaction identifiers and associated information.
- Financial data, such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, credit capacity, tax status, income and other revenues and/or financial products you have with ING, whether you are registered with a credit register, payment arrears and information on your income, electronic payment instrument data such as card number, expiry date or card verification code (CVV/CVC).
- Socio-demographic data, such as your gender, education, job position and marital status including whether you have children.

- Online behaviour and information about your devices, such as your IP address and device ID of your mobile device or computer and the pages you visit on ING websites and apps.
- Data about your interests and needs that you share with us, for example when you contact our call centre or fill in an online survey or when you use our platforms or fill in surveys.
- Know our customer data as part of customer due diligence and to prevent fraudulent conduct or behaviour that contravenes 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 premises, or recordings of phone or video calls or chats with our offices. We can use these recordings to verify telephone orders, for example, or for fraud prevention or staff training purposes.
- Your interactions with ING on social media, such as Meta (Facebook and Instagram), Twitter, LinkedIn and YouTube. We follow public messages, posts, likes and responses to and about ING on the internet.
- Information related to your location when making a payment or when accessing certain products/services, for example when you withdraw cash from an automated teller machine (ATM).

Sensitive personal data

Sensitive personal data is special category personal data such as personal data relating to your health, ethnicity, religious or political beliefs, genetic or biometric data, as well as well as data related to criminal offences such as fraud. We may process your sensitive personal data for the purposes -set out below in Section 3 link (What we do with your personal data), if we have your explicit consent or if we are otherwise allowed or required to do so by applicable local laws and regulations.

Please note that if you instruct us to make a payment to a political party, trade union, a religious institution or health care institution, this qualifies as sensitive personal data. Therefore, ING will not process this sensitive personal data for purposes other than executing the transaction or with your explicit consent. However, it is possible that as a result of our obligation to comply with anti-money laundering regulations and our interest in preventing fraud, we may further process such data, for example to verify the origin of the funds, but only in the context of anti-money laundering regulations.

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

We only collect personal data about children if they have an ING product or if you provide us with personal data about your own children in relation to a product you obtain from us. We will seek parental consent when it is required by local law.

3. What 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 use your personal data for:

Performing agreements to which you are a party or taking steps prior to entering into these agreements. We use your personal data when you enter into an agreement with us, or when we have to execute our obligations under these agreements.

For instance, we use your account details when you ask us to make a payment or carry out an investment order or to provide you with statements of your accounts or your annual overview. We also use these account details to block payments, investigate and remediate product dysfunctionalities and solve claims, petitions and complaints regarding the requested services, when necessary. We also use your personal data to contact you in order to notify you of issues such as contractual term changes, the expiry of a deadline/contractual condition, registering a debt or to provide you with information related to your services/relationship. We rely on the lawful basis of 'necessary for performing agreements' when we use your personal data for these and compatible purposes.

Compliance with our legal obligations. We use your personal data to comply with a range of legal obligations and statutory requirements, including banking and financial regulations that oblige us to perform or provide:

- Integrity checks: when entering into a customer relationship with you, we have a legal obligation to consult available incident registers and warning systems and national and international sanctions lists.
- Identity verification: when entering into a customer relationship with you, we have a legal obligation to confirm your identity (know your customer check). We can do this by making a copy of your identity document, which we will only use for identification and verification purposes. We may also rely on checks performed by other financial institutions to verify your identity.
- Credit checks: before entering into a customer relationship with you, we have a legal obligation to check whether you qualify as an eligible customer. We assess your credentials from a risk perspective and predict if you can meet your financial obligations towards us as set out in section 6 (Automated decision-making and profiling). In case of lending activities, information on address or geo-location details may be processed in order to ascertain the physical risk associated with your assets in the event of natural disasters.

- Fraud prevention and anti-money laundering and terrorism financing checks: we have a legal obligation to check for potential fraud, money laundering and terrorism financing. This includes monitoring unusual transactions and sanctions lists as set out in section 6 (Automated decision-making and profiling).
- Regulatory and statutory reports to our regulators as set out in section 4 link (Who we share your personal data with and why).

