# Privacy Statement for Suppliers

## 1. About this Privacy Statement

This is a Privacy Statement for personnel of all past, present and prospective third parties ('supplier' and hereafter referred to as 'you' or 'your') that provide goods or services to ING Bank (Australia) Limited, all its entities, subsidiaries, branches, representative offices, affiliates and other ING group companies ('ING', 'we', 'us'" and 'our').

This includes:

- Suppliers who would qualify as natural persons.
- Personnel who sign or represent on behalf of suppliers.
- Sales or delivery staff who visit or work at ING premises.

This Privacy Statement applies to us as long as we process personal information ("data") that belongs to individuals ('you'). This Privacy Statement is a statement to let you know how we process your personal data.

By 'personal data' we mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not'

By "processing" we mean everything we can do with this information such as collecting it, recording, storing, adjusting, organising, using, disclosing, transferring or deleting.

This Policy addresses the processing of all personal data of suppliers by ING or by a third party on behalf of ING.

## 2. Purpose and Scope of this Privacy Statement

### Background and Overview

At ING, we believe that it's important we handle all information with care. In particular, the security and confidentiality of all proprietary information and data processing, including suppliers' personal information, must be safeguarded in accordance with applicable laws and regulations.

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, we have implemented data protection principles on a global scale, through our Global Data Protection Policy (GDPP).

The GDPP is binding on all ING entities, subsidiaries, branches, representative offices, and affiliates worldwide and approved by the EU data protection authorities. Therefore, in addition to local privacy laws and regulations, we have resolved that all its entities, subsidiaries, branches, representative offices, and affiliates worldwide will comply with GDPP, regardless of geographical location, market typology or target customer.

ING Bank (Australia) Limited (ABN 24 000 893 292) is bound by the provisions of the Privacy Act 1988 (Cth) and the Privacy (Credit Reporting) Code 2014 (Version 2).

### Purpose

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

### Scope

This Privacy Statement applies to personnel of all past, present and prospective third parties that provide goods or services to ING. This includes:

- Suppliers who would qualify as natural persons.
- Personnel who sign or represent on behalf of suppliers.
- Sales or delivery staff who visit or work at ING premises.

### Commencement

This Privacy Statement was approved by the Non-Financial Risk Committee on 8 December 2021.

## 3. The types of personal data we process

**Principle: Personal data refers to any information that identifies you or can be linked to a natural person. At ING, we collect your personal data from a variety of sources. The personal data we collect and process and the circumstances of that collection includes the following categories:**

- **Identification data**, such as your name, surname, address, telephone number, email, title, nationality or a specimen signature, fiscal code/social security number may be collected from you or from your employer.
- **Public sources data**, such as government registers, commercial registers, registers of association and the media, or is legitimately provided by other companies within the ING entities or third parties such as a stock exchange or company registry body.
- **Audio-visual data**, such as surveillance videos at ING buildings or branches or recordings of phone calls to our service centres. For example, photographs may be used to provide access badges.
- **Online behaviour and preferences data**, such as the IP address of your mobile device or computer you use and the pages you visit on ING websites and apps.

### Sensitive data

**Principle: Sensitive data is information 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). At ING, we may process your sensitive data if strictly necessary and/or it is legally required under local law.**

Example:

- For Know Your Supplier (KYS) data obligations, we may process sensitive data to ensure that we engage with a supplier who is fair and its management is not engaged in ethical or fraud violations.
- When monitoring money laundering or terrorism financing, and reporting to the competent regulatory authorities.

## 4. What we do with your personal data

**Principle: 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.**

At ING, we only use your personal data for business purposes such as:

### Administration of contracts or purchase orders

As we need to administer the contracts and purchase orders, we may contact you via mail, message or call if your company nominates you as the point of contact. Furthermore, we process personal data of your management and/or personnel in a request for information, request for proposal or another competitive tendering procedure to assess whether you are eligible to provide the requested products and services.

### Payment of invoices

As a representative of a supplier, you would send us invoices. For this, we process your personal data to process the invoices or follow up on clarifications regarding the received invoices.

### Access and security management

As a representative of the supplier, you may visit us. For this, we process your personal data to provide you access to our buildings. Part of ensuring that our building remains secure, our security management team may process your personal data.

### Internal and external reporting

We may process your data for our administration and reporting to help our management to make better decisions inline our policies and procedures.

### Compliance with legal and regulatory 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. We process your data to comply with a range of legal obligations and statutory requirements. For example, to comply with regulations against money laundering, terrorism financing and tax fraud, such as Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and the Proceeds of Crime Act 2002, we may conduct supplier due diligence process to verify that your company or its management or its ultimate owners are not associated with terrorism or fraud related activities.

