Privacy Statement
for
ING Luxembourg S.A customers

v.2.0 May 2020

Contents

This is the Privacy Statement of ING Luxembourg (and its subsidiaries) acting as data controller – located 26, Place de la Gare, 2965 Luxembourg – *société anonyme* - and registered with the Luxembourg RCS under number B.6041. - www.ing.lu - May, 2020 .

ING Luxembourg is subject to the data protection obligations set out in the EU General Data Protection Regulation 2016/679 (GDPR).

This is the Privacy Statement of ING Luxembourg S.A, and its subsidiaries ("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 for you. This Privacy Statement explains in a simple and transparent way what personal data we collect, record, store, use 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 customers who are individuals ("you"). This includes one-person businesses, legal representatives or contact persons acting on behalf of our corporate customers;
- Anyone involved in any transaction with ING, whether it is in your personal capacity or as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, anyone that is a guarantor, ultimate beneficiary owner, etc.);
- Non-ING customers. These could include anyone that visits an ING website, branch or office; professional advisors; shareholders.

We obtain your personal data in the following ways:

- You share it with us when you become a customer, register for our online services, complete an online form, sign a contract with ING, use our products and services, contact us through one of our channels or visit our websites.
- From your organisation when it becomes a prospective customer or if it is an existing customer, 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 person. Personal data we process about you includes:

For our retail customers:

- **Identification data** such as the name, date and place of birth, ID number, email address, 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;

- **Financial data,** such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, credit capacity, financial products you have with ING, whether you are registered with a credit register, payment arrears and information on your income;
- **Socio-demographic data**, such as whether you are married and have children. Where local law considers this sensitive data, we respect the local law;
- **Online behaviour and preferences data,** IP address of your mobile device or computer you use 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;
- **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, for fraud prevention or staff training purposes;
- **Your interactions with ING on social media**, such as Facebook, Twitter, Instagram, Google+ and YouTube. We follow public messages, posts, likes and responses to and about ING on the internet.

For our legal entities banking customers :

- **Identification data** such as the name, date and place of birth, ID number, email address, telephone number, title, nationality and a specimen signature, fiscal code/social security number;
- **Financial data:** when you undertake a guarantee with us for the benefit of a customer, we may verify credit history, credit capacity, and other information relating to your creditworthiness and credit conditions;
- **Online behaviour and preferences data:** IP address of your mobile device or computer and the pages visited on ING websites and apps;
- **Data about customer´s interests and needs** shared with us when you contact our officers or participate in an ING survey;
- **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, or recordings of phone or video calls or chats with our offices.

Sensitive data

Sensitive data is data relating to your health, ethnicity, religious or political beliefs, genetic or biometric data, or criminal data (information on fraud is criminal data and we record it). We may process your sensitive data if:

For our retail customers:

- We have your explicit consent;

- We are required or allowed to do so by applicable local law. For example, we may be obliged to keep a copy of your passport or identity card when you become an ING customer;
- You instruct us to make a payment, for example, to a political party or religious institution.
- If allowed under local law, and you choose to use it, we may use face, fingerprint or voice as recognition for authentication to access mobile apps and perform certain operations therein.

For our legal entities :

- 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 customer (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 into mobile apps and certain operations.

Children´s data

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

In relation to the offer of information society services directly to a child under the age of 13, we would do so only if and to the extent that we have received authorization from the person holding parental responsibility.

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 process your personal data under one of the following legal grounds:

- To conclude and carry out our contract with you;
- To comply with our legal obligations;
- For our legitimate business interests. This data processing may be necessary to maintain good commercial relations with all our customers and other concerned parties. We may also process your data to prevent and combat fraud and to maintain the security of your transactions and of the operations made by ING;
- When we have your consent. In this case, you may withdraw your consent at any time.

We may process the data of our customers for the following purposes :

