

# Privacy Statement for ING customers

Switzerland – November 2018

## Contents

1. About this Privacy Statement	3
2. The types of data that we process	3
3. What we do with your personal data	3
4. Who we share your data with and why	4
5. Your rights and how we respect them	6
6. Your duty to provide data	6
7. How we protect your personal data	6
8. What you can do to help us keep your data safe	6
9. How long we keep your personal data	7
10. Contact us	7
11. Scope of this Privacy Statement	7

## 1. About this Privacy Statement

This Privacy Statement of ING Belgium, Brussels, Geneva Branch (hereinafter also referred to as the “Bank” or “ING”) aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following persons:

- **Any legal or natural person** we are in contact with or who are directly or indirectly related to ING clients and / or to operations of ING or transactions in which ING plays a role (the “Person”):
  - This could for instance be ING clients or persons factually or legally related to ING clients e.g. their legal or authorised representatives. It may also be company directors, direct or indirect shareholders, beneficial owners of the client and / or of its assets, legal or authorised representatives, directors or shareholders of client’s affiliates;
  - Persons who are not ING clients, such as, (i) beneficiaries of transfers, bank guarantees, letters of credit, letters of indemnity, (ii) (legal or authorised representatives, directors or shareholders of) counter-parties of our clients when for example ING has obtained a form of interest over the rights of its clients against such counter-party (iii) business partners or suppliers of ING and their legal or authorised representatives.

Personal data refers to any information that tells us something about you / a Person or that we can link to you / a Person. This includes information such as business activities, dealings, assets, beneficial ownership structure, corporate or family name, address, date of birth, account number, IP address, or information about transfers made from or to your / a bank account. By processing we mean everything we can do with this data such as collecting it, recording, storing, adjusting, organising, using, disclosing, transferring or deleting.

You share personal information with us when you become a client, register with our online services, complete an online form, sign a contract, use our products and services or contact us through one of our channels. Personal information related to you may also be provided to us when you are in relation with one of our clients or with us as a third party.

We also use data that is legally available from (public) sources such as debtor registers, land registers, commercial registers, registers of association, internet and the media, or is legitimately provided by other companies within the ING Group or third parties such as credit agencies or anti money laundering tools.

## 2. The types of data that we process

The personal data that we process includes:

- **Identification data**, such as corporate or family name, address, contact details, country of incorporation or domicile and of taxation, tax status, tax identification number, or data of individuals acting for you or in any way related to you,

or to a transaction in which ING plays a role for example their name, address, date of birth, function or role in your company or organisation or in the organisation of your counterparty;

- **Transaction data**, such as your bank account number and any transfers related to your account;
- **Financial data**, such as your business and dealings data, invoices, credit notes, transfers related to your account(s), the value of your property or other assets, your creditworthiness data, scoring/rating data, origin of assets, credit history, credit capacity, financial products you have with the Bank, whether you are registered with a credit register, payment arrears and information on your income;
- **In relation to ultimate beneficial owners, socio-demographic data**, such as information about marital status identity of spouse or children, and your or their political role where applicable;
- **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;
- **Audio-visual data**, such as surveillance videos at ING or recordings of phone calls to our client service centres.

### Sensitive data

We do not record sensitive data relating to your health, ethnicity, religious or political beliefs unless it is strictly necessary. When we do it is limited to specific circumstances, for example, when we are subject to various obligations, (e.g. laws of the financial sector, anti-money laundering and tax laws) and bank regulatory requirements (e.g. from the Swiss National Bank and FINMA). We are legally obliged to keep a copy of the passport of certain natural persons for client due diligence purposes.

### Children’s data

We only collect data about children if this is relevant for our client due diligence purposes or in relation to a transaction they may be involved in with the Bank.