### Protecting your vital interests

It may be necessary to process personal information to protect your vital interests, for example in a medical emergency while you are a visitor at our premises.

### Managing queries and complaints

We record conversations we may have with you online, by telephone, by email or in person in accordance with applicable local laws and our procedure.

Examples of when we may disclose your personal information:

- If it is required or permitted by an applicable law or regulation. For example, in case of theft at premises, the police may ask us data about all visitors on a particular day.
- It is requested for a valid legal process such as a search warrant, subpoena or court order.

***We endeavour to not disclose more personal information than is specifically required.**

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

**Principle: We may share certain data internally (with other ING businesses/departments) and externally (with third parties outside of ING).**

To be able to operate our business in effective and efficient ways, we share certain data. This may include disclosure of your personal data to recipients overseas. The countries to which your personal data may be sent include the Netherlands, Philippines, Poland, Singapore, Slovakia and the United Kingdom.

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

- Requirements based on applicable Australian 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.

### ING entities

We transfer data across ING businesses and branches for various purposes (see section 'What we do with your personal data'). 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 Global Data Protection Policy (GDPP), and any applicable local laws and regulations.

### Service providers

We share data with our service providers who act on our behalf or jointly with us. We only share personal data that is required for a particular assignment. These service providers are selected in accordance with our procurement requirements. Service providers support us with activities like:

- Performing certain services and operations, or
- Designing and maintenance of internet-based tools and applications.

### Authorities

To comply with our regulatory obligations we may disclose data to the relevant authorities, such as:

- **Public authorities, government 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 deposit, payment or savings accounts or holdings on an investment account) or your invoices. If required by local law, we may process your social security number for this.
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and external dispute resolution bodies on their express and legal request.
- **Lawyers, auditors, financial advisors, researchers and other professional advisors.**

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. However, as a general rule, we only keep the relevant identification data (also included in the contracts) for a period of 7 years after our relationship with you has ended.

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.

## 6. Your duty to provide data

**Principle: We aim to only ask you for personal data that is strictly necessary for the relevant purpose. Not providing this information may mean we cannot commence our relationship with you.**

There is certain information that we must know about you so that we can commence and execute our duties relating fulfilment of business relationship with your company.

There is also information that we are legally obliged to collect. Hence, it is expected that you will provide us with relevant personal data that is requested. If you do not provide us with personal data we request, we may not be able to fulfil the contractual duties we have towards you or your employer.

## 7. Your rights and how we respect them

**Principle: You have certain privacy rights when it comes to the processing of your personal data.**

These privacy rights may vary from jurisdiction to jurisdiction, depending on the applicable laws. If you have questions about which rights apply to you, please contact us through the email address mentioned in section 10.

We respect the following rights:

### Right to access information

You have the right to ask us for an overview of your personal data that we process and/or a copy of this data.

### 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 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.

### 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, and based on applicable local law, we will transfer your personal data.

### 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 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.

## 8. How we protect your personal data

**Principle: 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 remain current 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 your personal data may have been compromised.

## 9. Changes to this privacy statement

**Principle: We may amend this privacy statement to remain compliant with any changes in law and/or to reflect how we process personal data.**

## 10. Contacts and questions

To find out more about ING's data privacy policy and how we use your personal data, you can contact the procurement officer for your contract or contact us using the contact information below.

| Country | Contact details ING | Data protection authority |
|---|---|---|
| Australia | privacyaccessrequests@ing.com.au | Office of the Australian Information Commissioner https://oaic.gov.au/ |

## 11. Right to complain

Should you 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. If you are not satisfied with how your complaint is handled, you may make a complaint to the Privacy Commissioner. The Privacy Commissioner can be contacted on the following details:

**Visit** www.oaic.gov.au

**Email** enquiries@oaic.gov.au

**Call the Privacy Hotline** 1300 363 992

**Write** Office of the Australian Information Commissioner,
GPO Box 5218
Sydney NSW 2001

### Exercising your rights

When exercising your right, the more specific you are with your application, the better we can handle your question. For this, we ask you or your representative to prove your identity. We do this to ensure that someone else does not exercise your rights.

Our privacy policy contains information about how you may access the personal data we hold about you and seek correction of that information. It also includes information about how you can complain about a breach of the Australian Privacy Principles, and how we will deal with such a complaint.

We aim to respond to your request in one month of ING receiving the request. 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 you want to exercise your rights or submit a complaint, please contact us.

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