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

Our legitimate interest. We process your data for a range of purposes that are in our interests as described below. When relying on legitimate interest, we ensure that processing remains proportionate and that your interests, fundamental rights and freedoms are respected. If you would like more information about our reasoning behind our assessment in a specific case, please contact us using the details provided in section 11 (Contact and questions).
Please find below an overview of the purposes for which we process your personal data where we rely on legitimate interest:

- **To develop and improve our products and services.** We may use your personal data when analysing your visit to our website or app with the aim of improving these. We use cookies and comparable technologies for this. For more information, we refer to our cookie statement as published on our site. We will also ask your feedback on our current products and services or ask for your opinion on new product ideas. This can include recording your conversations with us, but we will always inform you about this beforehand unless this is not allowed according to local law.

- **To promote and offer you the best-suited products and services provided by us or other ING entities.** We will process your personal data when informing or advising you about similar products and services from ING. Of course, if you don't want to receive these offers you have the right to object or to opt out. We strive to understand you better and meet your changing needs by offering you services that will suit your specific situation. To achieve such personalisation, we may:

    - take into account your sociodemographic and financial situation;
    - analyse your habits and preferences in our various communications channels, visits to our website or other online environments, etc.);
    - analyse the products and services that you have already purchased from us.

- **To ensure effective and efficient internal business process execution and management reporting.** We process your data for our internal processes and operations and to help our management to make better data-driven decisions about

our operations and services. We will always choose aggregated data for this if we can, so that you are not identifiable. This includes:

- analysing our market position in different segments;
- performing a cost and loss analysis;
- training our staff, for example by analysing recorded phone calls (if recording is permitted by local law) in our call centres to improve our calling scenarios;
- automating our processes such as application testing, automatic filling of complaints handling, etc.;
- conducting litigation and complaint management.
- Meeting our environmental, social and governance commitments including external reporting.

- **To test Artificial Intelligence systems.** We may process customers' personal data collected and stored for the financial crime and fraud prevention purposes, in order to ascertain the efficiency and effectiveness of deploying Artificial Intelligence solutions in order to improve ING's financial crime and fraud prevention processes. ING Bank NV performs such testing activities based on its legitimate interest of using state of the art technology in order to ensure prevention, detection and containment of financial crime and fraudulent activities and to contribute to the security and stability of the financial system.

To protect your vital interests. We process your personal data when necessary to protect your interests which are essential for your life or that of another natural person. For example, for urgent medical reasons pertaining to you. We will only process your personal data necessary for the vital interests of another natural person if we cannot base it on one of the other purposes mentioned.

To respect your choice if we request your consent for specific personal data processing. For certain types of personal data processing, we will provide you with specific information about the process and request your prior consent before processing your personal data. This may include:

- the use of biometric data such as face or fingerprints as authentication and/or verification purposes such as for access to mobile apps;
- recording your conversations with us online, by telephone or in our branches;
- promotional activities where we inform you about products and services from ING partners.

You may withdraw your consent at any time as set out in section 7 "Your rights and how we respect them" (link to section 7)

4. Who we share your personal data with and why

There are situations in which we need to provide your personal data to other parties involved in the provision of our services. This could include data transfers within ING Group and to third parties.

Within ING
ING Bank N.V. is part of ING Group which provides financial services in over 40 countries. For more information about ING Group, please visit https://www.ing.com/About-us/Profile/ING-at-a-glance.htm
ING is committed to your privacy and it has adopted strong privacy principles through its Global Data Protection Policy ('GDPP'). The GDPP is approved by the Dutch Data Protection Authority, which is the lead supervisory authority for ING Bank N.V., and is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide (also known as 'Binding Corporate Rules'.)

We may share your personal data within ING to ensure that we're able to comply with our legal obligations such as:

- To comply with any regulatory and statutory reporting obligations and data requests as required by ING Group's European regulators, including the European Banking Authority (EBA), European Central Bank (ECB) and the Financial Stability Board (FSB). Unless data on an individual level is specifically requested by a regulator, we will always make sure that personal data is aggregated, meaning that only information about groups of customers will be shared with the Group's regulators to ensure that it can no longer be linked back to you.

- For the development of ING's internal credit models. Under EU banking rules, ING is obliged to develop these credit models to be able to calculate any counterparty risks and exposures. This allows ING to determine our risks as well as the extent of the financial buffer we are required to hold when providing financial services to you.

