

Information on the protection of personal data of natural persons by the ING Bank N.V. Czech Republic branch

General information

This information on personal data protection relates to the processing of personal data of natural persons by the Prague branch of ING Bank N.V., a public limited company incorporated under the laws of The Netherlands, with its registered seat at Bijlmerdreef 106, 1102 CT Amsterdam, The Netherlands, registered in the Trade Register of the Chamber of Commerce for Amsterdam under no. 33031431, represented in the Czech Republic by ING Bank N.V., Prague branch, with its company seat at Českomoravská 2420/15, Libeň, 190 00 Praha 9, Czech Republic, Business Identification No.: 49279866, registered in the Commercial Register maintained by the Municipal Court in Praha under the inserted file No. A 7930 (hereinafter “**ING**”).

This information is further elaborated and specified by the Privacy Statement issued by ING Bank N.V. and which is a personal data protection standard applicable to all persons whose personal data are processed by any branch of ING Bank N.V. in all countries where ING Bank N.V. provides its services. You can find it [here](#).

Clients, business partners and suppliers who are not natural persons may use this information to inform the natural persons representing them in relation to ING.

ING processes personal data in accordance with personal data protection legislation (in particular the General Data Protection Regulation (hereinafter “**GDPR**”) and seeks to ensure, by all available and commercially reasonable means, that any processing of personal data takes place in such a way that the privacy of the data subjects has been adequately protected and secured. To this end, ING has established and continuously improves the security of personal data through technical, physical and organizational measures to prevent accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. For this ING has established standards for the information technology used and other internal regulations and processes aimed at securing the personal data that ING processes.

ING processes personal data either a) with the consent of the person to whom the personal data relates, in which case the person is entitled not to provide personal data or to withdraw consent to their processing, or b) processes data regardless of the consent of the person that the personal data relates to. In such a case, ING is entitled to process personal data by a title other than consent, and therefore it is not possible to revoke the consent to the processing of data for these cases. Without the processing of personal data in such cases, ING could neglect its obligations, therefore ING does not provide services to persons who refuse to disclose personal data in cases other than consent.

Persons whose personal data are processed by ING

ING processes personal data, especially of natural persons:

- who are (potential and former) clients, business partners or suppliers of ING;
- who are visitors to the ING website;
- acting as shareholders, beneficial owners, employees, (executive) directors, authorized representatives or contact persons of ING's clients, business partners or suppliers;

- whose personal data are processed by ING as part of the processing of financial transactions or processing without a contractual relationship with the persons concerned, such as the recipients of financial transactions.

Personal data processed by ING

Personal data processed by ING may include, in particular:

- *identification data* - these are data stipulated by law which ING is obliged to collect about its clients and persons acting on their behalf, in particular: names, permanent residence, residential addresses, citizenship, birth number or other personal identifiers, place of birth, sex, type and number of the identity document, issuing authority and period of validity of the document;
- *authentication data* - internal data clearly identifying the client or user, security features of the client or user;
- *contact details* - in particular: address, e-mail, telephone, position with the employer or authorization (e.g. in the case of acting on behalf of a client, supplier or business partner);
- *location data* - in particular: IP addresses, information about the equipment used, visit to the ING website (cookies), location of the mobile device (accidental use for marketing purposes);
- *data on services* - these are data related to the client's behaviour, use of products that can be used for both client service and internal management of ING, development of new products and systems and also for marketing purposes, especially what services the client uses and how, related data, such as account number, payment cards, data on payments and other instructions according to the product type, authorization to handle the client's products, limits and other service restrictions, communication and service requirements of the client, which of these and similar data we derive/create for the needs of the bank;
- *records of a person* - in particular: records of camera systems taken by ING mainly for the protection of ING's property and personal safety and investigation of illegal activities, and records of telephone calls made mainly for the fulfilment of legal obligations, record keeping of services provided to clients for protection the rights of ING as well as clients and for the internal management of ING and the investigation of illegal activities (this is processing necessary for the purposes of the legitimate interests of the administrator or a third party, therefore the consent of the person is not required);
- *other data* - these are data stored and processed mainly for the purpose of providing services to clients and protecting ING security, or to meet legal requirements, in particular such data may be: personal status, account numbers or other unique identifiers, person's signature, copies of identity documents persons, including photographs, copies of documents and documents related to the provision of the service, which are delivered to us by the client, another authorized person or public administration body, complaints, investment questionnaire, written communication with the client or authorized person; in the case of representatives of legal persons also information from public sources;
- *financial data* - information obtained from the client or created during the provision of services to the client, in particular: (financial) transactions, payment details.

