Privacy Statement for ING Wholesale Banking customers

Switzerland – November 2020

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). 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. 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 client.

This is the Privacy Statement of ING Bank N.V., Amsterdam, Lancy/Geneva branch ("ING", "we", "us", the "Bank" and "our"), and it applies to us as long as we process personal data that belongs to you.

1. Purpose and scope of this Privacy Statement

At ING, we understand that your personal data is important for you. This Privacy Statement explains in a simple and transparent way what personal data we collect, record, store, use, share, transfer and process and how. Our approach can be summarised as: the right people use the right data for the right purpose.

This privacy statement applies to
- All past, present and prospective ING clients, including one-person businesses, legal representatives or contact persons acting on behalf of our corporate clients.
- Non-ING clients such as beneficiaries or payees, guarantors, ultimate beneficial owners, directors and officers, legal representatives, shareholders, debtors or tenants of our clients, visitors of our websites, or visitors of our physical locations, professional advisors, auditors, or other individuals involved in transactions.

We obtain personal data in the following ways:
- From your organisation when it becomes a prospective client or if it is an existing client, and your personal data is provided to help us contact your organisation.
- From other available sources such as debtor registers, land registers, commercial registers, registers of association, the online or traditional media, publicly available sources or other companies within ING or third parties such as payment or transaction processors, credit agencies, other financial institutions, commercial companies, or public authorities.

2. The types of personal data we process

Personal data refers to any information that identifies or can be linked to a natural or a legal person. Personal data we process about you includes without limitation:
- **Identification data:** the family or corporate name, date and place of birth or incorporation, ID number, email address, telephone number, title, nationality and a specimen signature, fiscal code/social security number, where applicable shareholders, controlling persons of our clients or beneficial owners of assets of our clients;
- **Financial data:** when you undertake a guarantee with us for the benefit of a client, we may verify credit history, credit capacity, and other information relating to your creditworthiness and credit conditions;
- **Data about client´s interests and needs** shared with us when you contact our officers or participate in an ING survey;
- **Know your client data as part of client due diligence and** to prevent fraudulent conduct or behaviour that contravenes international sanctions and to comply with regulations against money laundering, terrorism financing and tax fraud;
- **Audio-visual data:** where applicable and legally permissible, we process surveillance videos at ING branches, or recordings of phone or video calls or chats with our offices.

Sensitive data
Sensitive data is for example data relating to political beliefs, or to administrative or criminal proceedings or sanctions (Information on fraud is criminal data and we record it). We may process your sensitive data if:
- We have your explicit consent;
- We are required or allowed to do so by applicable local law; or
- You provide sensitive data as part of a contractual agreement or in connection with a requested product or service.

For example, we process sensitive data in connection with
- Know your client (KYC) data obligations: we may keep a copy of your passport or ID card, as applicable based on local law;
- Money laundering or terrorism financing monitoring: we monitor your activity and may report it to the competent regulatory authorities; and
- If allowed under local law, and you choose to use it, we may use your face, fingerprint or voice as recognition for authentication to access mobile apps and certain operations therein.

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, sharing, transferring, adjusting, organising, using, disclosing, transferring or deleting it in accordance with applicable laws. We only use your personal data for business purposes such as:
- **Performing agreements to which you are a party or taking steps prior to entering into agreements.** If you are a corporate client we may use your personal data to enter into an agreement with you. Equally if you are a representative of a corporate client, we may use your personal data to enter into an agreement with the client, and to contact the client when needed. If you are a person providing guarantee for the client, or a beneficiary of payment instruments we may use your personal data to enter into an agreement or executing a payment order in connection to our arrangements with the client. We may verify your capacity and powers using inter alia trade registers or incumbency certificates;
- **Relationship management.** We may ask you as the representative of the client to give us feedback on the products and services offered to the business client.;
  - **Providing the best-suited products and services.** When you as the representative of a client visit our website, call our client service centre, talk to an ING employee or visit us, we may gather information about the client;
  - **Improving and developing products and services.** Analysing how products and services are used helps us understand more about our performance and shows us where and how we can improve our products and services;

- **Business process execution, internal management and management reporting.** We process personal data for our financial services operations and to help our management make better decisions about our operations and services;
- **Safety and security.** We have a duty to protect all personal data and to prevent, detect and contain a data breach or fraud involving personal data collected to comply with regulations against money laundering, terrorism financing and tax fraud. To safeguard and ensure the security and integrity of ING, the financial sector, clients and employees, we may:
  - Process your personal data to protect your organisation´s assets from fraudulent activities, for instance in case your identity (e.g. username and password) is compromised.
  - Use certain personal data (e.g. name, account number, age, nationality, IP address, etc.) to detect fraudulent activities and the actors behind it.
  - Use your personal data to alert you in case we detect suspicious activities involving your business´s assets, for example a transaction is taking place from a non-typical location.
- **Compliance with legal obligations to which we are subject.** We process personal data to comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation etc.). For example, know your client (KYC) rules and regulations require ING to verify the identity before accepting you as a client. Upon request by authorities, ING may report the transactions carried out by clients.
- **Functioning of the Bank (inter alia outsourcing of its activities).** We process, transfer and/grant access to data in the context of ING's wider functioning, including when we are outsourcing some of our activities to other ING entities or to carefully selected service providers, such as:
  - The hosting, operation, maintenance and support of the Bank's IT infrastructure and applications, as well as of the Bank's various communication systems and payment platforms.
  - The processing of instructions as well as the surveillance (inter alia to ensure that the transactions that ING is facilitating comply in all aspects with international regulations and relevant laws), the monitoring, the recording and the storage/archiving of communications and payments.
  - The monitoring and calculation of account balances and preparation of account statements.
  - Any and all required activities, from document collection to final decision making and execution, in relation to or in connection with client due diligence, risk or tax classification processes as well as reporting obligations (e.g. FATCA, CRS, EMIR).
  - The commercial, operational and legal handling, from origination through credit decision process to deal execution, and the management, (as the case may be, automated) monitoring and review of certain transactions and files, in particular with respect to commercial lending.
  - The client support.
  - The monitoring and management of the Bank's accounts with its correspondent banks.