- For the development of ING's know your customer (KYC) models. To safeguard ING against involvement in financial economic crimes, KYC models are being developed on a group level for customer and transaction screening to detect potential or actual criminal activity. These KYC models incorporate mandatory requirements derived from the EU Directives and Regulations in the area of prevention of money laundering and terrorist financing, the Basel Committee on Banking Supervision Guidelines (BCBS) and EU, US and UN sanctions laws and regulations.

ING also continues to strive to make our everyday procedures more efficient and effective since it is in our legitimate interest to offer you the best possible services at competitive rates. As such, ING will share your personal data within ING to centralise certain operations to achieve economies of scale, such as: [DROP DOWN BOX]

- For efficiency reasons, certain operational and administrative tasks in relation to the agreements we have with our customers, client management (including screening) or the processing of transactions have been centralised in processing centres, named ING HUBS located in countries such as Slovakia, Poland, Romania and the Philippines. These entities will process your data on behalf of ING and are fully subject to ING's Global Data Protection Policy (GDPP) to ensure an adequate level of data protection.
- The development of models mainly related to improving customer processes such as optimisation of account management and product management in customer channels. For efficiency reasons, these models are mainly developed by our analytics department on a group level. Your personal data will be pseudonymised when transferred for this purpose.
- We may use centralised storage systems to process data at a central point within ING for efficiency purposes. For instance to create different types of credit risk models as mentioned above. These centralised storage systems are operated by ING or third parties such as Microsoft and might be located outside the EU. In any case, ING will always ensure that adequate measures are in place to safeguard your personal data.

Please note that ING will remain responsible for ensuring that the processing of your personal data - including any processing carried out by other ING entities on our behalf as set out above - complies with the applicable data protection regulations. Within ING there are strict requirements included in internal policies and contractual arrangements in place to ensure that your personal data will only be processed for a specific purpose on the basis of an appropriate legal basis if so required by local law (taking into account any effect such processing may have on you) and that adequate organisational and technical measures have been implemented to protect your rights. We will also remain responsible for handling any request you may have in relation to your personal data protection rights as described below.

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

Government, supervisory and judicial authorities

To comply with our regulatory obligations, we're obliged by law to disclose personal data to the relevant government, supervisory and judicial authorities, including:

- **Public authorities, regulators** and **supervisory bodies** such as the European Central Bank (ECB) and De Nederlandsche Bank (the Dutch central bank, DNB) in the Netherlands.
- **Local 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 at their express and legal request.

Other financial institutions

To process certain payment and withdrawal services, we share your personal data with another bank or a specialised financial company. We also share your personal data with financial sector specialists who assist us with financial services such as:

- Payments and credit card transactions worldwide, including Mastercard and VISA where applicable.
- Processing electronic transactions worldwide.
- Settling domestic and cross-border security transactions and payment transactions.
- Account information services: if you have specifically instructed an account information service provider to retrieve account information from your ING accounts on your behalf, we are obliged to share the necessary transaction data with such a provider as long as you have consented to this.
- Payment initiation services: if you have specifically instructed a payment initiation service provider to initiate payments from your ING accounts on your behalf, we are obliged to share access to your accounts with such a provider as long as you have consented to this.
- Other financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Joint controller

ING is working together with SWIFT as joint controllers to fulfill a common purpose: processing securely and reliable transaction services in line with our contractual

commitment. In order to fulfill this purpose, personal data such as identification data (e.g. name, address), order data (e.g. account number of the ordering party and the beneficiary in the case of a payment order), details of the intended use and transaction identifiers (e.g. transaction reference number) are being shared with SWIFT.

As joint controllers, ING and SWIFT agreed to address requests concerning data subject rights and/or other relevant data protection questions concerning the processing activities performed jointly (processing of payments) in a centralized manner; as such, ING will be the main point of contact for any such requests as stated under section 7 (PS) "Your Rights and how we respect them".

Separate controller

In certain cases, SWIFT can also act a separate controller (independent controller), when it comes to processing of your personal data for Statistical Analysis and Product development of SWIFT services and products. For these processes SWIFT directly will handle all requests concerning the rights granted to data subjects. In this situation SWIFT can be contacted via opt.out@swift.com or privacy.officer@swift.com.

