Privacy statement
for
ING applicants

(V1.0)

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, 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 of job applicants.

This is the privacy statement for applicants of ING Bank N.V., all its entities, subsidiaries, branches, representative offices, affiliates and other ING group companies ('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 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.

This privacy statement applies to

- all job applicants ('you')

This privacy statement does not apply to

- independent contractors or anyone else hired to work at ING on anything other than on the basis of an employment contract. Please refer to the 'Privacy statement for ING supplier personnel' that can be found on https://www.ing.com/Privacy-Statement.htm

We obtain your personal data in the following ways:

- You share it with us when you apply for a job or visit our websites.
- From the person who recommended your job application.
- From other available sources such as professional registers; online or traditional media; publicly available sources (such as Thompson Reuters, World Check or judicial platforms); other ING companies; or third parties such as public authorities.

2. The types of personal data we process

Personal data refers to any information that identifies you or can be linked to a natural person. Personal data we process about you includes:

- **Identification data**, such as your name, surname, date and place of birth, ID number, passport number, other data in your ID document, driving licence, passport or other document confirming your identity, social security number, home address or place of residence, phone number and email address.
- **Personal information,** such as nationality; gender; work permits; photographs; professional experience (profile, previous employers, termination of last employments and work carried out, special projects, outside positions); education, professional qualifications and continuous training (diplomas, certificates, internships);

- **Interests and needs**, for example hobbies and memberships you share with us.
- **Audio-visual data,** where it's applicable and legally allowed, we process surveillance videos of ING offices and car parks.

Sensitive data

Sensitive data is information relating to your health, ethnicity, religious or political beliefs, genetic or biometric data, or criminal records.

We may process your sensitive data if

- it is legally required and allowed to do so under local law. For example, we may be obliged to keep a copy of your passport or identity card when you become an ING employee.

3. What we do with your personal data

Processing refers to 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 the following business purposes:

Human resources and personnel management

As your potential employer we process information about you that is necessary to fulfil our contractual obligations, or to take necessary steps at your request before entering into a contract. We also process information about you when we have a legal obligation to do so, or it is in our legitimate interest, such as for administrative purposes, and to manage our relationship with you. Activities falling under this purpose include recruitment.

When processing personal data that is not compatible with one of the purposes above, we ask for your explicit consent, which you may withhold or withdraw at any time.

Retention of your personal data

We are legally required to retain your personal data for a specified period of time. This retention period is one month, and with your consent one year in case you withdraw your application or ING rejects your application. When you become an employee of ING you can find attached to this privacy statement a document called Retention Period with some examples of data with their retention period. When we no longer need your personal data for the process or activity we originally collected it for, we delete it, or aggregate it (bundle data at a certain abstraction level), render it anonymous and dispose of it in accordance with the applicable laws and regulations.

4. Who we share your data with and why

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

Whenever we share personal data in countries outside of the European Economic Area (EEA) -- whether internally or with third parties – we ensure there are safeguards in place to protect it. For this purpose, we rely on (among) others:

- 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.
- Applicable local laws and regulations.
- EU Model clauses, when applicable. We use standard contractual clauses in agreements with service providers to ensure personal data transferred outside of the EEA complies with EU General Data Protection Regulations (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'). We may also transfer data to centralised storage systems or for processing centrally within ING for efficiency purposes. For all internal data transfers we rely on our GDPP and on the applicable local laws and regulations.

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. All employees are subject to confidentiality obligations, also according to local requirements.

Government, supervisory and judicial authorities

To comply with our regulatory obligations we may disclose data to the relevant government, supervisory or judicial 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 and other financial sector supervisors in 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 or tax identification 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 and other third parties

When it is required for a particular task, we may share your personal data with external service providers or other third parties who carry out certain activities for ING in the normal course of our business.

Service providers support us with activities like:

- performing certain services and operations
- designing, developing and maintaining internet-based tools and applications
- IT services such as applications or infrastructure e.g. cloud services
- preparing reports and statistics, printing materials and product design
- recruitment

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 (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. This personal data is shared at an aggregated level and, as far as possible, 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.

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.

5. Your rights and how we respect them

You have certain privacy rights when it comes to processing of your personal data. These 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 via the contact details in chapter 9.

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 have shared data about you with a third party, we will also notify that party of any corrections made.

Right to object to processing

You can object to us using your personal data for our own legitimate interest – if you have a justifiable reason. We will consider your objection and assess whether there is 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 for fulfilling a contract with you.