Personal data that ING does not process

- *children's personal data*, if they were not our clients
- *sensitive personal data* - in particular data on health, religious or political preferences, etc. Such data may appear in the provision of ING services if you provide them to us yourself, but ING no longer handles this data.

Purposes of personal data processing

ING processes personal data (examples of personal data used) mainly for the following purposes:

Processing necessary for the performance of the contract, therefore, does not require the consent of the person

- provision of services to clients and conclusion and implementation of contracts with clients and business partners - provision of services and related activities that result from the existing contractual relationship, or from the process leading to a contractual relationship, such as evaluation and verification of the client (e.g. identification data, contact data, other data, financial data), it may be the provision of agreed services (e.g. service data, other data, person records), the provision of service to a (potential) client, the resolution of client complaints (e.g. other data, data on services, authentication data);
- the process of verifying the identity of the client or authorized person (e.g. identification data, authentication data), records of persons involved in the contract, i.e. insured persons, beneficiaries, intermediaries, (e.g. identification data, contact details, other data).

Processing on the basis of legal obligations, therefore the consent of the person is not required

- fulfilment of ING's obligations in the fight against money laundering and terrorist financing, in accordance with the laws governing banking services and provision of information to public authorities - procedures for fulfilling ING's obligations under the law, in particular the registration of data identifying the client and persons represent, storage of certain documents on the client's transactions, analysis of transactions, reporting to tax authorities, investigation of suspicious transactions and fulfilment of other obligations imposed by legal and industry regulations (e.g. person records, identification data, contact information, other data, financial data, service data) ;
- obtaining and keeping records for the purpose of fulfilling legal obligations;
- obtaining clients' personal data from public registers in order to update client's data for the fulfilment of ING's obligations in the fight against money laundering and terrorist financing.

Processing necessary for the purposes of the legitimate interests of the controller or a third party, therefore the consent of the person is not required

- ensuring the functioning of the services on the part of ING, including through third parties as suppliers (e.g. data on services);
- protection of security and integrity of ING and/or the financial sector includes a) searching for, preventing, investigating and combating (attempts) illegal or undesirable activities or actions against ING, the ING Group, clients and employees or other financial institutions, b)) use and participation in alert systems (e.g. internal and external fraud databases), c) verification of the status and access rights of clients and business partners and d) processing for the protection of legitimate interests, in particular in the event of litigation (e.g. identification data, financial data, service data, person records, other data, authentication data);
- ING reporting and internal management, statistical evaluation and creation of models, evaluation of client data for aggregated outputs intended for reporting and analysis of processes and products and their changes and their use by clients in order to improve and manage ING product offerings, evaluation of marketing campaigns effectiveness, improving the communication of ING employees with clients, creating a global approach to the client,

managing ING assets, conducting internal audits, accounting and financial matters, implementing controls, measures of central processing solutions to increase efficiency, managing mergers, acquisitions and divisions (e.g. identification data , financial data, person records, data on services, other data, location data, financial data);

- security and protection of ING property and persons in ING premises - use of camera systems, IT systems (e.g. person records, identification data);
- implementation of IT systems - in particular improving the security of the assets of ING, its clients and business partners, improving services to clients and cost-effective provision of central IT systems (e.g. identification data, contact details, service details, financial data);
- keeping a telephone record of the services provided to clients for the protection of ING's and clients' rights and for ING's internal management and investigation of illegal activities (e.g. person records);
- addressing persons representing clients with surveys, especially satisfaction surveys (e.g. identification data, contact details, service details, location details).
- sending ING's and its business partners' marketing offers and sending newsletters (e.g. identification data, contact data, service data, location data);
- customer relationship management (CRM) and (targeted) marketing to build a business relationship and maintain and expand it (e.g. contact information, service information).

Processing based on a consent

- sending ING marketing offers and sending news to persons who are not clients but have given their consent to the processing (e.g. identification data, contact data, location data)
- in the event that a person needs for his/hers purposes, e.g. for the exercise of legal claims, etc., that ING keep his personal data longer than he is entitled to keep and that ING expressly requests this before the expiry of the personal data retention period, see below.

