

**Privacy statement for  
ING applicants**  
(v. 2.1)

Contents

- 1. Purpose and scope of this privacy statement ..... 3
- 2. The types of personal data we process ..... 3
- 3. What we do with your personal data..... 5
- 4. Who we share your data with and why ..... 6
- 5. Your rights and how we respect them ..... 8
- 6. Your duty to provide data ..... 10
- 7. How we protect your personal data ..... 10
- 8. Changes to this privacy statement ..... 10
- 9. Contact and questions ..... 10

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 also ING Hubs B.V. established and existing under the laws of Netherlands, based in Amsterdam, address: Bijlmerdreef 106, 1102 CT Amsterdam, the Netherlands, registered in the Netherlands Chamber of Commerce Commercial Register under the number 65184769, operating in Poland as a Branch under the business name ING Hubs B.V. spółka z ograniczoną odpowiedzialnością Oddział w Polsce with its registered office in Katowice, ul. Zabrska 19, 40-083 Katowice, Tax Identification Number [NIP]: 2050005130, National Court Register 0000702305, (“ING Hubs Poland”) who is a Controller of your personal data. 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.

## 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 contractors, their representatives, their employees and their co-workers. Please refer to the 'Privacy statement for ING supplier personnel' that can be found on ING Hubs Poland website.

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; publicly available sources; 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 such data as:

- **Identification data**, such as your name, surname, date and place of birth, ID number, passport number, other data in your ID document, , passport or other document confirming your identity, home address or place of residence, phone number and email address - In case of foreigners we may also process data present on: Residence card, Voivode's decision, visa, The Card of the Pole, temporary residence permission, student status in Poland. - pursuant to the provision of article 6 clause 1 letter b) and c) GDPR, in accordance with article 22 [1] of the Labour Code.
- **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) - pursuant to the provision of article 6 clause 1 letter b) and c) GDPR, in accordance with article 22 [1] of the Labour Code.
- **Interests and needs**, for example hobbies and memberships you share with us - pursuant to the provision of article 6 clause 1 letter a) GDPR in accordance with

article 22 [1a] of the Labour Code.

- **Audio-visual data**, where it's applicable and legally allowed, e.g. our online meetings during recruitment process via communication platforms, like MS Teams - pursuant to article 6 clause 1 letter f) GDPR
- **Other personal data** provided to us in the CV or cover letter are processed basing on your consent - pursuant to article 6 clause 1 letter a) GDPR in accordance with article 22 [1a] of the Labour Code.

Your personal data processed for the needs of future recruitments are processed on the basis of your consent pursuant to article 6 clause 1 letter a) GDPR; Your personal data to the extent it is necessary to take the actions necessary to conclude an employment contract will be processed by us on the basis of article 6 clause 1 letter b) and c) GDPR.

Your personal data (name, surname, e-mail address) will be provided by us in order to verify contractual obligations towards recruitment agencies and, upon request, fraudulent settlements to the program of recruitment of job candidates ("Recommend = Benefit"). Data for this purpose will be processed by us on the basis of article 6 clause 1 letter f) GDPR, our legitimate interest is the need to verify candidates with recruitment agencies or other recommending candidates for work and to counteract fraud and reputational damages.

## 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 pursuant to article 9 and 10 GDPR 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 which may contain biometric data, when you become an ING employee. - pursuant to the provision of article 6 clause 1 letter b) and c) GDPR in accordance with article 22 [1] of the Labour Code.
- We are obliged to perform employee due diligence obligations. We may run a background check when you apply for a job at ING. This could include checking your criminal convictions in accordance with the Act of 12 April 2018 on the principles of obtaining information about criminal convictions of employees and candidates for employment in entities of financial sector - in accordance with the article 6 clause 1 letter b) and c) GDPR."
- We process your sensitive data (other than criminal records) based on your consent (article 6 clause 1 letter a) GDPR in accordance with article 22 [1a] of

the Labour Code) – if you choose to share your data with us during recruitment process.

Your personal data mentioned above may be the scope of our work also to verify and enforce claims and defend against possible claims. Data condemned for this purpose pursuant to article 6 clause 1 letter f) GDPR, our legitimate interest is to establish the existence, investigation and enforcement of possible claims and defence by claims in response to courts and other state authorities.

### 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.

If you choose to apply for Job Area, meaning you are interested in the job offers not only published by ING Hubs Poland but also by the whole ING Group, please be informed that your data will be accessible for other ING entities who may contact you within open recruitment processes.

#### **Retention of your personal data**

We are legally required to retain your personal data for a specified period of time.

Your personal data will be stored:

a. for the duration of the recruitment process, but not longer than 3 months from its completion; After this time, your personal data (CV) will be automatically deleted from our database, unless your personal data is necessary for the purpose of pursuing and enforcing claims or defending against possible claims - in which case your data will not

- be stored longer than until the dispute is resolved or the expiry of the limitation period, unless we have any other basis for their storage;
- b. for a period of 12 months from the end of the recruitment process conducted by ING Hubs Poland. We will retain your name and e-mail address for verification under our contractual obligations to recruitment agencies and for the purpose of preventing abuse in relation to the internal referral program of job applicants (“You Recommend = You Gain”);
  - c. if you consent to participation in other recruitments conducted by ING Hubs Poland - for a period not longer than 1 year or until you withdraw your consent;
  - d. in the case of concluding a contract - for the period required by relevant provisions of labour law or until the expiry of the limitation period for claims; for 12 months to prevent financial frauds as part of an internal candidate referral program ('You Recommend = You Gain).

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

If you wish to know more of which third parties may process your personal data, please contact us via [DPO.INGHubsPoland@ing.com](mailto:DPO.INGHubsPoland@ing.com)

### 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.

## 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 i.e. the President of the Office for Personal Data Protection (PUODO).

### 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 information which are required by applicable law 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 01.02.2023.

## 9. Contact and questions

To find out more about ING's data privacy policy and how we use your personal data you can contact:

<b>Country</b>	<b>Contact details ING</b>	<b>Data protection authority</b>
Poland	For ING Hubs Poland: DPO.INGHubsPoland@ing.com	Prezes Urzędu Ochrony Danych Osobowych <a href="https://uodo.gov.pl/">https://uodo.gov.pl/</a>
Netherlands	hrlegal.industrialrelations@ing.com	Autoriteit Persoonsgegevens <a href="https://autoriteitpersoonsgegevens.nl/">https://autoriteitpersoonsgegevens.nl/</a>