# Privacy Statement for ING BANK (EURASIA) JSC (ING) employees (version 2.0)

## Contents

## 1. About this Privacy Statement

This Privacy Statement aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to all past, present and prospective ING employees.

We are legally obliged to retain personal data about you, also for a certain period once your relationship with ING has ended, in compliance with GDPR.

Personal data refers to any information that tells us something about you or that we can link to you. This includes your name, address and date of birth, among other things. By processing we mean everything we can do with this data such as collecting it, recording, storing, adjusting, organising, using, disclosing, transferring or deleting.

This Privacy Statement applies to processing personal data of ING employees (including former employees, trainees and job applicants). It does not apply to processing personal data of independent contractors or anyone else hired to work at ING on anything other than on the basis of an employment contract.

## 2. The types of data we collect about you

The personal data we collect includes:

- **Identification data**, such as your name, surname, date and place of birth, ID number, phone number and email address.
- **Personal information,** such as nationality, gender, work permits, photographs, absenteeism, professional experience (profile, previous employers, termination of last employments and work carried out, special projects, outside positions) and education (diplomas, certificates, internships).
- **Financial data,** such as salary information, expenses, payslips and credit worthiness.
- **Socio-demographic data**, such as whether you have a partner and have children.
- **Dependents data**, such as information about your partner and children or other dependents.
- **Online behaviour,** such as the web pages you visit and use of social media.
- **Interests and needs**, for example hobbies and memberships you share with us.
- **Audio-visual data,** such as surveillance videos at ING offices and car parks or recordings of phone calls to our service centres.

### Sensitive data

We do not record sensitive data relating to your health, ethnicity, religion, criminal record or political beliefs unless it is strictly necessary and is legally allowed. When we do, it is limited to specific circumstances, for example running a background check when you apply for a job.

We are legally obliged to keep a copy of your passport.

## 3. What we do with your personal data

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

### Human resources and personnel management.

As your employer we process information about you that is necessary to fulfil our employment or other contract with you (or to take necessary steps at your request before entering into a contract), for administrative purposes, and to manage our relationship with you, i.e. recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, insider trading regulations, performance evaluations, training, travel and expenses, employee communications, workforce analytics, international assignments, dispute resolution and litigation.

### Executing business processes and internal management.

We may process information about you for activities such as scheduling work, recording time, managing company assets, providing centralised processing facilities for greater efficiency, conducting internal audits and investigations, implementing insider trading and other similar regulations, implementing business controls, and facilitating efficient and effective electronic communications within ING.

### Health, safety and security.

To keep you safe and healthy at work and to protect ING's assets, products, services and reputation, we process data about you that authenticates your employee status, access rights and monitors your compliance with ING regulations.

### Organisational analysis and development and management reporting.

This purpose addresses activities such as conducting employee surveys, managing

mergers, acquisitions and divestitures, and processing your personal data for management reporting and analysis.

### Compliance with legal obligations :

We have a legal obligation to process certain personal data to comply with the laws, regulations and sector-specific guidelines that ING is subject to.

### Protecting your vital interests

It may be necessary to process personal information to protect your vital interests, for example in a medical emergency.

### Preventing and detecting fraud and data security

We have a duty to safeguard ING's security and integrity as well as that of the financial sector as a whole. This means collecting information that will help us identify, prevent and investigate activities that may have a negative effect on ING or other financial institutions; defend, prevent and trace actual or attempted conduct that is criminal or undesirable; use and participate in sector-specific and other warning systems and comply with our legal requirements and regulations against money laundering and terrorist financing.

### Examples of when we may disclose your personal information:

- If it is required or permitted by an applicable law or regulation. We endeavour to not disclose more personal information than is specifically required.
- It is requested for a valid legal process such as a search warrant, subpoena or court order;
- As part of ING's regular reporting activities to other ING entities.

### Personalised marketing:

We will not provide, use or otherwise process your data for direct marketing purposes on behalf of third parties without your prior consent. We may use your data to provide benefits for ING staff, such as agreed upon discounts for products or services, unless it is not legally allowed without your consent.