Transfer of personal data

ING may share personal data and pass on personal data to other branches and entities of the ING Group (e.g. taking over identification, providing services on global basis, security and integrity of ING) and/or to third parties such as business partners, other financial institutions (e.g. taking over identification, security and integrity of the financial market, provision of services) or other service providers, intermediaries, recipients of transactions, courts, public authorities, alert systems or other third parties, e.g. suppliers, auditors, law firms (e.g. legal obligations, ING security and integrity, ING internal management) that are involved in achieving any of the purposes listed above. ING shares personal data with third parties and branches and entities of the ING Group, provided that their involvement is necessary to achieve any of the purposes set out above or is required by law. These third parties and branches and entities of the ING Group may also be located outside the European Economic Area.

In addition to the recipients to whom we are obliged to transfer personal data in accordance with applicable law, we transfer personal data mainly to ensure the provision of services to clients, to ensure risk management and ING processes (especially joint group systems and service improvement centres). For marketing purposes we pass on personal data to third parties, such as contractual call centres and intermediaries of our electronic, SMS or physical correspondence. We may also pass them on for identification purposes to another entity.

Third parties who process the transferred personal data are obliged to use the personal data for specified purposes and to ensure the security of personal data at an appropriate level. Third parties

are obliged to comply with the rules on personal data protection and, if they are located outside the European Economic Area, they are obliged to comply with the rules on personal data protection in force in the European Economic Area using standard contractual clauses issued by the European Commission.

Retention period of personal data in ING

- the data required by law are kept by ING for the period required by law, i.e. in the most cases for 10 years from the termination of the business relationship;
- ING also retains data related to the services provided to our clients for 10 years from the termination of the business relationship due to the legitimate interests of both ING and the client, in particular the interest in preserving evidence for judicial and administrative proceedings;
- phone records are retained by ING for a period of 10 years from the termination of the business relationship for the purposes of fulfilling legal obligations and due to the legitimate interests of ING and the client, especially the interest in preserving evidence for court and administrative proceedings;
- in the case of personal data communicated by a non-client in the event of incomplete conclusion of a contract by means of distance communication, ING processes the person's data for a period of 3 months for the purpose of completing the process of concluding the contract;
- for the period for which the client has given ING consent in the event that it processes ING data on the basis of consent;
- for marketing purposes for the period for which the client or a person who is not a client but participates in competitions or other events has given his/her consent for the use of his/her personal data;
- camera recordings in order to protect ING's property and the safety of persons and to investigate illegal activities for a period of 1 month;
- for as long as the person requests ING to retain personal data in order to fulfil his/her interests in the event that ING no longer needs personal data.

Right of access, repair, blocking and deletion

The person whose personal data is processed by ING has the following rights, which can be exercised, for example, by using the form on the ING website:

- the right to request information on the processing of personal data processed by ING or for ING. This information may be in certain situations subject to reasonable charges by ING;
- the right to correct incorrect, incomplete or inaccurate data;
- the right to delete, block or restrict the processing of personal data connected with a person if ING is unauthorized to process said personal data;
- the right to object to processing that is necessary for the purposes of legitimate interests;
- the right to withdraw consent to any purpose of the processing of personal data at any time in cases where the processing of personal data takes place on the basis of a given consent. This consent may also be granted again. Withdrawal of consent does not affect the lawfulness of processing based on the consent that was given before its withdrawal.
- transferability of personal data - a person whose personal data are processed by ING on the basis of a contract or consent has the right to request ING for his/her personal data provided

to ING based on the Article 20 of the GDPR. ING forwards this personal data to a person in the form of a data file via the client's internet banking or by e-mail.

- Every person has the right to object at any time to the processing of his or her personal data for direct marketing purposes.

Contact information

Questions and inquiries regarding the processing of personal data by ING or ambiguities regarding this information may be sent by e-mail at dpo-cz@ing.com or may be sent in writing to:

ING Bank N.V.
Data protection officer
Českomoravská 2420/15
190 00 Prague 9
Czech Republic

The contact person for personal data matters is the Data protection officer, dpo-cz@ing.com.

Each request must include a clear verification of the identity of the person sending the request (officially verified signature) in order to prove that he or she is the subject of the requested data.

If you believe that ING is not complying with data protection law, you can file a complaint with the Office for Personal Data Protection.

This document will be updated regularly.

In Prague on August 4, 2021