ING BANK N.V. Hungary Branch

Privacy statement for ING job applicants

(V2.0)

Contents

ING Bank N.V., and ING Bank N.V. Hungary Branch are a European financial institution and are 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 job applicants of **ING Bank N.V.** (a corporation organized and existing under the laws of the Netherlands having its registered office at Bijlmerdreef 106, 1102 CT in Amsterdam, place and number of registration: Trade Register of the Chamber of Commerce and Industry for Amsterdam, no. 33031431) represented by its financial branch office **ING Bank N.V. Hungary Branch** (having its registered office at H-1068 Budapest, Dózsa György út 84/B, place and number of registration: Metropolitan Court as court of Registration, Budapest; Cg.: 01-17-000547) acting on behalf of its founder in accordance with Section 24 of the Act CXXXII of 1997 on Hungarian Branch Offices and Commercial Representative Offices of Foreign-Registered Companies ("ING", "we", "us" and "our"). and it applies to us as long as we process personal data that belongs to individuals.

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

- past and present employees, including trainees, and
- independent contractors or anyone else hired to work at ING on anything other than on the basis of an employment contract.

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 (eg. CV database sites, such as Profession.hu or LinkedIn); 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, number of your driving licence, passport number or other document confirming your identity, social security number, home address or place of residence, phone number and email address.
  Please be informed that we do not keep copy of those cards, which proves your identity.

- **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 number, certificates, internships) criminal data.
  Please be informed that we do not keep a copy of your certificate of good conduct, driving licence or any other documents, which proves your education, professional qualifications.
- **Financial data,** such as salary information, bank account number
- **Social Media Check,** we check your social media activity only with reference to your professional experience (such as: LinkedIn)
- **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

- we have your explicit consent;
- it is legally required and allowed to do so under local lawyou provide sensitive data as part of a contractual agreement

For example, we process sensitive data related to:

- Employee due diligence obligations. We may run a background check when you apply for a job at ING. This could include checking your conduct or your involvement in judicial proceedings, according to public sources.

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 a 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 and outplacement. We process your curriculum vitae ('CV') based on your consent, Article 6 (1) b) of the GDPR ((data processing is necessary in order to take steps at the request of the Candidate, to assess the application prior to entering into a contract

of employment)) and in the event of application for a position which requires the establishment of an employment relationship, Article 10 (1) of Act I of 2012 on the Labour Code shall be governing. In accordance with the Act, data and data sheets necessary for the establishment of an employment relationship may be requested before the establishment of an employment relationship.
In the event of a successful application, if it is done through recruitment companies, the Company shall notify recruitment companies on the admission and the initial salary of the Candidate in accordance with the data protection policy of the recruitment company to allow the company to calculate the commission to be paid after a successful recruitment. In the above case, the legal basis for data transfer shall be Article 6 (1) f) of the GDPR (legitimate interests pursued by the Company and the recruiter).
The data processing includes clarification of the content of the job application on the job interview (if any) and processing of personal data related to the professional expectations, wishes communicated by the Candidate on the job interview, professional questions, tasks and competencies.
Such data are received by the Company either directly from the Candidate, or from a third party transferring the data of the Candidate (such as recruiters). In the latter case, data processing shall also be governed by the data processing policy of the third party.
In addition to the above, the Company may keep internal records related to the job applications on the professional competence of the Candidate and related assessment criteria.

Organisational analysis and development and management reporting
This purpose addresses activities such as conducting employee surveys (both locally and globally); managing mergers, acquisitions and divestitures; and processing your personal data for management reporting and analysis, which is performed to fulfil a legitimate interest.

Compliance with legal obligations
In certain instances 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. For example, to fulfil employee due diligence requirements under anti-money laundering legislation.

Preventing and detecting fraud and data security
We have a legal duty and a legitimate interest 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 could 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. This includes detecting and preventing the loss of personal data, as well as the loss or theft of intellectual or physical business property.

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.

Limitations on processing data of your dependents

ING may process the personal data of a dependent if

- you (or your dependent) has provided the data with consent
- it is reasonable and necessary for fulfilling your employment contract or for managing our employment relationship, or
- it is legally required or permitted under local law.

Retention of your personal data

We are legally required to retain your personal data for a specified period of time. This retention period may vary from a few days to years, depending on the applicable local law. 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. Relevant retention period:

- Candidates' curriculum vitae: 6 months, from the date of giving your consent. Having signed the employment agreement, it will change to till end of the employment + 3 years.
- In accordance with Section 6:22 of the Civil Code, the data retention time shall be 6 months after the conclusion of the application (that is the selection of the successful Candidate), in order to ensure the possibility of defense in the event of litigation or official proceedings initiated by the Candidate (data may be processed until the final decision of the proceedings) or for the future assessment of job applications it may be justified for the Company to keep it on record internally for the afore-mentioned period in case somebody earlier applied for a job at the Company. In this case, the legal basis for data processing is Article 6 (1) f) of the GDPR (legitimate interest of the Company). The data processing is necessary for pursuing the legitimate interests of the Company, that is the participation in proceeding(s) related to the enforcement of claims, and the presentation of the Company's defense, or the registration of the former applications of the Candidate to the Company. The Candidate may be considered as potential applicant in other similar position in the future.
- In certain cases, a shorter data retention is applicable to the Company, for example, there may be a case, when the Company receives the personal data of the Candidate from a third party's CV database. In such case, the Company must delete the personal data within the deadline determined by the third party who is operating the database. For example, the general terms and conditions of profession.hu provides that in case of access to the CV database according to the above general terms and conditions, the Company may contact the relevant person within 90 days from downloading his/her CV or other document, and process his/her data.

- Should the Candidate cancel his/her application before the end of the application process at one of the contacts of the Company, the Company shall immediately delete the data of the Candidate after the cancellation. The Company shall consider the cancellation of the application, as if the Candidate has expressed that he/she did not wish to enforce any claims with respect to the application and does not want to enter into a contract with the Company.

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, LDPP 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

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 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 *(The Hungarian National Authority for Data Protection and Freedom of Information*) in Hungary.

Right to withdraw consent

Once you have provided consent for one of the data processing purposes previously defined and no other legal basis for processing, or applicable legal regulation would oblige ING to further process your personal data, you may be able to provide for the withdrawal of your consent by indicating the scope of personal data, for which you withdraw your consent from at the *dataprotection.hu@ing.com*.

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 Employee Data) 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.. In some instances, this could take up to one month. We shall respond to your enquiry within a month (30 days), otherwise should we 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.

If the request requirements (as set out in GDPP for Employee Data) 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

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 25 May 2021.

9. Contact and questions

To find out more about ING's data privacy policy and how we use your personal data, You can also 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
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/

Country	Contact details ING	Data protection authority
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 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

Country	Contact details ING	Data protection authority
United Kingdom	ukdpo@ing.com	Information Commissioner's Office) https://ico.org.uk

10. Additional remedies

The National Authority for Data Protection and Freedom of Information (NAIH)

1374 Budapest, Pf. 603.

Website: www.naih.hu

Tel .: + 36-1-391-1400

Court
In Hungary, the court may, at the option of the person concerned, also institute proceedings before the court of the place of residence or stay of the person concerned.