- **Performing agreements to which you are a party or taking steps prior to entering into agreements.** We use information about you when you enter into an agreement with us, or we have to contact you. We analyse information about you to assess whether you are eligible for certain products and services. For example, we may look at your payment behaviour and credit history when you apply for a loan or a mortgage. And we use your account details when you ask us to make a payment or carry out an investment order.
- **Administration.** For example, when you open an ING account we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport) and to assess whether we can accept you as a customer. We also need to know your postal, e-mail address or phone number to contact you.
- **Relationship management and marketing.** We may ask you for feedback about our products and services, or record your conversations with us online, by telephone or in our branches. We may share this with certain members of our staff to improve our offering or to customise products and services for you. We may send you newsletters informing you about these products and services. Of course, if you don't want to receive these offers you have the right to object or to withdraw your consent.
- **Providing you with the best-suited products, services and marketing.** We may use your data for commercial activities, including processing which is necessary for developing and improving our products and/or services, customer service, segmentation of customers and profiling and the performance of (targeted) marketing activities. We do this to establish a relationship with you and/or to maintain and extend a relationship with you and for performing statistical and scientific purposes. You have the right to withdraw your consent or object to personalised direct marketing or commercial activities, including related profiling activities. Moreover, you can always unsubscribe from receiving personalised offers.
- **To improve and develop our products and services**. Analysing how you use and interact with our products and services helps us understand more about you and shows us where and how we can improve. For instance:
    - When you open an account, we measure how long it takes until you are able to use your account.
    - We analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns.
    - Sometimes we analyse your personal data using automated processes, such as algorithms, to speed up credit decisions for loans and mortgages.
- **For credit risk and behaviour analysis.** We use and analyse data about your credit history and payment behaviour to assess your ability to repay a loan, for example.
- **Business process execution, internal management and management reporting.** We process your data for our banking operations and to help our management make better decisions about our operations and services.
- **Safety and security.** We have a duty to protect your personal data and to prevent, detect and contain any breaches of your data. This includes data we are obliged to collect about you, for example to verify your identity when you become a customer. Furthermore, we not only want to protect you against fraud and cybercrime, we have also a duty to ensure the security and integrity of ING and the financial system as a whole by combatting crimes like money laundering, terrorism financing and tax fraud.

- To protect your assets from fraudulent activities online, for example, if you are hacked and your username and password are comprised.
- We may use certain information about you (e.g. name, account number, age, nationality, IP address, etc.) for profiling purposes to detect fraudulent activities and the perpetrators.
- We may use your personal data to alert you if we detect suspicious activity on your account, for example when your debit or credit card is used in a non-typical location.

- **Protecting your vital interests.** We process your 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. We will only process your data necessary for the vital interests of another natural person if we cannot base it on one of the other purposes mentioned.
- **Compliance with legal obligations to which we are subject.** We process your data to comply with a range of legal obligations and statutory requirements.
- **Personalised marketing based on profiling**

With your consent, we may send you letters, e-mails, or text messages offering you a product or service based on your personal profile (payment data or other similar details) or show you such an offer when you log in to our website or mobile apps. You may at any time unsubscribe from such personalised offers.

For legal entities banking customers (e.g. companies, financial institutions, etc.):

- **Performing agreements to which you are a party or taking steps prior to entering into agreements.** We may process the personal data of legal representatives proxies, ultimate beneficiaries owners (UBOs), and other intervenient such as contact person, guarantors, etc. for the following purposes:
- **Administration.** For example, when a legal entity client open an ING account we are legally obliged to collect personal data of its representatives, proxies, guarantors and ultimate beneficiary owners (UBO), to verify their identity (such as a copy of their ID card or passport) and to assess whether we can accept you as a customer. We also need to know their professional post address, phone number and e-mail information to reach out to these persons
- **Performing agreements to which our legal entities banking customers** are a party or taking steps prior entering into an agreement with the customer, and to contact the customer when needed. If you are an individual providing guarantee for the customer, 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 customer. We may verify your capacity and powers using trade registers or incumbency certificates; **Relationship management and marketing.** We may ask you as the representative of the customer to give us feedback on the products and services offered to the business client. We may send newsletters regarding new and existing products and services offered by ING. You may opt out of any communication at any time;
    - **Providing the best-suited products and services.** When you as the representative of a customer visit our website, call our customer service centre, talk to an ING employee or visit a branch, we may gather information about the customer;
    - **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.) for profiling 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 customer (KYC) rules and regulations require ING to verify the identity before accepting you as a customer. Upon request by authorities, ING may report the transactions carried out by customers.

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.

Whenever we share your personal data externally (i.e., outside of ING) with third parties in countries outside of the European Economic Area (EEA) we ensure the necessary safeguards are in place to protect it. . In case of transfer to a country outside the European Economic Area whose local regime is considered as inadequate by the European Commission, ING relies upon, amongst others:

- Requirements based on applicable local laws and regulations.
- The conclusion or the execution of an agreement, one of your transactions or a third-party transaction in your favour;

- 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.
- Data transfer that are necessary for reasons of public interests;
- Your explicit consent;
- Adequacy decisions by the European Commission, which establish whether a country outside of the EEA ensures personal data is adequately protected.

For both our retail and legal entities banking customers:

ING entities

We transfer data across ING businesses and branches for various purposes (see section 'What we do with your personal data' for the full list). We may also transfer data to centralised storage systems or to process it at a central point within ING for efficiency purposes. For all internal data transfers we rely on our Binding Corporate Rules as defined in EC Regulation (EU) 2016/679, which is our Global Data Protection Policy (GDPP), and on the applicable local laws and regulations.

Government, Supervisory and Judicial authorities

To comply 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 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 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 express and legal request.

Financial institutions

To process certain payment and withdrawal services, we may have to share information about the customer or its representative with another bank or a specialised financial company. 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. We can also share information with business partners whose financial products we sell, such as insurance companies.

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;
- 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 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).