Rights regarding the use of automated decisions

When it's legally permissible, we sometimes use systems to make automated decisions based on your personal information that are necessary for fulfilling a contract with you. If automated decisions are used, we will inform you about this. You have the right to object to such automated decisions and 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 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

We are legally obliged to keep certain personal data for a specified period of time. You may ask us to erase your online personal data and the right to be forgotten is applicable if:

- we no longer need your personal data for its original purpose
- you withdraw your consent for processing it
- you object to us processing your personal data for our own legitimate interests and we find your claim to be legitimate
- we unlawfully process your personal data
- a local law 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 to us. If you are 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 if applicable.

Exercising your rights

If you want to exercise your rights or submit a complaint, please contact us via the contact details under chapter 9.

If the requirements for your request (as set out in the GDPP for employees) are not fulfilled, your request may be denied. If permitted by law, we will notify you of the reason for denial.

We aim to address your request as quickly as possible. However, our response time may vary based on your location and applicable local laws. Should we require to complete your request than is legally allowed, we will notify you immediately and provide reasons for the delay.

6. Your duty to provide data

As your potential employer, there is certain personal information we are legally required to collect, or that we need to execute our duties and fulfil our contractual obligations. There is also information that we need for certain HR processes. 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 hire you.

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 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.

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 we process personal data. This version was created on 1 January 2021.

9. Contact and questions

To find out more about ING's data privacy policy and how we use your personal data you can find contact information per country below.

Country	Contact details ING	Data protection authority
Australia	privacyaccessrequests@ing.com.au	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/
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

Country	Contact details ING	Data protection authority
Germany	datenschutz@ing.de	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit https://datenschutz.hessen.de/
Hong Kong	dpohongkong@asia.ing.com	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_dipendenti@ing.it	Garante per la protezione dei dati personali www.gpdp.it www.garanteprivacy.it www.dataprotection.org
Japan	dpotokyo@asia.ing.com	Personal Information Protection Commission Japan https://www.ppc.go.jp/en/
Luxembourg	dpo@ing.lu	Commission Nationale pour la Protection des Données https://cnpd.public.lu
Malaysia	dpomalaysia@asia.ing.com	Jabatan Perlindungan Data Peribadi http://www.pdp.gov.my/index.php/en/
Netherlands	privacyloket@ing.com	Autoriteit Persoonsgegevens https://autoriteitpersoonsgegevens.nl/
Philippines	dpomanila@asia.ing.com	National Privacy Commission https://privacy.gov.ph/
Poland	For ING bank abi@ingbank.pl For IBSS Poland: DPO.TechPL@ing.com	Prezes Urzędu Ochrony Danych Osobowych https://uodo.gov.pl/
Portugal	dpo@ing.es	Comissão Nacional de Protecção de Dados https://www.cnpd.pt
Romania	protectiadatelor@ing.ro	National Supervisory Authority for Personal Data Processing http://www.dataprotection.ro/
Russia	Mail.russia@ingbank.com	Federal Service for Supervision of Communications, Information

Country	Contact details ING	Data protection authority
		Technology, and Mass Media https://rkn.gov.ru/
Singapore	dposingapore@asia.ing.com	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) https://ico.org.uk

Retention periods

Data of a temporary nature which are kept in the (digital) personnel files:

Retention period (maximum):

- performance assessments, agreements on career objectives, mid-year reviews, coaching interviews, and training and education data as well as notes/reports of conversations between manager and employee:
  5 years
- company test results (assessment), psychological examination report:
  2 years
  documents relating to complaints procedures (the complaint or request to decide on a complaint, the recommendation of the complaints committee; senior management's decision):
  5 years
- written request to exercise the right of access; overview of data provided:
  2 years
- additional positions:
  3 months after expiry
- attachment of earnings:
  for the duration of the attachment
- data for performance of a specific employment condition/arrangement or individual agreements after termination of the employment contract:
  2 years
- payment
  records: 7
  years
- payroll accounts data of a permanent nature after termination of employment:
  7 years
- File on rejected job applicant:
  up to 4 weeks after termination of selection procedure
- Administrative sickness absence data/Reintegration file:
  in principle up to 2 years after the end of the employment contract, unless a longer period must be observed pursuant to other legal provisions

NB:
The data must be deleted after the retention period expires.
That does not mean that the data must also be destroyed in all cases. It is sufficient for the data to be placed beyond the reach of active administration and records keeping
and to be stored in a repository or on a separate disk.
The personal data may be kept in an archive if it is designated for historical, statistical or scientific purposes.