## 3. What we do with your personal data

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

- **Administration.** When you open an account with the Bank, we are legally obliged to collect personal data that verifies your corporate identity (such as a copy of your company register excerpt and articles of association and the identity of the legal representatives or natural persons connected with you (such as a copy of an ID card or passport), to assess whether we can accept you as a client. We also need to know your address or phone number to contact you;
- **Product and service delivery.** We use information about you (as a client or not) to be able to assess and/or execute agreements with, or instructions of, the Bank’s clients, such as the opening of accounts or the arranging of loans, the issuance of guarantee or payment instruments, the maintaining and improving of relationships with, and services to, our clients, the settling of payment transactions and

other banking services for our clients and third parties. When executing a payment order or issuing a bank guarantee, for example, we register the name of the person giving us the relevant instruction and the details of the beneficiary of the payment or the guarantee. We will also share client data with third parties e.g. at the request of our client when issuing a recommendation letter or, from time to time, at the request of the beneficiary's bank or any correspondent bank, when we perform an outbound payment;

- **Managing client relationships.** We may ask you for feedback about our products and services and share this with certain members of our staff to improve our offering. We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you;
- **Credit risk and behaviour analysis.** To assess your ability to repay a loan we apply specific statistical risk models based inter alia on (your) personal data;
- Providing you with the best-suited products and services. When you visit our website, call our client service centre or visit us we gather information about you. We analyse this information to identify your potential needs and assess the suitability of products or services;
- **Improving and developing products and services.** Analysing how you use our products and services helps us understand more about you and shows us where we can improve. For instance:
  - when you open an account, we measure the time it takes until your first transaction to understand how quickly you are able to use your account;
  - we analyse data on transactions between you and our corporate clients to offer information services to our corporate clients or provide them advice on how they can make better use of ING's products and services. When ING processes personal data for this purpose, aggregated data may be made available to the corporate client. A corporate client cannot identify you from these aggregated data;
- **Preventing and detecting fraud and data security:** We have a duty to protect your personal data and to prevent, detect and contain data breaches. This includes information we are obliged to collect about you, for example to comply with regulations against money laundering, terrorism financing and tax fraud:
  - We may process your personal information to **protect you and your assets** from fraudulent activities, for example if you are the victim of identity theft, if your personal data was disclosed or if you are hacked. To this effect, the Bank may use and participate in warning systems (such as internal or external fraud registers);
  - We may use certain information about you (e.g. (corporate) name, account number, age, nationality, IP address, etc.) to quickly and efficiently detect a particular crime and the person behind it;
  - We use contact and security data (such as passwords) to secure transactions and communications made via remote channels. We could use this data to alert our clients, for example in case of unusual movements on our clients' account(s);

- **Internal and external reporting:** We process your data for our banking operations and to help our management make better decisions about our operations and services. To comply with a range of legal obligations and statutory requirements (anti-money laundering legislation and tax legislation for example);
- **In the context of balancing interests:** Where required, we process your data beyond the actual fulfilment of the contract for the purposes of the legitimate interests pursued by us or a third party. Examples:
  - in case of any legal threat or action involving the Bank and/or the client;
  - to secure, collect and/or enforce the Bank's claims against the client or collateral granted by the client or third parties;
  - to hedge or insure any risk related to a transaction entered into by the Bank with or on behalf of the client, to grant any participation in such transaction or in any other manner to obtain capital relief in that respect;
  - in the case of allegations made by the client or its representatives against the Bank in public or to authorities in Switzerland or abroad;
  - in case of a contemplated assignment, transfer and creation of security over all or part of Bank's rights and obligations under its business relationship with the client or over any related security interest, including ancillary rights related thereto.

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

#### 4. Who we share your data with and why

Subject to your rights under Swiss banking secrecy and Swiss data protection laws (and to the extent that such rights have been waived by yourselves - for your own account and / or on behalf of other person(s) - from time to time), we may share certain data internally and outside of ING to be able to offer you the best possible services and remain competitive in our business. This includes:

##### ING entities

We may share, grant access and/or transmit from time to time, for further processing, storage, sharing and consultation data **to any offices and affiliates of the ING Group** in Switzerland or abroad (including, without limitation, EU and/or Asia in particular the Philippines, Singapore) when it is necessary, incidental or desirable for operational, commercial, regulatory or reporting purposes, for example:

- under global supervision and management of the clientele of the ING Group, inter alia credit and commercial processes and decisions, profitability, quality and risk management policies;
- for the purpose of internal cross-selling to enable the client and/or its affiliates to benefit from the global reach of the ING Group;
- in relation to our operations and services and/ or products offered to the client or any of its affiliates inter alia by us or other ING offices;