Account information and payment initiation services within the EU

The revised EU Payment Service Directive (PSD2) allows you to instruct a third-party payment service provider (TPP) to retrieve account information or initiate payments on your behalf with respect to your accounts with ING. The TPP may do so only if you have given your explicit consent to those services.

When we receive a request from a TPP on your behalf, we are obliged to carry out the request for payment or account information, as requested.

Additionally you can also use the PSD2 services to manage your accounts with other banks through your ING channels or apps. You may use the ING app or channel to :

- View account information of your current payment accounts with other banks;
- Make online payments from your current payment account with other banks.

In this case, we will be the TPP and we may only offer these services if we receive your explicit consent. If you decide that you no longer want to use these PSD2 services, you can simply turn off the feature in the ING online environment.

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 which jointly offer products and services with us, such as insurance. 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 help you get ahead in life and in business. For this reason, we exchange personal data (when it's legally allowed) with partners like 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. The personal data is shared at an aggregated level and the results of the research are anonymous.

5. Your rights and how we respect them

We respect your individual rights which include among others :

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. 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

You can also object to receiving commercial messages from us (by e-mail, mail and phone) or to have your personal data used for statistical purposes. When you become an ING customer, we may ask you whether you want to receive personalised offers (based on your payment data and other similar details). Should you later change your mind, you can choose to opt out of receiving these messages by, amongst others:

▪Using the 'unsubscribe' button at the bottom of each commercial e-mail;
▪Adapting your privacy settings directly at www.ing.lu;
▪Calling ING 44.99.1;

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 (applicable to retail customers only)

You have the right not to be subject to decisions which may legally or significantly affect you and that were based solely on automated processing using your personal information. In such cases you may ask to have a person to make the decision instead.

Some of our decisions are the result of automated processes for which you gave us explicit consent or these decisions are necessary to perform or fulfil a contract with you. In both cases, you may ask for human intervention and contest the resulting decision (e.g. automatic refusal of an online credit application).

Your right to object and to contest may be impeded if automated decisions are made for legal reasons.

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

Right to data portability

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

Right to erasure

You may ask us to erase your personal data. However, at times ING is legally obliged to keep your personal data. Your right to be forgotten is only applicable if :

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

Right to complain

Should you as a customer 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 Data Protection Officer (DPO) of ING Luxembourg. You can also contact the Luxembourg data protection authority as mentioned in item 10.

Exercising your rights

How you exercise your rights depends on your ING product and the availability of services in your country. 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 we may charge a reasonable fee for

processing your request if it is considered as abusive, repetitive, or if the request generates excessive costs.

We want to address your request as quickly as possible, and no longer than thirty (30) days following the date of submission of the complaint. However, we could 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's 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 updated 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 May 2020 and enters into force on 1st June 2020. The most recent version is available at www.ing.lu. e.

9. Contact and questions

To learn more about ING's data privacy policies and how we use your personal data, you can primarily contact us through our usual channels by:

- Connecting to your My ING and send us a message with a reference to "Data Protection"
- Visiting your local branch, contacting your relationship manager, your personal or private banker

If you are a Client of ING Luxembourg S.A.: contact ING via dpo@ing.lu referring to "Data Protection"

If you are a Client of ING Lease Luxembourg S.A.: contact ING Lease via contact@lease.ing.lu referring to "Data Protection"

If you are a Client of ING Solutions Investment Management S.A. (ISIM): contact ISIM via data.protection@ing-isim.lu referring to "Data Protection"

In case of disagreement or complaints related to the processing of your personal data, you can send us a request with " Data Protection" as reference via:

- Letter: Complaints Service, 26, Place de la Gare, L-2965 Luxembourg
- E-mail : complaints@ing.lu

If you did not obtain a satisfactory resolution of your case, you can submit a written request to the Data Protection Officer of ING via :
- E-mail: dpo@ing.lu
- Letter: Data Protection Office, 26, Place de la Gare, L-2965 Luxembourg.

You may also lodge your complaint with the Local Data Protection Authority La Commission Nationale pour la Protection des Données (CNPD), L-4370 Belvaux, 15, Boulevard du Jazz, http://cnpd.public.lu) as well as to the judicial authorities.

10. Scope of this Privacy Statement

This is the Privacy Statement of ING Luxembourg and its subsidiaries:

- ING Luxembourg, Société Anonyme, with registered office at 26, Place de la Gare, L-1616 Luxembourg (B.P. L-2965 Luxembourg), R.C.S. number B 6041;
- ING LEASE Luxembourg, Société Anonyme, with registered office at 26, Place de la Gare, L-1616 Luxembourg (B.P. L-2965 Luxembourg), R.C.S. number B 31049;
- ING Solutions Investment Management S.A. (ISIM), Société Anonyme, with registered office at 26, Place de la Gare, L-1616 Luxembourg (B.P. L-2965 Luxembourg), R.C.S. number B 162705

It applies to all entities and branches of ING to the extent that they process personal data.