However, ING will assist SWIFT in authenticating the ING client who has filed such a request by relying on the client identification information available to us; no further details would be shared with SWIFT in this scenario. You can find details about these processing activities and their purpose as well as contact details applicable for requests or complaints concerning them in the SWIFT Privacy Protection policy.

Service providers and other third parties

When we use other service providers or other third parties to carry out certain activities in the normal course of business, we may have to share personal data required for a particular task. We carefully select these companies and enter into clear agreements with them on how they are to handle your personal data. We remain responsible for your personal data. These service providers support us with activities such as:

- Designing, developing and maintaining internet-based tools and applications.
- IT service providers who may provide application or infrastructure services (such as cloud services).
- Marketing activities or events and managing customer communications.
- 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 advisers.
- Identifying, investigating or preventing fraud or other misconduct by specialised companies.

- Performing specialised services such as postal mail by our agents, archiving of physical records, contractors and external service providers.
- Carrying out securitisation arrangements (such as trustees, investors and the advisers).

Independent agents, brokers and business partners

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

Researchers

We are always looking for new insights to empower you to stay a step ahead in life and in business. For this reason, we exchange personal data (when it is legally allowed) with partners such as universities and other independent research institutions, who use it in their research and innovation. The researchers we engage must satisfy the same strict requirements as ING employees. When possible, the personal data will be shared at an aggregated level to ensure the results of the research are anonymous.

5. Transfer of personal data outside the European Economic Area

Whenever we share your personal data (if EU data protection laws apply) with third parties or other ING entities located in countries outside the European Economic Area (EEA) that do not offer an adequate level of data protection, we will make sure there are adequate measures in place to ensure that your personal data is sufficiently protected.

For this purpose, we rely on so-called transfer tools, including:

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

- **Binding Corporate Rules -** for personal data transfers within ING Group, we also rely on binding internal Group policies (i.e. the Binding Corporate Rules) to ensure that ING entities located in a non-adequate country adhere to an adequate level of data protection when processing personal data as set out in section 4 (Who we share your personal data with and why). (link)

Furthermore, we will assess on a case-by-case basis whether any organisational, technical (such as encryption) and/or contractual safeguards need to be implemented

to ensure your personal data is adequately protected, taking into account the legal framework of the country where the data importer is located.

6. Automated decision-making and profiling

Automated decision-making is when we make decisions by technological means without significant human involvement. Profiling involves the automated processing of personal data with a view to evaluating or predicting personal aspects such as the economic situation, reliability or likely behaviour of a person.

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

Credit risk rating
When you apply for a loan or credit, we create a profile to assess whether you can meet your financial obligations to us and to ensure that we don't offer loans that are not suitable for you. We assess the risk connected to a contract with you via a method called credit scoring. Your credit score is calculated based on automated decision-making. You have to achieve a pre-defined minimum score to ensure an acceptable risk for us.

The credit score is calculated mainly on your financial standing. Based on the personal data you provide in the credit-scoring process, we consult external credit rating agencies to acquire relevant financial information (credit rating, financial statements, turnover/solvency, payment history). If you already have or had a relationship with us in the past (taking into account applicable retention periods), we combine the external financial information with your internal payment history. If you don't achieve the minimum score, the automated credit scoring will decline your application. In that case, we will not enter into an agreement with you since we consider the risks for you and us to be too high. You have the right to object to such automated decisions. We refer to section 7 (Your rights and how we respect them) (link) on how to do this.

Prevention of fraud and money laundering and terrorism financing
We are obliged to perform customer and transaction screening to detect potential and actual criminal activity. As a result, we pay particular attention to unusual transactions and to transactions that, by their nature, result in a relatively high risk of fraud, money laundering or terrorism financing. To do this we create and maintain a risk profile for you. If we suspect that a transaction is connected with money laundering or terrorist financing, we are obliged to report this to the authorities.

Examples of factors that we take into account that may indicate an increased risk of fraud or money laundering and terrorist financing are:

- Changes in a person's normal spending and payment behaviour, such as unexpectedly large amounts being transferred or debited.
- Payments to or from suspicious countries, stores or addresses.
- Two PIN payments by a single person in two vastly different locations at the same time.
- Being listed on any public national or international sanctions lists.