### Limitations on processing data of your dependents:

ING may process the personal data of your dependents if you (or your dependent) gave us the data with consent; if it is reasonable and necessary to fulfil your employment contract; for managing our employment relationship; or it is legally required or permitted under local law.

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

We share certain information internally and outside of ING. This includes with:

### ING entities

We transfer data across ING businesses and branches for operational, regulatory or reporting purposes, for example to comply with certain laws, secure IT systems or provide certain services. We may also transfer data to centralised storage systems or to process it globally for more efficiency. All internal data transfers are in line with our Global Data Protection Policy.

### Authorised ING employees

Certain employees are authorised to process your personal data for legitimate purposes (see section 3 'What we do with your personal data'). They are only authorised to do so to the extent that is needed for that purpose and to perform their job.

### Government authorities

To comply with our regulatory obligations we may disclose data to the relevant authorities. In some cases, we are obliged 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. your salary). We may process your social security number for this.
- Judicial/investigative authorities such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.

### Service providers

When we use external service providers we only share personal data that is required for a particular assignment. Service providers support us with activities like:

- performing certain services and operations
- developing and maintenance of software tools, applications and new services
- preparing reports and statistics.

### Researchers

We are always looking for new insights to help you get ahead in life and in business. For this, we may exchange personal data with partners like universities, who use it in their research, and innovators. The researchers we engage must satisfy the same strict requirements as ING employees. This personal data is shared at an aggregated level and the results of the research are anonymous.

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 safeguards are in place to protect it. For this, ING 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.
- 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.
- Privacy Shield framework that protects personal data transferred to the United States.

## 5. Your rights and how we respect them

We respect your rights as an employee 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 to ask us to rectify it. If we shared data about you with a third party we will also notify that party.

### Right to object to processing

You can object to ING using your personal data. We will consider your objection and assess 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 to fulfil a contract with you.

## Rights regarding the use of automated decisions

We sometimes use systems to make automated decisions based on your personal information if this is necessary to enter into a contract with you or fulfil a contract. You have the right to 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 information 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
- 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. Where technically feasible, we will transfer your personal data.

## Right to erasure

You may ask us to erase your personal data if:

- we no longer need it for its original purpose
- you object to us processing your data for our own legitimate interests and your claim has been found legitimate
- ING unlawfully processes your personal data
- a law of the European Union or a member state of the European Union requires ING to erase 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. If you are still unhappy with our reaction to your complaint, you can escalate it to your local data protection officer. You can also contact the data protection authority in your country.

## Exercising your rights

If you want to exercise your rights or submit a complaint, please contact us via the information provided on the privacy tab under your profile page on One Intranet - https://intranet.ing.net/sites/HR-

We aim to respond to your request as quickly as possible. In some instances this could

take up to one month (if 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.

If the request requirements (as set out in GDPP for Employees) are not fulfilled, we may deny your request. Within a month we will let you know why your request was denied.

## 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 an employer and fulfil our associated contractual duties. There is also information that we are legally obliged to collect or that we need to perform certain HR processes. What we expect from you is to deliver us the data needed. Without this data we may not be able to hire you into ING or maintain your contract.

## 7. How we protect your personal data

We apply an internal framework of policies and minimum standards across all of ING 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.

For more information, look at our Global Minimum Standard or the complete Global Data Protection Policy (GDPP) for Employee Data.

In addition, all 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:

- Log off from your system 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

ING collects and stores data globally as we operate across many borders. We must therefore align with the local retention laws in each country. We are only allowed to keep your personal data for as long as it's still necessary for the purpose we initially required it. Your personal data will be retained no longer than legally necessary.

Once the applicable retention period ends, we act promptly to make sure the data is securely deleted or destroyed, anonymised or transferred to an archive (unless prohibited by law or an applicable records retentions schedule).

## 10. Contact us

If you want to know more about ING's data policies and how we use your personal data, including contact information per country please visit the privacy tab under your profile on One Intranet.

## 11. Scope of this Privacy Statement

This is the Privacy Statement of ING Bank N.V. and its group companies (referred to as 'ING'). It applies to all entities of ING to the extent that they process 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. The most recent version is available at the ING Intranet as well as on the local ING intranet in each country where we operate.