Privacy Statement for ING supplier personnel
(V1.1)

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 and approved by the EU Data Protection Authorities. 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 customer.

This is the Privacy Statement of ING Bank N.V. and its group companies (hereafter referred to as 'ING', 'we', 'us' or 'our'). It applies to all entities and branches of ING to the extent that they process personal data.

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 is a Privacy Statement for personnel of all past, present and prospective third party that provides goods or services to ING ('supplier' and hereafter referred to as 'you' or 'your'). 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.

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:

- **Identification data**, such as your name, surname, address, telephone number, email, title, nationality or a specimen signature, fiscal code/social security number.
- **Public sources data**, we collect and use data that is available from public sources 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 badge.
- **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;

In situations wherein your company assigns you to work for ING as an external contractor, your personal data are generally processed similar to the processing of personal data of an ING employee. For details of such processing we refer to the ING Privacy Statement for Employees (if applicable) as published on the ING's intranet.

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

- We are required or allowed by applicable local law to process such sensitive data.
- You provide sensitive data to enter into or perform an agreement or in a payment order.

For 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 on money laundering or terrorism financing, and reporting to the competent regulatory authorities.

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 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, 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. We endeavor to not disclose more personal information than is specifically required. 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;

4. Who we share your data with and why

To be able to operate our business in effective and efficient ways, we share certain data. We share data internally and externally i.e., outside ING.

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. 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.
- Adequacy decisions by the European Commission, which establish whether a country outside of the EEA ensures personal data is adequately protected.

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.

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.

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.

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.
-

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.

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. You can also contact the data protection authority in your country if applicable.

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.

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.

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 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.

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 January 22th, 2021.

9. Contact and questions

If you want to know more about ING's data privacy policies and how we use your personal data, you can contact the procurement officer for your contract or send us an email.

Country	Contact details ING	Data Protection Authority
Australia	customer.service@ing.com.au	OAIC- Office of the Australian Information Commissioner https://oaic.gov.au/
Belgium	ing-be-privacyoffice@ing.com	Belgian Privacy Commission http://www.privacycommission.be
Bulgaria	Emil.Varbanov@ing.com	Commission for Personal Data Protection https://www.cpdp.bg/

Country	Contact details ING	Data Protection Authority
China	dpochina@asia.ing.com	
Czech Republic	Dpo-cz@ing.com	Úřad pro ochranu osobních údajů https://www.uoou.cz
France	Dpo.privacy.france@ing.com	Commission Nationale Informatique et Libertés https://www.cnil.fr/fr
Germany	datenschutz@ing.de	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de/
Hong Kong	dpohongkong@asia.ing.com	PCPD- Privacy Commissioner for Personal Data, Hong Kong https://www.pcpd.org.hk/
Hungary	communications.hu@ingbank.com	Hungarian National Authority for Data Protection and Freedom of Information http://www.naih.hu/
Italy	privacy@ingdirect.it	Garante per la protezione dei dati personali www.gpdp.it www.garanteprivacy.it www.dataprotection.org
Japan	dpotokyo@asia.ing.com	PPC – Personal Information protection Commission Japan https://www.ppc.go.jp/en/
Luxembourg	dpo@ing.lu	CNPD - Commission Nationale pour la Protection des Données https://cnpd.public.lu
Malaysia	dpomalaysia@asia.ing.com	PDP - Jabatan Perlindungan Data Peribadi http://www.pdp.gov.my/index.php/en/
Netherlands	privacyloket@ing.nl	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/
Philippines	dpomanila@asia.ing.com	National Privacy Commission https://privacy.gov.ph/
Poland	abi@ingbank.pl	Generalny Inspektor Ochrony Danych Osobowych http://www.giodo.gov.pl/
Portugal	dpo@ing.es	CNPD- Comissão Nacional de Protecção de Dados https://www.cnpd.pt

Country	Contact details ING	Data Protection Authority
Romania	protectiadatelor@ing.ro	National Supervisory Authority for Personal Data Processing (ANSPDCP) http://www.dataprotection.ro/
Russia	Mail.russia@ingbank.com	The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) https://rkn.gov.ru/
Singapore	dposingapore@asia.ing.com	PDPC- Personal Data Protection Commission Singapore https://www.pdpc.gov.sg/
Slovakia	dpo@ing.sk	Úrad na ochranu osobných údajov Slovenskej republiky https://dataprotection.gov.sk/uoou/
South Korea	dposouthkorea@asia.ing.com	
Spain	dpo@ing.es	Agencia Española de Protección de Datos https://www.agpd.es
Taiwan	70th floor, Taipei 101 Tower 7 XinYi Road, Sec. 5 11049 Taipei Taiwan	
Ukraine	dpe.offfice@ing.com	Personal Data Protection department of Ombudsman http://www.ombudsman.gov.ua
United Kingdom	ukdpo@ing.com	Information Commissioner's Office (ICO) https://ico.org.uk