7. Your rights and how we respect them

If your personal data is processed, you have rights. Based on applicable laws, your personal data protection rights may vary from jurisdiction to jurisdiction. If you have questions about which rights apply to you, please get in touch with us using the email address mentioned in section 9 (How we protect your personal data.) (link)

You have the following rights:

Right of access

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 share data about you with a third party and that data is later corrected, we will also notify that party accordingly.

Right to object to processing

You can object to ING using your personal data for its own legitimate interests if you have a justifiable reason. We will consider your objection and whether processing your personal data has any undue impact on you that would require us to stop processing your personal data.

You may not object to us processing your personal data if:

- we are legally required to do so; or
- it is necessary to fulfil a contract with you.

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 change your mind later on, you can choose to opt out of receiving these messages. For example, you can use the 'unsubscribe' link at the bottom of commercial emails or manage your preferences on our website or mobile banking app.

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.

Right to object to automated decisions

We sometimes use systems to make automated decisions based on your personal data 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 (e.g. in relation to credit scoring as explained above) 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 personal data is inaccurate;
- we are processing the personal data unlawfully;
- we no longer need the personal data, but you want us to keep it for use in a legal claim;
- you have objected to us processing your personal data for our own legitimate interests.

Right to data portability

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

Right to erasure ('right to be forgotten')

ING is sometimes legally obliged to keep your personal data. However, if you exercise your right to be forgotten, we will erase your personal data when:

- we no longer need it for its original purpose;
- you withdraw your consent for processing it;
- you object to us processing your personal data for our own legitimate interests or for personalised commercial messages;
- ING unlawfully processes your personal data; or
- local law requires ING to erase your personal data.

Right to complain

Should you as a customer or as a customer's representative be unsatisfied with the way we have responded to your concerns, you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the ING Bank data protection officer. You can also lodge a complaint with the data protection authority located in the country where your personal data is processed by us.

Right to withdraw consent

If you have given your consent to us for specific processing of your personal data as set out in section 3 (What we do with your personal data) link , you can withdraw your consent at any time. From that moment, we are no longer allowed to process your personal data. Please be aware that such withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Exercising your rights

To exercise any of the rights as set out above, please send your request to your ING branch location where you hold your bank account. For generic questions related to this privacy statement, please send your request to DPO.office@ing.nl

When exercising your right, the more specific you are with your request, the better we can assist you. We may ask you for additional information to verify your identity. In some cases, we may deny your request and, if permitted by law, we will notify you of the reason for denial of your request. If permitted by law, we may charge a reasonable fee for processing your request.

We want to address your request as quickly as possible. However, based on your location and applicable laws, the response times may vary. Should we require more time (than normally permitted by law) to complete your request, we will notify you immediately and provide reasons for the delay.

8. Retention

We do not store your personal data longer than we need to for the purposes (as set out in section 3 (What we do with your personal data), for which we have processed it. For applicable retention periods we refer to the applicable local privacy statement. Sometimes we use different storage periods. For example, if the supervisory authority requires us to store certain personal data longer or if you have filed a complaint that makes it necessary to keep the underlying personal data for a longer period. If we no longer need your personal data as described above, we delete or anonymise the personal data, in accordance with regulatory provisions and applicable law.

9. How we protect your personal data

We take appropriate technical and organisational measures to ensure the availability, confidentiality and integrity of your personal data and the way it is processed. This includes state-of-the-art IT security, system and access controls, security monitoring, segregation of duties. We apply an internal framework of policies and minimum standards across all our businesses to keep your personal data safe. These policies and standards are periodically reviewed to keep them up to date with regulations and market developments.

In addition, ING employees are subject to confidentiality obligations and may not disclose your personal data unlawfully or unnecessarily. To help us continue to protect your personal data, you should always contact ING if you suspect that your personal data may have been compromised.

10. Changes to this Privacy Statement

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 June 2023.

11. Contact and questions

To learn more about how we protect and use your personal data, or if you wish to exercise your rights as a data subject, please send an email to the local data protection executive office as indicated in the overview below. While we encourage you to always contact the local data protection executive office first, you can also directly contact the local data protection officer, using the dedicated email address as indicated in the overview below

For generic questions related to this statement you can send an email to : dpo.office@ing.nl