- in relation to duties of the Bank and/or the ING Group as prescribed in any relevant legislation such as the Swiss Anti-Money Laundering Act, the EU Directive 2015/849, the Swiss Automatic Exchange of information Act, the EU Common Reporting Standards and relevant FATCA's implementation act(s), all as amended or replaced from time to time, as well as under any related group-wide ING policy;
- hosting, operation, maintenance and support of the Bank's IT infrastructure and applications, as well as of the Bank's various (electronic) messaging systems and payment platforms or system (including manual data feeding as well as the processing, surveillance (mainly for data-loss-prevention purposes);
- monitoring, storage and archiving of messages and payments;
- calculation of account balances and preparation of account statements;
- filtering and screening of messages and payments, as well as of documents to ensure that the transactions that the Bank is facilitating comply in all aspects with international regulations and relevant laws;
- any and all required activities, from document collection to final decision making, in relation to or in connection with customer due diligence, risk or tax classification processes, as well as reporting obligations (e.g. FATCA, CRS, EMIR);
- the recording, processing, monitoring, storage and archiving of financial market instructions (inter alia when given over the phone);
- the commercial and legal handling, from origination through credit decision process to deal execution, the management, (as the case may be automated) monitoring and review of certain transactions.

All data transfers within the ING Group will be made in compliance with Swiss law and ING Global Data Protection Policy (GDPP), relying on one of the safeguards described below.

### Authorities

To comply inter alia with our regulatory obligations we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering. In some cases, we are **required by law**, to share your data with external parties, including:

- **Public authorities, regulators and supervisory bodies** such as the central banks of the countries where we operate;
- **Tax authorities** may require us to report your assets (e.g. balances on your account or information in relation to your beneficial owners or shareholders);
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request, in case of any legal threat or action involving the Bank and/or the client;
- **Lawyers**, for example, in case of bankruptcy or restructuring arrangements, **notaries**, for example, when registration of a security is required, **trustees** who take care of other parties' interests, and **company or Bank's auditors**.

### Financial institutions

When you make a transfer to an account at another bank, the transaction always involves another bank or a specialised

financial company. To process payments we have to share information about you with the other bank, such as your corporate or family name and account number or, upon request, information about the ultimate beneficial owner of the structure and / or of the assets. We also share information with financial sector specialists who assist us with financial services like:

- exchanging secure financial transaction messages;
- payments and credit transactions worldwide;
- processing electronic transactions worldwide;
- settling domestic and cross-border security transactions and payment transactions.

Sometimes we share information with banks or financial institutions in other countries, for example when you make or receive a foreign payment<sup>1</sup>. And we share information with business partners whose financial products or services may be involved, such as insurance companies.

### Third Party Service Providers

We may grant access and/or transmit from time to time, for further processing, storage, sharing and consultation, data to third parties in Switzerland or abroad, including, without limitation, to the EU or outside the EU, (e.g. IT service providers, innovative CRM service providers via a cloud, exchanges, brokers, auditors, banks, processing units, third-party custodians, issuers, authorities and their representatives) in the operation of our business, when it is necessary, desirable or incidental to our functioning or chosen operational set up and / or to services related to our clients such as:

- the hosting, operation, maintenance and support of the Bank's IT infrastructure and applications, as well as some of the Bank's (electronic) messaging systems and payment platforms (including manual data feeding as well as the processing, surveillance (mainly for data-loss prevention purposes);
- monitoring and storage/archiving of messages;
- commercial support, marketing and client relationship management;
- the recording, processing, monitoring and storage/archiving of financial market instructions (inter alia when given over the phone).

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

### Safeguards

Whenever we share your personal data internally or with third parties in other countries, we ensure the necessary relevant safeguards are in place to protect it. For this, the Bank notably relies on:

- Binding Corporate Rules as defined in EC Regulation (EU) 2016/679. These are known as the ING Global Data Protection Policy (GDPP) and have been approved by the data protection authorities in all EU member states;

<sup>1</sup> For more details, please refer to clause 23 of the General Terms and Conditions of ING Belgium, Brussels, Geneva Branch and clause 14 of the Wholesale Banking Conditions of ING.

- **EU Model clauses**, which are standardised contractual clauses used in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with EU data protection law; or
- **Privacy Shield** framework that protects personal data transferred to the United States; or
- the Bank's contractual arrangements including but not limited to the "Waiver of banking secrecy and data protection rights".