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

Applicable laws require us to retain personal data for a period of time. This retention period may vary from a few months to a several years, depending on the applicable local law. When your personal data is no longer necessary for a process or activity for which it was originally collected, we delete it, or bundle data at a certain abstraction level (aggregate), render it anonymous and dispose of it in accordance with the applicable laws and regulations.

4. Who we share your data with and why

To offer you the best possible services and remain competitive in our business, we share certain data internally i.e., with other ING businesses and externally (i.e., outside of ING) with third parties, located (or headquartered) without limitation in the EU and/or Asia in particular India, the Philippines and Singapore and/or in the USA.

Whenever we share your personal data externally (i.e., outside of ING) with third parties we ensure the necessary safeguards are in place to protect it. For this purpose, we rely upon, amongst others:

- Requirements based on applicable local laws and regulations.
- EU Model clauses, when applicable, we use standardised contractual clauses in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with GDPR.
- International treaties such as the EU US Privacy Shield framework that protects personal data transferred to certain service providers in the United States.
- The Bank's contractual arrangements including but not limited to the "Waiver of Banking Secrecy".

ING entities

We transfer data across ING businesses and branches for various purposes (see section 'What we do with your personal data' for a list of examples). We may also transfer data to centralised storage systems or to process it at a central point within ING for efficiency purposes.

Government, Supervisory, Judicial and international authorities and committees

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

- **Public authorities, regulators** and **supervisory bodies** such as the central banks and other financial sector supervisors in the countries where we operate.
- **Tax authorities** may require us to report client 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 like social security number, tax identification number or any other national identifier in accordance with applicable local law.

- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their request.

Financial institutions
To process certain payment and withdrawal services, we may have to share information about the client or its representative with another bank or a specialised financial company based in other countries . 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; or
- Other financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

Service providers and other third parties
When we use other service providers or other third parties to carry out certain activities in the normal course of business, we may have to share personal data required for a particular task. Service providers support us with activities like:
- Designing, developing and maintaining internet-based tools and applications;
- IT service providers who may provide application or infrastructure (such as cloud) services for example ING's global client relationship management platform;
- Corporate events and activities and managing client 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, brokers, insurers or other professional advisors;
- Identifying, investigating or preventing fraud or other misconduct by specialised companies;
- Performing specialised services like postal mail by our agents, archiving of physical records, contractors and external service providers; or
- Carrying out securitisation arrangements (such as trustees, investors and the advisers), as well as transactions having a capital relief effect.

5. Your rights and how we respect them

If your personal data is processed, you have privacy rights. Based on applicable laws, your privacy rights may vary from jurisdiction to jurisdiction. If you have questions about which rights apply to you, please get in touch with us through the email address mentioned in item 9.

Subject to local law, we grant the following rights:

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 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 information 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 or one of our corporate clients.

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 data unlawfully;
- ING no longer needs the data, but you want us to keep it for use in a legal claim; or
- You have objected to us processing your data for our own legitimate interests.

Right to erasure
ING is legally obliged to keep your personal data. You may ask us to erase your online personal data and right to be forgotten would be applicable if
- We no longer need it for its original purpose;
- You withdraw your consent for processing it;
- You successfully object to us processing your data for our own legitimate interests;
- ING unlawfully processes your personal data; or
- A local law requires ING to erase your personal data.

Right to complain
Should you as a client or its representative be unsatisfied with the way we have responded to your concerns, you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the ING Bank data protection officer. You can also contact the data protection authority in Switzerland if applicable.

Exercising your rights
How you exercise your rights depends on your ING product and the availability of services in Switzerland. If you want to exercise your rights or submit a complaint, please contact us. When exercising your right, the more specific you are with your application, the better we can assist you with your question. We may ask you for a copy of your ID, or additional information to verify your identity. In some cases we may

deny your request and, if provided for by law, we will notify you of the reason for denial. If permitted by law, we may charge a reasonable fee for processing your request.

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

6. Your duty to provide data

In some cases, we are legally required to collect personal data or your personal data may be needed before we may perform certain services and provide certain products. We undertake to request only the personal data that is strictly necessary for the relevant purpose. Failure to provide the necessary personal data may cause delays in the availability of certain products and services.

7. How we protect your personal data

We take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it is processed. We apply an internal framework of policies and minimum standards across all our business to keep your personal data safe. These policies and standards are periodically revised to keep them up to date with regulations and market developments.

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

8. 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 on 20 November 2020.

9. Contact and questions

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

Country	Contact details ING	Data Protection Authority
Switzerland	bp.dp@ing.ch ING Bank N.V., Amsterdam, succursale de Lancy/Genève Avenue des Morgines 10 CH -1213 Petit-Lancy/Genève	Préposé fédéral à la protection des données et à la transparence | Federal Data Protection and Information Commissioner https://www.edoeb.admin.ch/edoeb/en/home.html