## 5. Your rights and how we respect them

We respect your rights as a client to determine how your personal information is used. These rights include:

### Right to access information

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

### Right to rectification

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

### Right to object to processing

You can object to the Bank using your personal data for its own legitimate interests. You can do this online or by mail. We will consider your objection and whether processing your information has any undue impact on you that requires us to stop doing so.

You cannot object to us processing your personal data if we are legally required to do so; if it is necessary to fulfil a contract with you or with a client which employs you; or if there are security issues with your account.

### Right to restrict processing

You have the right to ask us to restrict using your personal data, notably if:

- you believe the information is inaccurate;
- we are processing the data unlawfully;
- the Bank no longer needs the data, but you want us to keep it for use in a legal claim;
- you have successfully objected against the processing of your data for our own legitimate interests.

### Right to erasure

You may ask us to erase your personal data, notably if:

- we no longer need it for its original purpose and we are not anymore obliged to keep your personal data as exposed under clause 9 below;
- you withdraw your consent for processing it;
- you object successfully against the processing of your data for our own legitimate interests; or
- the Bank unlawfully processes your personal data.

### Right to complain

Should you not be satisfied with the way we have responded to your concerns you have the right to submit a complaint to

us. If you are still unhappy with our reaction to your complaint, you can escalate it to the Bank's Data Protection Officer. If applicable, you can also contact the data protection authority in Switzerland.

### Exercising your rights

If you want to exercise your rights or submit a complaint, please contact us. The contact details of the Bank's office in Switzerland are indicated at the end of this Privacy Statement.

How you exercise your rights depends on the availability of services provided by the Bank. It could be through our website or by mail. We aim to respond to your request as quickly as possible. In some instances this could take up to one month (as legally allowed). Should we require more time to complete your request, we will let you know how much longer we need and provide reasons for the delay.

In certain cases, we may deny your request. If it is legally permitted, we will let you know in due course why we denied it.

## 6. Your duty to provide data

There is certain information that we must know about you so that we can commence and execute our duties as a bank and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this data we may not be able to open or maintain an account for you or for the client you are related to and /or perform certain banking activities. However, the Bank and/or any member of ING Group shall not be liable for inaccuracies concerning personal data if these errors are due to erroneous information being supplied to the Bank by clients or third parties.

## 7. How we protect your personal data

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

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

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

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

- Install anti-virus software, anti-spyware software and a firewall. Keep them updated;
- Do not leave equipment (e.g. your personal computer) unattended;

- Log off from online banking when you are not using it;
- Keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures;
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing emails requesting personal information.

## 9. How long we keep your personal data

We will retain personal data only:

- for the period required to serve the purposes for which the personal data were collected or for which they are further processed; and/or
- to the extent necessary to comply with an applicable regulatory and legal requirement; and/or
- as advisable in light of any (potentially) applicable statute of limitations; and/or
- for legal holds that we can face as a bank, which require us to keep records for an undefined period of time. A legal hold is a process that an organisation uses to preserve all forms of relevant information when litigation is reasonably anticipated.

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

## 10. Contact us

If you want to know more about ING's data policies and how we use your personal data, you can send us an email at the following address: [BP.DP@ing.ch](mailto:BP.DP@ing.ch). There are contact details of the Bank Data Protection Officer at the end of this Privacy statement, as well as the contact details of the Swiss Data Protection Authority.

## 11. Scope of this Privacy Statement

This is the Privacy Statement of ING Belgium, Brussels, Geneva branch. It applies to ING Belgium, Brussels, Geneva branch to the extent that it processes personal data.

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created on 20 November 2018. The most recent version is available at [ing.com](http://ing.com).

Country	Contact details for Data Protection Officer	Data Protection Authority
Switzerland	<p><a href="mailto:BP.DP@ing.ch">BP.DP@ing.ch</a>            ING Belgique, Bruxelles, succursale de Genève            (ING Belgium, Brussels, Geneva branch)            Rue Jean-Petitot 6            1204 Genève            Suisse</p>	<p>Préposé fédéral à la protection des données et à la transparence   Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter   Incaricato federale della protezione dei dati e della trasparenza            Feldeggweg 1            CH - 3003 Berne            Tel.: +4158 462 43 95            Fax: +4158 465 99 96</p>